Canad. J. Math. Vol. **62** (4), 2010 pp. 787–807
doi:10.4153/CJM-2010-032-0

An Explicit Treatment of Cubic Function Fields with Applications

E. Landquist, P. Rozenhart, R. Scheidler, J. Webster, and Q. Wu

Abstract. We give an explicit treatment of cubic function fields of characteristic at least five. This includes an efficient technique for converting such a field into standard form, formulae for the field discriminant and the genus, simple necessary and sufficient criteria for non-singularity of the defining curve, and a characterization of all triangular integral bases. Our main result is a description of the signature of any rational place in a cubic extension that involves only the defining curve and the order of the base field. All these quantities only require simple polynomial arithmetic as well as a few square-free polynomial factorizations and, in some cases, square and cube root extraction modulo an irreducible polynomial. We also illustrate why and how signature computation plays an important role in computing the class number of the function field. This in turn has applications to the study of zeros of zeta functions of function fields.

1 Introduction

The study of algebraic function fields occupies the intersection between algebraic geometry, complex analysis, algebraic number theory, and arithmetic geometry. Algebraic geometry studies the underlying curves of algebraic function fields. The connection to complex analysis is through meromorphic functions on compact Riemann surfaces, which form a function field over the complex numbers. The algebraic approach to function fields via the study of algebraic functions dates back to the 1800's and produced major results in the first half of the twentieth century through the work of Artin, Schmidt, Weil, and others; in the interest of space, we forego citing individual references. Arithmetic geometry focuses on the number theory of function fields; this is the context of this paper.

More recently, algebraic curves and function fields have begun to undergo investigation from a more algorithmic perspective. While algorithmic questions in function fields are of interest in their own right, they have additional significance due to their applications to cryptography (particularly elliptic and hyperelliptic curves) and coding theory, *e.g.*, Goppa codes. For example, efficient arithmetic for divisors on a curve is the subject of intense study, since it is a necessary ingredient for implementing curve-based public key cryptography, computing the class number, solving the dis-

Received by the editors November 21, 2007; revised April 30, 2008.
Published electronically January 26, 2010.
Research of the third author supported by NSERC of Canada.
AMS subject classification: **14H05**, 11R58, 14H45, 11G20, 11G30, 11R16, 11R29.
Keywords: cubic function field, discriminant, non-singularity, integral basis, genus, signature of a place, class number.

crete logarithm problem in the Jacobian, and other problems. Generally, these types of algorithms require prior knowledge of such quantities as the genus, the discriminant, an integral basis (describing the coordinate ring as a module over the ring of polynomials), the set of singular points, or signatures of certain places of the rational function field in the extension field.

Generic methods for finding some of these quantities certainly exist. For example, the well-known Hurwitz formula can be used to find the genus, provided the signatures of all the ramified primes are known; for the finite primes, this amounts to knowing the field discriminant. Kummer's theorem provides signatures, but does not give conclusive answers for primes corresponding to singular points. According to [5], an integral basis can be computed in polynomial time, and the Round 2 algorithm and its variants [3, 18] will produce such a basis. However, actual implementations of this method are not very efficient for large fields.

Ideally, one should be able to deduce all these quantities simply and directly from a defining curve and the order of the base field, without any advanced computations. This is certainly the case for elliptic and hyperelliptic curves, *i.e.,* quadratic function fields, but is too much to ask in general. Partial answers in this regard were given for purely cubic function fields in [20, 23], general cubic extensions in [21], and biquadratic function fields in [36].

This paper continues the work of [21] and provides an explicit treatment of cubic function fields of characteristic at least 5. We provide a fast technique for converting the minimal polynomial of such a field to standard form, formulae for the field discriminant and the genus, a simple characterization for non-singularity of the underlying curve, and an efficient algorithm for finding all triangular integral bases of the extension. The only algorithmic ingredient beyond simple arithmetic that is required for any of these results is the square-free factorization of a few polynomials. Our main contribution is a simple description of the signature of any rational place in the function field extension, thereby extending the work done for the place at infinity in [21]. For the finite places, our signature result is new. As desired, the signature can easily be obtained just from the defining curve and the order of the base field; in certain cases, it may be necessary to perform square or cube root computations modulo a prime polynomial.

One of the main applications of this work is the class number algorithm for cubic function fields given in [24], which has since been extended to arbitrary function fields [22]. This algorithm requires the computation of the signature of a very large number of places, so a method for doing this efficiently is of key importance. We give a brief overview of this class number algorithm, how signature generation fits into its context, and how it relates to heuristics on zeros of zeta functions.

We begin with a general overview of algebraic function fields in Section 2 and their signatures in Section 3. The standard form of a cubic function field is explained in Section 4. Section 5 provides a formula for the discriminant and a simple characterization of non-singularity, and Section 6 gives a straightforward description of all triangular integral bases. An easy method for determining the signature of every rational place is presented in Sections 7 and 8. The applications to class numbers and zeros of zeta functions referred to above are illustrated in Sections 9 and 10, respectively. We conclude with a survey of open problems in Section 11.

2 Overview of Algebraic Function Fields

For a general introduction to algebraic function fields, we refer the reader to [8, 19, 30]. Much of the material on cubic function fields is taken from [21]. Let $\mathbb{F}_q$ be a finite field, set $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$, and let $\overline{\mathbb{F}}_q$ be some algebraic closure of $\mathbb{F}_q$. Denote by $\mathbb{F}_q[x]$ and $\mathbb{F}_q(x)$ the ring of polynomials and the field of rational functions in x over $\mathbb{F}_q$, respectively. For any non-zero $G \in \mathbb{F}_q[x]$, we denote by $\deg(G)$ the degree, and by $\operatorname{sgn}(G)$ the leading coefficient of G.

A(n) (*algebraic*) *function field* is a finite extension K of $\mathbb{F}_q(x)$; its *degree* is the field extension degree $n = [K:\mathbb{F}_q(x)]$. It is always possible to write a function field as $K = \mathbb{F}_q(x, y)$ where $F(x, y) = 0$ and $F(Y)$ is a monic polynomial of degree n with coefficients in $\mathbb{F}_q[x]$ that is irreducible over $\mathbb{F}_q(x)$. Note that we do not require the curve $F(x, y) = 0$ to be nonsingular[1], *i.e.,* there may exist points on the curve such that the partial derivatives of F with respect to x and Y vanish at those points. We will always assume that $\gcd(q, n) = 1$, so that $K/\mathbb{F}_q(x)$ is *separable*, *i.e.,* $F(Y)$ has no multiple roots. Furthermore, we assume that $\mathbb{F}_q$ is the *full constant field* of K, *i.e.,* $\mathbb{F}_q$ is algebraically closed in K.

The powers y^i, $0 \le i \le n-1$, form an $\mathbb{F}_q(x)$-basis of the $\mathbb{F}_q(x)$-vector space K. An $\mathbb{F}_q(x)$-basis $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ is *triangular* if α_i is an $\mathbb{F}_q(x)$-linear combination of $1, y, \ldots, y^i$ for $0 \le i \le n-1$. The *n conjugate mappings* map y to the n (distinct) roots $y = y^{(0)}, y^{(1)}, \ldots, y^{(n-1)}$ of $F(Y)$. Extending these mappings $\mathbb{F}_q(x)$-linearly to K now defines for every $\alpha \in K$ its *n conjugates* $\alpha = \alpha^{(0)}, \alpha^{(1)}, \ldots, \alpha^{(n-1)}$.

The *discriminant* of n elements $\alpha_0, \alpha_1, \ldots \alpha_{n-1} \in K$ is

$$\operatorname{disc}(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) = \det(\alpha_i^{(j)})_{0 \le i,j \le n-1}^2 \in \mathbb{F}_q(x).$$

If $\alpha_i = \alpha^i$ for some non-zero $\alpha \in K$ and $0 \le i \le n-1$, then $\operatorname{disc}(\alpha) = \operatorname{disc}(1, \alpha, \ldots, \alpha^{n-1})$ is simply called the discriminant of α, and

$$\operatorname{disc}(\alpha) = \prod_{i<j} (\alpha^{(i)} - \alpha^{(j)})^2.$$

We have $\operatorname{disc}(y) = \operatorname{disc}(F)$, the discriminant of F as a polynomial in Y.

The *maximal order* or *coordinate ring* $\mathcal{O}_K$ of $K/\mathbb{F}_q(x)$ is the integral closure of $\mathbb{F}_q[x]$ in K. It is a free $\mathbb{F}_q[x]$-module of rank n, and an $\mathbb{F}_q[x]$-basis of $\mathcal{O}_K$ is an *integral basis* of $K/\mathbb{F}_q(x)$. There always exists a triangular integral basis, and since $1 \in \mathcal{O}_K$, one of the triangular basis elements must be a constant in $\mathbb{F}_q^*$. The *discriminant*[2] of $K/\mathbb{F}_q(x)$ is $\operatorname{disc}(K) = \operatorname{disc}(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ where $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ is any integral basis of $K/\mathbb{F}_q(x)$. The polynomial $\operatorname{disc}(K) \in \mathbb{F}_q[x]$ is independent of the basis chosen and unique up to square factors in $\mathbb{F}_q^*$. For every non-zero element $\alpha \in K$, the *index* of α, denoted by $\operatorname{ind}(\alpha)$ and unique up to square factors, is the rational function in $\mathbb{F}_q(x)$ satisfying $\operatorname{disc}(\alpha) = \operatorname{ind}(\alpha)^2 \operatorname{disc}(K)$. If $\alpha \in \mathcal{O}_K$, then $\operatorname{ind}(\alpha) \in \mathbb{F}_q[x]$, so $\operatorname{disc}(\alpha) \in \mathbb{F}_q[x]$.

[1] Throughout the paper, singularity will always refer to the affine part of a curve, *i.e.,* the curve may be singular at infinity.

[2] By abuse of language, we speak of *the* discriminant of $\mathcal{O}_K$ and *the* index of an element in $\mathcal{O}_K$, keeping in mind that these notions are only unique up to a square factor in $\mathbb{F}_q^*$. They can be made unique by requiring the index to be monic.

It is obvious that $\mathrm{ind}(y) \in \mathbb{F}_q^*$, *i.e.,* $\mathrm{disc}(y) = \mathrm{disc}(K)$ up to constant square factors, if and only if the powers y^i, $0 \le i \le n-1$, form an integral basis of $K/\mathbb{F}_q(x)$, *i.e.,* if and only if $\mathcal{O}_K = \mathbb{F}_q[x][y] = \mathbb{F}_q[x,Y]/(F(Y))$ where $(F(Y))$ is the principal ideal generated by $F(Y)$ in $\mathbb{F}_q[x,Y]$. By [17, Corollary 9.10], this is the case if and only if the curve $F(x,y) = 0$ is non-singular[3].

A *common inessential discriminant divisor* of $K/\mathbb{F}_q(x)$ is a monic irreducible polynomial of $\mathbb{F}_q(x)$ that divides $\mathrm{ind}(\alpha)$ for every non-zero $\alpha \in \mathcal{O}_K$. If $F(x,y) = 0$ is non-singular, then $K/\mathbb{F}_q(x)$ obviously has no such divisors. In an algebraic number field of degree n over the rationals, every common inessential discriminant divisor (that is, every prime dividing every index) must be strictly less than n [32]. The function field analogue states that for every common inessential discriminant divisor P of $K/\mathbb{F}_q(x)$, $|P| = q^{\deg(P)} < n$, so $\deg(P) < \log_q(n)$. It follows that function field extensions of degree $n \le q$ over $\mathbb{F}_q(x)$ have no common inessential discriminant divisors.

3 Signature and Genus of an Algebraic Function Field

The places of $\mathbb{F}_q(x)$ consist of the *finite* places, identified with the monic irreducible polynomials in $\mathbb{F}_q[x]$, and the *place at infinity* P_∞, identified with the rational function $1/x$. If P is any place of $\mathbb{F}_q(x)$, let ν_P denote its associated discrete valuation on $\mathbb{F}_q(x)$ and $\mathcal{O}_P = \{G \in \mathbb{F}_q(x) \mid \nu_P(G) \ge 0\}$ the discrete valuation ring of P. In particular, for any non-zero polynomial $G \in \mathbb{F}_q[x]$, $\nu_P(G)$ is the exact power of P dividing G if P is a finite place, and $\nu_{P_\infty}(G) = -\deg(G)$.

For any place P of $\mathbb{F}_q(x)$, the *degree* $\deg(P)$ is the degree of the polynomial P if P is finite, and $\deg(P_\infty)$ is set to be 1. The completion of $\mathbb{F}_q(x)$ with respect to any place P is the field of *Laurent series* $\mathbb{F}_{q^d}\langle P\rangle$ in P over $\mathbb{F}_{q^d}$, where $d = \deg(P)$. Non-zero elements in this field have the form $\sum_{i \ge m} a_i P^i$ where $m \in \mathbb{Z}$, $a_i \in \mathbb{F}_{q^d}$ for $i \ge m$, and $a_m \ne 0$. The valuation ν_P on $\mathbb{F}_q(x)$ extends uniquely to $\mathbb{F}_{q^d}\langle P\rangle$ via $\nu_P(\alpha) = m$. For $P = P_\infty$, we have $\mathbb{F}_{q^d}\langle P\rangle = \mathbb{F}_q\langle x^{-1}\rangle$, and we write $\deg(\alpha) = -\nu_{P_\infty}(\alpha)$ for $\alpha \in \mathbb{F}_q\langle x^{-1}\rangle$.

The places of K consist of the finite places, *i.e.,* the non-zero prime ideals in $\mathcal{O}_K$, and the infinite places, *i.e.,* the non-zero prime ideals in the integral closure of $\mathcal{O}_{P_\infty}$ in K. Fix any place $\mathfrak{p}$ of K and let $\nu_\mathfrak{p}$ be its associated discrete valuation on K. Then $\mathcal{O}_\mathfrak{p} = \{\alpha \in K \mid \nu_\mathfrak{p}(\alpha) \ge 0\}$ is the discrete valuation ring of $\mathfrak{p}$. There exists a unique place P of $\mathbb{F}_q(x)$ with $\nu_\mathfrak{p}(P) > 0$; we say that $\mathfrak{p}$ *lies above* P and write $\mathfrak{p} \mid P$. The positive integer $e(\mathfrak{p}|P) = \nu_\mathfrak{p}(P)$ is the *ramification index* of $\mathfrak{p}$. The place P is said to be *ramified* if $e(\mathfrak{p}|P) > 1$ for some $\mathfrak{p} \mid P$ and *unramified* otherwise. It is well known that a finite place P of $\mathbb{F}_q(x)$ is ramified if and only if $P \mid \mathrm{disc}(K)$. If P is finite and (P) is the principal ideal generated by P in $\mathcal{O}_P$, then the field extension degree $f(\mathfrak{p}|P) = [\mathcal{O}_\mathfrak{p}/\mathfrak{p} : \mathcal{O}_P/(P)]$ is the *residue degree* of $\mathfrak{p}$. The residue degree of the infinite place P_∞ is $f(\mathfrak{p}|P_\infty) = [\mathcal{O}_\mathfrak{p}/\mathfrak{p} : \mathbb{F}_q]$.

A ramified place P of $\mathbb{F}_q(x)$ is *tamely* ramified if $\gcd(e(\mathfrak{p}|P), q) = 1$ for all places $\mathfrak{p}$ of K lying above P. Henceforth, we assume that $K/\mathbb{F}_q(x)$ is a tamely ramified ex-

[3] In [17], this corollary is stated over an algebraically closed base field. However, an analogous result holds when the base field is not algebraically closed, as is the case here.

tension, *i.e.,* all places of $\mathbb{F}_q(x)$ are tamely ramified in K. If the characteristic of $\mathbb{F}_q$ exceeds the extension degree $n = [K:\mathbb{F}_q(x)]$, then $K/\mathbb{F}_q(x)$ is tamely ramified.

Every place P of $\mathbb{F}_q(x)$ has a unique factorization $(P) = \prod_{\mathfrak{p}|P} \mathfrak{p}^{e(\mathfrak{p}|P)}$ into the places of K lying above P; here $\sum_{\mathfrak{p}|P} e(\mathfrak{p}|P) f(\mathfrak{p}|P) = n$. The tuple of pairs $(e(\mathfrak{p}|P), f(\mathfrak{p}|P))$ with $\mathfrak{p}|P$, usually sorted in lexicographical order, is the *P-signature* of $K/\mathbb{F}_q(x)$. In most, but not all cases, it is possible to completely determine the P-signature from the prime factorization of the minimal polynomial $F(Y)$ of $K/\mathbb{F}_q(x)$ in $\mathcal{O}_P/(P)$ as described in [30, Theorem III.3.7]. Alternatively, it may be possible to find the P-signature of $K/\mathbb{F}_q(x)$ by considering the roots of $F(Y)$.

Theorem 3.1 *Let $K = \mathbb{F}_q(x, y)$ be an algebraic function field, where $F(x, y) = 0$ and $F(Y) \in \mathbb{F}_q[x][Y]$ is a monic polynomial that is irreducible over $\mathbb{F}_q(x)$. Let P be any place of $\mathbb{F}_q(x)$, $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ the places of K lying above P, and write $e_i = e(\mathfrak{p}_i|P)$, $f_i = f(\mathfrak{p}_i|P)$, and $n_i = e_i f_i$ for $1 \le i \le r$. Then there exists an enumeration of the roots $y^{(0)}, y^{(1)}, \ldots, y^{(n-1)}$ of $F(Y)$ as*

$$(y^{(0)}, y^{(1)}, \ldots, y^{(n-1)}) = (y_{1,1}, \ldots, y_{1,n_1}, y_{2,1}, \ldots, y_{2,n_2}, \ldots, y_{r,1}, \ldots, y_{r,n_r})$$

so that $y_{i,j}$ lies in an extension E of $\overline{\mathbb{F}}_q\langle P\rangle$ of degree e_i, but in no proper subfield of E, for $1 \le j \le n_i$ and $1 \le i \le r$. If $e_i = 1$ for some $i \in \{1, 2, \ldots, r\}$, then $y_{i,j} \in \mathbb{F}\langle P\rangle$ for $1 \le j \le n_i$, where $\mathbb{F}$ is an extension of degree at most f_i of $\mathbb{F}_{q^{\deg(P)}}$.

Finally, set

$$\epsilon_P(K) = \sum_{\mathfrak{p}|P} (e(\mathfrak{p}|P) - 1) f(\mathfrak{p}|P) = n - \sum_{\mathfrak{p}|P} f(\mathfrak{p}|P) \tag{3.1}$$

for any place P of $\mathbb{F}_q(x)$. Note that $\epsilon_P(K) \le n - 1$. We have $\nu_P(\mathrm{disc}(K)) = \epsilon_P(K)$ for all finite places P of $\mathbb{F}_q(x)$. By the Hurwitz genus formula (see [30, Theorem II.4.12]), the *genus* of K is

$$g = \frac{1}{2} \sum_P \deg(P) \epsilon_P(K) - n + 1 = \frac{1}{2} (\deg(\mathrm{disc}(K)) + \epsilon_{P_\infty}(K)) - n + 1, \tag{3.2}$$

where the sum in (3.2) runs over all places of $\mathbb{F}_q(x)$.

4 Standard Form of a Cubic Function Field

A *cubic function field* is a separable algebraic function field $K = \mathbb{F}_q(x, y)$ of degree 3 over $\mathbb{F}_q(x)$, where for our purposes, we assume that the characteristic of $\mathbb{F}_q$ is at least 5. Note that $K/\mathbb{F}_q(x)$ is tamely ramified. By applying a suitable translation by a polynomial in $\mathbb{F}_q[x]$ to y, it is always possible to write a cubic function field as $K = \mathbb{F}_q(x, y)$, where $F(x, y) = 0$ and $F(Y) = Y^3 - AY + B \in \mathbb{F}_q[x][Y]$ is irreducible over $\mathbb{F}_q(x)$. Note that this transformation maps singular points to singular points, leaving their multiplicities unchanged. Moreover, it preserves $\mathrm{ind}(y)$ as well as the P-signature in $K/\mathbb{F}_q(x)$ of every place P of $\mathbb{F}_q(x)$.

Since $\mathbb{F}_q$ is assumed to be the full constant field of K, at least one of A, B is non-constant. A cubic function field is said to be *purely cubic* if it is a radical extension, that is, it can be written as $K = \mathbb{F}_q(x, y)$ with $y^3 \in \mathbb{F}_q[x] \setminus \mathbb{F}_q$ (this corresponds to the case $A = 0$). The discriminant of F is

$$D = 4A^3 - 27B^2 = I^2\Delta \quad \text{with } I = \operatorname{ind}(y) \text{ and } \Delta = \operatorname{disc}(K). \tag{4.1}$$

Furthermore, we may assume that F is in *standard form*, *i.e.,* there is no non-constant polynomial $Q \in \mathbb{F}_q[x]$ with $Q^2 \mid A$ and $Q^3 \mid B$. Note that conversion to standard form eliminates some, but not necessarily all, singular points from the curve $F(x, y) = 0$. The following algorithm is the cubic analogue to [36, Algorithm 3.1] and efficiently converts a cubic function field to an $\mathbb{F}_q(x)$-isomorphic one in standard form. Here, we recall that the *square-free factorization* of a polynomial $G \in \mathbb{F}_q[x]$ is the unique factorization of G of the form $G = \operatorname{sgn}(G) \prod_i G_i^i$, where all the $G_i \in \mathbb{F}_q[x]$ are monic, square-free, and pairwise coprime. The square-free factorization of G can be found using at worst $O(\deg(G)^2 \max\{\deg(G), \log(q)\})$ operations in $\mathbb{F}_q$ (see [6, Algorithm 3.4.2]); this asymptotic complexity can be considerably improved in many cases.

***Algorithm 4.1* (Standard Form)**

Input $A, B \in \mathbb{F}_q[x]$ *where* $F(Y) = Y^3 - AY + B$ *is irreducible over* $\mathbb{F}_q(x)$.
Output $A_0, B_0 \in \mathbb{F}_q[x]$ *so that the polynomial* $F_0(Y) = Y^3 - A_0Y + B_0$ *is in standard form and the two cubic function fields defined by* $F(Y)$ *and* $F_0(Y)$ *are* $\mathbb{F}_q(x)$*-isomorphic.*
Algorithm

(i) *Compute the square-free factorizations of* A *and* B*, say* $A = \operatorname{sgn}(A) \prod_i A_i^i$, $B = \operatorname{sgn}(B) \prod_j B_j^j$.
(ii) *Compute* $G = \prod_i A_i^{\lfloor i/2 \rfloor}$ *and* $H = \prod_j B_j^{\lfloor j/3 \rfloor}$. *Set* $Q = \gcd(G, H)$, $A_0 = A/Q^2$, $B_0 = B/Q^3$. *Output* A_0, B_0.

For the remainder of this paper, we assume that $K = \mathbb{F}_q(x, y)$ is a cubic function field given by an irreducible equation

$$F(y) = y^3 - Ay + B = 0 \quad (A, B \in \mathbb{F}_q[x]) \tag{4.2}$$

in standard form.

5 Field Discriminant and Non-Singularity

We begin by computing the field discriminant $\Delta = \operatorname{disc}(K)$ from the polynomial discriminant $D = \operatorname{disc}(y)$. According to [21, Lemma 2.3], we have the following.

Lemma 5.1 *Let* $K = \mathbb{F}_q(x, y)$ *be a cubic function field in standard form given by* (4.2). *Let* $\Delta = \operatorname{disc}(K)$ *and* D *be given by* (4.1). *Then for any finite place* P *of* $\mathbb{F}_q(x)$,

(i) $v_P(\Delta) = 2$ *if and only if* $v_P(A) \geq v_P(B) \geq 1$;
(ii) $v_P(\Delta) = 1$ *if and only if* $v_P(D)$ *is odd;*

(iii) $v_P(\Delta) = 0$ *otherwise,* i.e., *if and only if* $v_P(D)$ *is even and*[4] $v_P(A)v_P(B) = 0$.

Note that the characterization of the "otherwise" case is correct, since it requires $v_P(D)$ even and $v_P(B) = 0$ or $v_P(A) < v_P(B)$. But $1 = v_P(A) < v_P(B)$ implies $v_P(D)$ odd and $2 \leq v_P(A) < v_P(B)$ violates our standard form assumption. So $v_P(D)$ is even and $v_P(A) < v_P(B)$ forces $v_P(A) = 0$.

Corollary 5.2 *Let* $K = \mathbb{F}_q(x, y)$ *be a cubic function field in standard form given by* (4.2). *Let* $\Delta = \operatorname{disc}(K)$ *and* D *be given by* (4.1). *If* $D = \operatorname{sgn}(D) \prod_i D_i^i$ *is the square-free factorization of* D, *then up to square factors in* $\mathbb{F}_q^*$

$$\Delta = \operatorname{sgn}(D) G \cdot \gcd(D_2 D_4, B)^2 \quad \textit{with } G = \prod_{i \text{ odd}} D_i.$$

Proof We have $v_P(\Delta) \leq 2$ for all finite places P of $\mathbb{F}_q(x)$. So let $\Delta = \operatorname{sgn}(\Delta)\Delta_1\Delta_2^2$ be the square-free factorization of Δ. By normalizing so that $\operatorname{ind}(y)$ is monic, we see that $\operatorname{sgn}(\Delta) = \operatorname{sgn}(D)$. We need to show that $\Delta_1 = G$ and $\Delta_2 = \gcd(D_2D_4, B)$. To that end, let P be any finite place of K. Then $P \mid \Delta_1$ if and only if $v_P(\Delta) = 1$, which by Lemma 5.1 holds if and only if $v_P(D)$ is odd. This in turn is the case if and only if there exists an odd index $i \in \mathbb{N}$ with $P \mid D_i$, and since all D_i are square-free and pairwise coprime, this holds if and only if $v_P(G) = 1$.

We next observe that $\gcd(D_2D_4, B)$ is square-free and coprime to G, since all the D_i are square-free and pairwise coprime. Hence $v_P(G \cdot \gcd(D_2D_4, B)^2) \leq 2$ for all finite places P of $\mathbb{F}_q(x)$. So by Lemma 5.1, it suffices to show that a finite place P divides $\gcd(D_2D_4, B)$ if and only if $v_P(A) \geq v_P(B) \geq 1$.

Suppose first that $P \mid \gcd(D_2D_4, B)$. Then $v_P(D) = 2$ or 4. Also, since $P \mid D$ and $P \mid B$, we see that $P \mid A$. If $v_P(D) = 2$, then the strict triangle inequality for degrees applied to (4.1) implies $v_P(B) = 1$, and if $v_P(D) = 4$, then similar reasoning forces $v_P(B) = 2$ and $v_P(A) \geq 2$. In either case $v_P(A) \geq v_P(B) \geq 1$. Conversely, suppose that $v_P(A) \geq v_P(B) \geq 1$. Then $v_P(D) = 2v_P(B)$. By our standard form assumption $v_P(B) = 1$ or 2. If $v_P(B) = 1$, then $v_P(D) = 2$, so $P \mid D_2$, and if $v_P(B) = 2$, then $P \mid D_4$. In either case, $P \mid \gcd(D_2D_4, B)$. This concludes the proof. ∎

We can now characterize non-singularity of (4.2) as follows (this is a corrected version of [21, Corollary 2.2]). We denote by D' and D'' the first and second derivative of D with respect to x, respectively.

Lemma 5.3 *Let* $K = \mathbb{F}_q(x, y)$ *be a cubic function field in standard form given by* (4.2) *and* D *given by* (4.1). *Set* $H = \gcd(D, D')$. *Then the curve* $F(x, y) = 0$ *is non-singular if and only if any one of the following equivalent properties holds:*

(i) $\gcd(H, D'') = 1$ *and* $H \mid B$;
(ii) $\gcd(H, D'') = 1$ *and* $H = \gcd(D, B)$;
(iii) *the square-free factorization of* D *is* $D = \operatorname{sgn}(D)D_1D_2^2$ *and* $D_2 \mid B$.

Proof We first show that the above three properties are equivalent. We have $\gcd(H, D'') = 1$ if and only if D has no cube factors, which holds if and only if

[4] [21, Lemma 2.3] incorrectly stated $v_P(A) = v_P(B) = 0$ here.

the square-free factorization of D is $D = \operatorname{sgn}(D)D_1D_2^2$. In this case, $H = D_2$, so parts (i) and (iii) above are equivalent. To prove that (i) and (ii) are equivalent, suppose that $D = \operatorname{sgn}(D)D_1D_2^2$ is cube-free and set $G = \gcd(D, B)$. Then $G \mid A$ and hence $G^2 \mid D$, implying $G \mid D_2 = H$. Now $H \mid B$ if and only if $H \mid \gcd(D, B) = G$, which in turn holds if and only if $H = G$.

Next, we prove that non-singularity is equivalent to property (iii) above. We recall that the curve (4.2) is non-singular if and only if $D = \Delta$ up to square factors in $\mathbb{F}_q^*$. If this holds, then since Δ is cube-free, the square-free factorization of D is $D = \operatorname{sgn}(D)\, D_1D_2^2$. In addition, Corollary 5.2 implies $D_2 = \gcd(D_2, B)$, so $D_2 \mid B$. Conversely, if $D = \operatorname{sgn}(D)D_1D_2^2$ with $D_2 \mid B$, then by Corollary 5.2, $\Delta = \operatorname{sgn}(D)D_1 \cdot \gcd(D_2, B)^2 = \operatorname{sgn}(D)D_1D_2^2 = D$. ∎

6 Triangular Integral Bases and Some Index Computations

For cubic number fields, the computation of the field discriminant and integral bases goes back to [1]. Here, we characterize all triangular integral bases of a cubic function field extension $K/\mathbb{F}_q(x)$ given in standard form (4.2) with D, Δ, and I given by (4.1). The index I can be determined from (4.1) using Corollary 5.2. Once I and Δ are known, it is possible to efficiently compute any triangular integral basis of $K/\mathbb{F}_q(x)$.

All triangular integral bases of $K/\mathbb{F}_q(x)$ are essentially determined by a solution $T \in \mathbb{F}_q[x]$ of the higher order congruence pair

$$\begin{aligned} 3T^2 - A &\equiv 0 \pmod{I}, \\ T^3 - AT + B &\equiv 0 \pmod{I^2}. \end{aligned} \tag{6.1}$$

The key idea will be to reduce (6.1) to an equivalent pair of linear congruences, namely (6.2) below, so that the problem of finding all integral triangular bases reduces to a simple application of the Chinese Remainder Theorem.

Lemma 6.1 *Let $K = \mathbb{F}_q(x, y)$ be a cubic function field in standard form given by* (4.2). *Let $\Delta = \operatorname{disc}(K)$, D and I as specified in* (4.1), *and P any finite place of $\mathbb{F}_q(x)$. If $P \mid \gcd(I, A)$, then $v_P(B) \geq 2$ and $v_P(I) = 1 \leq v_P(\Delta)$, so $v_P(D) = 3$ or 4.*

Proof Assume $P \mid \gcd(I, A)$. Then $P \mid D$, so $P \mid B$. Assume by way of contradiction that $v_P(B) = 1$. Then $v_P(D) = 2v_P(B) = 2$. Now $P \mid A$ implies $v_P(A) \geq v_P(B) = 1$, so Lemma 5.1 yields $v_P(\Delta) = 2$. But then $2 = v_P(D) = 2v_P(I) + v_P(\Delta) \geq 4$, a contradiction. So $v_P(B) \geq 2$.

If $v_P(A) = 1$, then $v_P(D) = 3$, so $v_P(I) = v_P(\Delta) = 1$. If $v_P(A) \geq 2$, then the standard form assumption forces $v_P(B) = 2$, so $v_P(A) \geq v_P(B) \geq 1$. By Lemma 5.1, $v_P(\Delta) = 2$. Also, $v_P(D) = 2v_P(B) = 4$, so $v_P(I) = 1$. ∎

Corollary 6.2 *Let $K = \mathbb{F}_q(x, y)$ be a cubic function field in standard form given by* (4.2), *with D and I given by* (4.1). *Set $G = \gcd(I, A)$. Then the following hold:*

(i) *G is square-free;*
(ii) *$G^3 \mid D$;*
(iii) *I/G is coprime to A, and hence to G.*

Proof Let P be any finite place of $\mathbb{F}_q(x)$. If $P \mid G$, then $1 \leq v_P(G) \leq v_P(I) = 1$, where the last equality follows from Lemma 6.1. Hence $v_P(G) = 1$, so G is square-free. By the same lemma, $v_P(D) \geq 3$, so since G is square-free, $G^3 \mid D$.

By way of contradiction, suppose that P divides both I/G and A. Then $P \mid I$ and $P \mid A$, hence $P \mid G$. As in the previous paragraph, we infer that $v_P(G) = 1$. But this contradicts $P \mid I/G$. It follows that I/G is coprime to A. Since G divides A, I/G must also be coprime to G. ■

Part (iii) of the above corollary implies that there exists $T \in \mathbb{F}_q[x]$ such that

$$T \equiv \begin{cases} 3B/2A & (\mathrm{mod}\ I/\gcd(I,A)), \\ 0 & (\mathrm{mod}\ \gcd(I,A)), \end{cases} \tag{6.2}$$

and T is unique modulo I. We will see that any solution to (6.2) is in fact a solution of (6.1) and vice versa.

Lemma 6.3 *Let $T \in \mathbb{F}_q[x]$. Then T satisfies* (6.2) *if and only if T satisfies* (6.1).

Proof For brevity, we again set $G = \gcd(I, A)$. Suppose T satisfies (6.2). By part (iii) of Corollary 6.2, it suffices to prove the first congruence of (6.1) modulo both G and I/G, and the second congruence of (6.1) modulo both G^2 and $(I/G)^2$.

Clearly, the second congruence of (6.2) implies $3T^2 - A \equiv 0 \pmod{G}$. Part (ii) of Corollary 6.2 implies $G^3 \mid B^2$, so $G^2 \mid B$ by part (i) of the same corollary. Thus, $T^3 - AT + B \equiv 0 \pmod{G^2}$.

Now $2AT \equiv 3B \pmod{I/G}$ implies $(2A)^2(3T^2 - A) \equiv -D \equiv 0 \pmod{I/G}$. Writing $2AT = 3B + UI/G$ for suitable $U \in \mathbb{F}_q[x]$, it is also easy to verify that $(2A)^3(T^3 - AT + B) \equiv -D(B + UI/G) \equiv 0 \pmod{I^2/G^2}$. The desired result now follows from part (iii) of Corollary 6.2.

Conversely, suppose T satisfies (6.1). Then the first congruence of (6.1) implies $3T^2 \equiv 0 \pmod{G}$. Since G is square-free by part (i) of Corollary 6.2, we see that $T \equiv 0 \pmod{G}$. Furthermore, $3B \equiv T(3A - 3T^2) \equiv 2TA \pmod{I}$. Again invoking part (iii) of Corollary 6.2, we obtain $T \equiv 3B/2A \pmod{I/G}$. ■

Theorem 6.4 *Let $K = \mathbb{F}_q(x, y)$ be a cubic function field in standard form given by* (4.2)*, with I given by* (4.1)*. Then a triangular basis of $K/\mathbb{F}_q(x)$ is an integral basis if and only if up to order and constant factors of basis elements, it is of the form $\{1, \alpha, \beta\}$ where $\alpha = y + U$, $\beta = (y^2 + Ty + V)/I\}$ with $T, U, V \in \mathbb{F}_q[x]$, T is a solution of* (6.2)*, and $V \equiv -2T^2 \equiv -2A/3 \pmod{I}$.*

Proof By Lemma 6.3, we may replace (6.2) in the statement of the theorem by (6.1). By [21, Corollary 3.2], the set $\{1, \rho, \omega\}$, with $\rho = \alpha - (U + T)$ and $\omega = \beta + (T^2 - A - V)/I$, is an integral basis of $K/\mathbb{F}_q(x)$. Since $V \equiv T^2 - A \pmod{I}$ by (6.1), $\{1, \alpha, \beta\}$ is also an integral basis of $K/\mathbb{F}_q(x)$, and every integral basis has the desired form. ■

We point out that if T is given as in (6.1), or equivalently, (6.2), then the factorization of $F(Y)$ modulo I is easily seen to be $F(Y) \equiv (Y - T)^2(Y + 2T) \pmod{I}$.

We conclude this section with a note on common inessential discriminant divisors. In a cubic number field, the only possible common inessential discriminant

divisor is the prime 2 (see [7, p. 120], and there exist fields where this occurs. The first such example was given by Dedekind and is the cubic number field with minimal polynomial $F(Y) = Y^3 - Y^2 - 2Y - 8$. Furthermore, there exist cubic number fields that have no common inessential discriminant divisors, but still do not have an integral basis of the form $\{1, y, y^2\}$; for details, see [8, pp. 457–462]. We also refer to the treatment of index divisors of cubic number fields in [31]; interestingly, the author normalizes the minimal polynomial of the cubic extension so that the Y term, rather than the Y^2 term, vanishes.

We saw earlier that by the function field analogue of [32], a cubic function field of characteristic at least 5 cannot have common inessential discriminant divisors. However, this result can also be proved in an elementary way by computing some simple indices $\text{ind}(\alpha)$ for certain $\alpha \in \mathcal{O}_K$ as follows.

Lemma 6.5 *Let T be defined as in* (6.1)*, and write $3T^2 - A = EI$, $T^3 - AT + B = CI^2$ with $E, C \in \mathbb{F}_q[x]$. Let α, β be given as in Theorem* 6.4*, and for any $S \in \mathbb{F}_q[x]$, set $\beta_S = \beta + S\alpha$. Then $\text{ind}(\alpha) = I$ and $\text{ind}(\beta_S) = C_S$, where $C_S = C + S(E + 3TS + IS^2)$. Furthermore,* $\gcd(I, C_0, C_1, C_2) = 1$.

Proof Let $y^{(0)} = y, y^{(1)}, y^{(2)}$ denote the roots of $F(Y)$, where $F(Y)$ is given by (4.2). Since $\alpha^{(i)} - \alpha^{(j)} = y^{(i)} - y^{(j)}$ for $0 \le i, j \le 2$, we see that $\text{disc}(\alpha) = \text{disc}(y)$, so $\text{ind}(\alpha) = \text{ind}(y) = I$. Now note that

$$\beta_S^{(i)} - \beta_S^{(j)} = \frac{1}{I}(y^{(i)} - y^{(j)})(y^{(i)} + y^{(j)} + T + IS) = \frac{1}{I}(y^{(i)} - y^{(j)})(T + IS - y^{(k)})$$

for $\{i, j, k\} = \{0, 1, 2\}$, and

$$(T + IS - y^{(i)})(T + IS - y^{(j)})(T + IS - y^{(k)}) = F(T + IS).$$

So

$$\begin{aligned}\text{disc}(\beta) &= \left((\beta^{(0)} - \beta^{(1)})(\beta^{(1)} - \beta^{(2)})(\beta^{(2)} - \beta^{(0)})\right)^2 \\ &= \frac{F(T + IS)^2 \ \text{disc}(y)}{I^6} = \left(\frac{F(T + IS)}{I^2}\right)^2 \Delta,\end{aligned}$$

yielding $\text{ind}(\beta_S) = F(T + IS)/I^2$. By Taylor expansion,

$$\begin{aligned}F(T + IS) &= F(T) + F'(T)IS + \frac{F''(T)}{2}(IS)^2 + \frac{F'''(T)}{6}(IS)^3 \\ &= CI^2 + EI^2S + 3TI^2S^2 + I^3S^3,\end{aligned}$$

implying that $\text{ind}(\beta_S) = C + S(E + 3TS + IS^2) = C_S$.

To prove that $\gcd(I, C_0, C_1, C_2) = 1$, let Q be any divisor of I, C_0, C_1, C_2. Then Q divides both $C_1 - C_0 - I = E + 3T$ and $(C_2 - C_0)/2 - 4I = E + 6T$. It follows that $Q \mid T$ and $Q \mid E$. Then $Q^2 \mid 3T^3 - EI = A$ and $Q^3 \mid CI^2 - T^3 + AT = B$. By our standard form assumption $Q \in \mathbb{F}_q^*$, proving our claim. ■

Corollary 6.6 *A cubic function field of characteristic at least* 5 *has no common inessential discriminant divisors.*

7 Signatures of Cubic Function Fields: Preliminaries

Before we can compute P-signatures, we require a simple lemma, which is a generalization of [21, Lemma 4.1] (with a minor error corrected).

Lemma 7.1 *Let P be any place of $\mathbb{F}_q(x)$ of degree d, p a rational prime not dividing q, and $\alpha = \sum_{i\geq m} a_i P^i \in \mathbb{F}_{q^d}\langle P\rangle$ with $a_m \neq 0$. Then the following hold.*

- *α has a p-th root in $\mathbb{F}_{q^d}\langle P\rangle$ if $p \mid m$ and a_m has a p-th root in $\mathbb{F}_{q^d}$.*
- *α has a p-th root in $\mathbb{F}_{q^d}(b)\langle P\rangle \setminus \mathbb{F}_{q^d}\langle P\rangle$, where $b \in \overline{\mathbb{F}}_q \setminus \mathbb{F}_{q^d}$ is any p-th root of a_m, if $p \mid m$ and a_m does not have any p-th roots in $\mathbb{F}_{q^d}$.*
- *All the p-th roots of α lie in a degree p extension of $\overline{\mathbb{F}}_q\langle P\rangle$, but not in $\overline{\mathbb{F}}_q\langle P\rangle$ itself, if $p \nmid m$.*

Proof Let $\beta = \sum_{i\geq n} b_i P^i \in \overline{\mathbb{F}}_q\langle P\rangle$ with $b_n \neq 0$. Then $\beta^p = \sum_{i\geq pn} c_i P^i$ where $c_{pn} = b_n^p$ and for $i \in \mathbb{N}$, $c_{pn+i} = p b_n^{p-1} b_{n+i} + g_i$, with g_i a homogeneous polynomial of degree p in $b_n, b_{n+1}, \ldots, b_{n+i-1}$ with coefficients in $\mathbb{F}_q$. In particular, if $\beta^p \in \mathbb{F}_{q^d}\langle P\rangle$, *i.e.*, $c_i \in \mathbb{F}_{q^d}$ for $i \geq pn$, then inductively $b_i \in \mathbb{F}_{q^d}(b_n)$ for $i \geq n$.

Now let $\alpha = \sum_{i\geq m} a_i P^i \in \mathbb{F}_{q^d}\langle P\rangle$ with $a_m \neq 0$, and write $m = pn + r$ with $0 \leq r < p$. Then $\gamma = a_m^{-1}\alpha P^{-r} = \sum_{i\geq pn} c_i P^i \in \mathbb{F}_{q^d}\langle P\rangle$ with $c_{pn} = 1$ and $c_i = a_m^{-1} a_{r+i}$ for $i > pn$. Recursively define $b_n = 1$ and $b_{n+i} = (c_{pn+i} - g_i)/p$ for $i \in \mathbb{N}$, where g_i is the polynomial in $b_n, b_{n+1}, \ldots, b_{n+i-1}$ described above. If we set $\beta = \sum_{i\geq n} b_i P^i$, then $\beta \in \mathbb{F}_{q^d}\langle P\rangle$ and $\beta^p = \gamma$.

If $p \mid m$, then $r = 0$, so $\alpha = a_m\gamma = a_m\beta^p$. Thus, α has a p-th root in $\mathbb{F}_{q^d}\langle P\rangle$ if a_m is a p-th power in $\mathbb{F}_{q^d}\langle P\rangle$; otherwise, α has a p-th root in $\mathbb{F}\langle P\rangle \setminus \mathbb{F}_{q^d}\langle P\rangle$ where $\mathbb{F}$ is an extension of $\mathbb{F}_{q^d}$ obtained by adjoining a p-th root of a_m to $\mathbb{F}_{q^d}$.

Assume now that $p \nmid m$. Then any p-th root of α lies in a field of the form $L = \overline{\mathbb{F}}_q\langle P\rangle(\pi)$ with $\pi^p = P^r$, but not in $\overline{\mathbb{F}}_q\langle P\rangle$. Since $\pi \notin \overline{\mathbb{F}}_q\langle P\rangle$ and p is coprime to r, L is a degree p extension of $\overline{\mathbb{F}}_q\langle P\rangle$, and α has no p-th root in $\overline{\mathbb{F}}_q\langle P\rangle$. ■

We will also require Cardano's well-known formulae for the roots of a cubic equation:

Lemma 7.2 **(Cardano's formulae)** *Let $\mathbb{F}$ be any field of characteristic not equal to 2 or 3, and let $A, B \in \mathbb{F}$. Then the roots t_0, t_1, t_2 of the equation $t^3 - At + B = 0$ are given by*

$$t_i = \frac{1}{3}(u^i\delta_+ + u^{-i}\delta_-) \quad (i = 0, 1, 2), \tag{7.1}$$

where u is a primitive cube root of unity in some extension of $\mathbb{F}$,

$$\delta_+ = \sqrt[3]{-\frac{3}{2}(9B + \sqrt{-3D})}, \quad \delta_- = \sqrt[3]{-\frac{3}{2}(9B - \sqrt{-3D})},$$

with $D = 4A^3 - 27B^3$, and where the cube roots are taken so that $\delta_+\delta_- = 3A$. We also have

$$\delta_+ = t_0 + u^2 t_1 + u t_2, \quad \delta_- = t_0 + u t_1 + u^2 t_2. \tag{7.2}$$

Note that the choice of cube roots so that $\delta_+\delta_- = 3A$ leaves three choices for the cube root of δ_+, but different choices for this cube root only lead to a different ordering of the roots t_0, t_1, t_2.

For any place P of $\mathbb{F}_q(x)$, the possible P-signatures of a cubic extension $K/\mathbb{F}_q(x)$ are $(1,1;1,1;1,1)$, $(1,1;1,2)$, $(1,1;2,1)$, $(1,3)$, and $(3,1)$. We can characterize these five signatures using the polynomial discriminant and the Lagrange resolvent.

Lemma 7.3 *Let $K = \mathbb{F}_q(x,y)$ be a cubic function field in standard form given by* (4.2)*, D given by* (4.1)*, u a primitive cube root of unity, δ_+ as given in Lemma* 7.2*, and P any place of $K/\mathbb{F}_q(x)$ of degree d. Then the following hold.*

- *If P is unramified in K, then $\delta_+ \in \overline{\mathbb{F}}_q\langle P\rangle$. In this case, if $K/\mathbb{F}_q(x)$ has P-signature*
  - *$(1,1;1,1;1,1)$, then D is a square in $\mathbb{F}_{q^d}\langle P\rangle$ and $\delta_+ \in \mathbb{F}_{q^d}(u)\langle P\rangle$;*
  - *$(1,1;1,2)$, then D is not a square in $\mathbb{F}_{q^d}\langle P\rangle$;*
  - *$(1,3)$, then D is a square in $\mathbb{F}_{q^d}\langle P\rangle$ and $[\mathbb{F}_{q^d}(u)\langle P\rangle(\delta_+) : \mathbb{F}_{q^d}(u)\langle P\rangle] = 3$.*
- *If P is ramified, then $\delta_+ \notin \overline{\mathbb{F}}_q\langle P\rangle$. In this case, if $K/\mathbb{F}_q(x)$ has P-signature*
  - *$(1,1;2,1)$, then D is not a square in $\overline{\mathbb{F}}_q\langle P\rangle$;*
  - *$(3,1)$, then D is a square in $\overline{\mathbb{F}}_q\langle P\rangle$ and $[\overline{\mathbb{F}}_q\langle P\rangle(\delta_+):\overline{\mathbb{F}}_q\langle P\rangle] = 3$.*

Proof Let $y^{(0)}, y^{(1)}, y^{(2)}$ denote the three roots of (4.2). By Theorem 3.1, P is unramified if and only if $y^{(0)}, y^{(1)}, y^{(2)} \in \overline{\mathbb{F}}_q\langle P\rangle$, which holds if and only if $\delta_+ \in \overline{\mathbb{F}}_q\langle P\rangle$ by (7.1) and (7.2).

Suppose first that P is unramified, and set $L = \mathbb{F}_{q^d}\langle P\rangle$, $N = L(y^{(0)}, y^{(1)}, y^{(2)})$ for brevity. Then $N \subset \overline{\mathbb{F}}_q\langle P\rangle$ and $[N:L] \le 3$ by Theorem 3.1. Note also that

$$\sqrt{D} = \pm(y^{(0)} - y^{(1)})(y^{(1)} - y^{(2)})(y^{(2)} - y^{(0)}). \tag{7.3}$$

If $K/\mathbb{F}_q(x)$ has P-signature $(1,1;1,1;1,1)$, then $y^{(0)}, y^{(1)}, y^{(2)} \in L$ by Theorem 3.1, so $\sqrt{D} \in L$ by (7.3). By (7.2), $\delta_+ \in L(u)$.

If $K/\mathbb{F}_q(x)$ has P-signature $(1,1;1,2)$, then $[N:L] = 2$, and one of the roots, say $y^{(0)}$, belongs to L by Theorem 3.1. Then N/L is a Galois extension with minimal polynomial $G(Y) = (Y-y^{(1)})(Y-y^{(2)}) \in L[Y]$; in particular, $G(y^{(0)}) \in L$. Now since $y^{(1)} + y^{(2)} = -y^{(0)} \in L$, we cannot have $y^{(1)} - y^{(2)} \in L$, as otherwise $y^{(1)}, y^{(2)} \in L$, contradicting $[N:L] = 2$. It follows that $\sqrt{D} = (y^{(1)} - y^{(2)})G(y^{(0)}) \notin L$.

If $K/\mathbb{F}_q(x)$ has P-signature $(1,3)$, then $[N:L] = 3$ by Theorem 3.1. Furthermore, N/L is a Galois extension with minimal polynomial $F(Y)$. Thus, its discriminant, and hence also D, must be a square in L. It follows that $\delta_+^3 \in L(u)$. If we had $\delta_+ \in L(u)$, then $N \subseteq L(u)$ by (7.1), so $3 = [N:L] \le [L(u):L] \le 2$, a contradiction. Thus, $[L(u)(\delta_+):L(u)] = 3$.

Now suppose that P is ramified, and set $L = \overline{\mathbb{F}}_q\langle P\rangle$ and $N = L(y^{(0)}, y^{(1)}, y^{(2)})$. The proof for the case of P-signature $(1,1;2,1)$ applies verbatim to the scenario of P-signature $(1,1;1,2)$. If $K/\mathbb{F}_q(x)$ has P-signature $(3,1)$, then $[N:L] = 3$ by Theorem 3.1. In fact, since N/L is tamely ramified, it is a cyclic Galois extension with minimal polynomial $F(Y)$. So $\sqrt{D} \in L$. Then $\delta_+^3 \in L$, and since $\delta_+ \notin L$, we have $[L(\delta_+):L] = 3$. ∎

Corollary 7.4 *Let K, D, u, and δ_+ be as in Lemma* 7.3*. Then $K/\mathbb{F}_q(x)$ has P_∞-signature*

- $(1,1;1,1;1,1)$ *if* $\deg(D)$ *is even,* $\operatorname{sgn}(D)$ *is a square in* $\mathbb{F}_q$, $\deg(\delta_+^3) \equiv 0 \pmod 3$, *and* $\operatorname{sgn}(\delta_+^3)$ *is a cube in* $\mathbb{F}_q(u)$*;*
- $(1,1;1,2)$ *if* $\deg(D)$ *is even,* $\operatorname{sgn}(D)$ *is not a square in* $\mathbb{F}_q$, *and* $\deg(\delta_+^3) \equiv 0 \pmod 3$*;*
- $(1,3)$ *if* $\deg(D)$ *is even,* $\operatorname{sgn}(D)$ *is a square in* $\mathbb{F}_q$, $\deg(\delta_+^3) \equiv 0 \pmod 3$ *and* $\operatorname{sgn}(\delta_+^3)$ *is not a cube in* $\mathbb{F}_q(u)$*;*
- $(1,1;2,1)$ *if* $\deg(D)$ *is odd;*
- $(3,1)$ *if* $\deg(D)$ *is even and* $\deg(\delta_+^3) \not\equiv 0 \pmod 3$.

Proof By Lemma 7.1, $\sqrt{D} \in \overline{\mathbb{F}}_q\langle x^{-1}\rangle$ if and only if $\deg(D)$ is even, and $\sqrt{D} \in \mathbb{F}_q\langle x^{-1}\rangle$ if and only if in addition $\operatorname{sgn}(D)$ is a square in $\mathbb{F}_q$. Now $\delta_+^3 \in \mathbb{F}_q(x)(\sqrt{-3D})$. So if $\deg(D)$ is even, then again by Lemma 7.1, $\delta_+ \in \overline{\mathbb{F}}_q\langle x^{-1}\rangle$ if and only if $\deg(\delta_+^3) \equiv 0 \pmod 3$. If in addition $\operatorname{sgn}(D)$ is a square in $\mathbb{F}_q$, then $\delta_+ \in \mathbb{F}_q(u)\langle x^{-1}\rangle$ if and only if $\operatorname{sgn}(\delta_+^3)$ is a cube in $\mathbb{F}_q(u)$. The corollary now follows immediately from Lemma 7.3. ■

Corollary 7.5 *Let K, D, u, and δ_+ be as in Lemma 7.3, and let P be a finite place of $\mathbb{F}_q(x)$ of degree d. Then $K/\mathbb{F}_q(x)$ has P-signature*

- $(1,1;1,1;1,1)$ *if* $v_P(D)$ *is even,* $D/P^{v_P(D)}$ *is a square modulo P in* $\mathbb{F}_{q^d}$, $v_P(\delta_+^3) \equiv 0 \pmod 3$, *and* $\delta_+^3/P^{v_P(\delta_+^3)}$ *is a cube modulo P in* $\mathbb{F}_{q^d}(u)$*;*
- $(1,1;1,2)$ *if* $v_P(D)$ *is even,* $D/P^{v_P(D)}$ *is not a square modulo P in* $\mathbb{F}_{q^d}$, *and* $v_P(\delta_+^3) \equiv 0 \pmod 3$*;*
- $(1,3)$ *if* $v_P(D)$ *is even,* $D/P^{v_P(D)}$ *is a square modulo P in* $\mathbb{F}_{q^d}$, $v_P(\delta_+^3) \equiv 0 \pmod 3$, *and* $\delta_+^3/P^{v_P(\delta_+^3)}$ *is not a cube modulo P in* $\mathbb{F}_{q^d}(u)$*;*
- $(1,1;2,1)$ *if* $v_P(D)$ *is odd;*
- $(3,1)$ *if* $v_P(D)$ *is even and* $v_P(\delta_+^3) \not\equiv 0 \pmod 3$.

Proof This follows analogous to Corollary 7.4. Again by Lemma 7.1, $\sqrt{D} \in \overline{\mathbb{F}}_q\langle P\rangle$ if and only if $v_P(D)$ is even, and $\sqrt{D} \in \mathbb{F}_{q^d}\langle P\rangle$ if and only if in addition $D/P^{v_P(D)}$ is a square modulo P in $\mathbb{F}_q[x]$. If $v_P(D)$ is even, then $\delta_+ \in \overline{\mathbb{F}}_q\langle P\rangle$ if and only if $v_P(\delta_+^3) \equiv 0 \pmod 3$. If in addition $D/P^{v_P(D)}$ is a square modulo P in $\mathbb{F}_q[x]$, then $\delta_+ \in \mathbb{F}_{q^d}(u)\langle P\rangle$ if and only if $\delta_+^3/P^{v_P(\delta_+^3)}$ is a cube modulo P in $\mathbb{F}_{q^d}(u)$. ■

8 Signatures and Genus of a Cubic Function Field

We now have all the ingredients for a straightforward characterization of the P-signature of a cubic function field $K/\mathbb{F}_q(x)$ for any place P of $\mathbb{F}_q(x)$.

The signature at infinity of a purely cubic function field was first presented in [23, Theorem 2.1]. The case of arbitrary cubic function fields was discussed in [21, Theorem 4.2]; the characterization given below is slightly different from that source. We also point out that a more algebraic investigation of the unit rank of a cubic function field, which is one less than the number of places at infinity (see for example [19, p. 243] or [8, p. 595]), was provided in [13].

Theorem 8.1 *Let $K = \mathbb{F}_q(x,y)$ be a cubic function field in standard form given by* (4.2)*, with D given by* (4.1)*, and let $u \in \overline{\mathbb{F}}_q$ be a primitive cube root of unity. If* $\deg(D)$ *is even and* $\operatorname{sgn}(D)$ *is a square in* $\mathbb{F}_q$*, set* $s = -3\ \operatorname{sgn}(9B + \sqrt{-3D})/2 \in \mathbb{F}_q(u)$*. Then* $K/\mathbb{F}_q(x)$ *has* P_∞*-signature*

- $(1, 1; 1, 1; 1, 1)$ *if*
  - $3\deg(A) > 2\deg(B)$, $\deg(A)$ *is even, and* $\operatorname{sgn}(A)$ *is a square in* $\mathbb{F}_q$*;*
  - $3\deg(A) < 2\deg(B)$, $\deg(B) \equiv 0 \pmod 3$, $\operatorname{sgn}(B)$ *is a cube in* $\mathbb{F}_q$*, and* $q \equiv 1 \pmod 3$*;*
  - $3\deg(A) = 2\deg(B)$, $\deg(D)$ *is even,* $\operatorname{sgn}(D)$ *is a square in* $\mathbb{F}_q$*, and* s *is a cube in* $\mathbb{F}_q(u)$.
- $(1, 1; 1, 2)$ *if*
  - $3\deg(A) > 2\deg(B)$, $\deg(A)$ *is even, and* $\operatorname{sgn}(A)$ *is not a square in* $\mathbb{F}_q$*;*
  - $3\deg(A) < 2\deg(B)$, $\deg(B) \equiv 0 \pmod 3$*, and* $q \equiv -1 \pmod 3$*;*
  - $3\deg(A) = 2\deg(B)$, $\deg(D)$ *is even, and* $\operatorname{sgn}(D)$ *is not a square in* $\mathbb{F}_q$*;*
- $(1, 3)$ *if*
  - $3\deg(A) < 2\deg(B)$, $\deg(B) \equiv 0 \pmod 3$*, and* $\operatorname{sgn}(B)$ *is not a cube in* $\mathbb{F}_q$*;*
  - $3\deg(A) = 2\deg(B)$, $\deg(D)$ *is even,* $\operatorname{sgn}(D)$ *is a square in* $\mathbb{F}_q$*, and* s *is not a cube in* $\mathbb{F}_q(u)$.
- $(1, 1; 2, 1)$ *if* $\deg(D)$ *is odd;*
- $(3, 1)$ *if* $3\deg(A) < 2\deg(B)$ *and* $\deg(B) \not\equiv 0 \pmod 3$.

Proof Let δ_+ and δ_- be defined as in Lemma 7.2. If $\deg(D)$ is even and $\operatorname{sgn}(D)$ is a square in $\mathbb{F}_q$, then $\delta_+^3 \in \mathbb{F}_q(u)\langle x^{-1}\rangle$ and $s = \operatorname{sgn}(\delta_+^3) \in \mathbb{F}_q(u)$. In this case, we have $\deg(\delta_+^3), \deg(\delta_-^3) \le \max\{\deg(B), \deg(\sqrt{-3D})\}$, and equality must hold for at least one of δ_+ and δ_-. Furthermore, $\deg(\delta_+^3) \equiv 0 \pmod 3$ if and only if $\deg(\delta_-^3) \equiv 0 \pmod 3$, and $\operatorname{sgn}(\delta_+^3) \in \mathbb{F}_q(u)$ if and only if $\operatorname{sgn}(\delta_-^3) \in \mathbb{F}_q(u)$. The theorem now follows by verifying the conditions of Corollary 7.4 for each of the cases listed above. ■

Note that it is easy to determine whether or not an element $a \in \mathbb{F}^*$ is a square or a cube in a finite field $\mathbb{F}$ of cardinality $r \equiv 1 \pmod 6$. Namely, a is a square in $\mathbb{F}$ if and only if $a^{(r-1)/2} = 1$, and a is a cube in $\mathbb{F}$ if and only if $a^{(r-1)/3} = 1$.

Furthermore, consider the case where $\deg(D) = 3\deg(A) = 2\deg(B)$ and $\operatorname{sgn}(D) = 4\operatorname{sgn}(A)^3 - 27\operatorname{sgn}(B)^2$ is a square in $\mathbb{F}_q$. Then we need to compute a square root of $\operatorname{sgn}(D)$ in $\mathbb{F}_q$ (a square root of -3 is $u - u^2 = 2u + 1$). There are a number of efficient well-known methods for finding square roots in finite fields, see [15, 25] and the many improvements to these methods. Note that in this case, the equation $t^3 - \operatorname{sgn}(A)t + \operatorname{sgn}(B)$ has three roots in $\mathbb{F}_q$ if s is a cube in $\mathbb{F}_q(u)$ and no roots in $\mathbb{F}_q$ otherwise; it has exactly one root in $\mathbb{F}_q$ if $\deg(D) = 3\deg(A) = 2\deg(B)$ and $\operatorname{sgn}(D) = \operatorname{sgn}(A)^3 - 27\operatorname{sgn}(B)^2$ is a non-square in $\mathbb{F}_q$. This was used in the characterization of the P_∞-signature of $K/\mathbb{F}_q(x)$ given in [21].

We can now easily compute the genus of K. By (3.1) and Theorem 8.1, we have

$$\epsilon_{P_\infty}(K) = \begin{cases} 2 & \text{if } 3\deg(A) < 2\deg(B) \text{ and } \deg(B) \not\equiv 0 \pmod 3, \\ 1 & \text{if } \deg(D) \text{ is odd}, \\ 0 & \text{otherwise.} \end{cases}$$

Then by (3.2), the genus of K is $g = \frac{1}{2}(\deg(\Delta) + \epsilon_{P_\infty}(K)) - 2$.

We now proceed to characterize signatures of finite places. The description of the signature of any finite place of $\mathbb{F}_q(x)$ is analogous to the one for primes different from 2 and 3 in cubic number fields given in [16]. The case of purely cubic function fields was first presented in [20, Theorem 3.1].

Theorem 8.2 *Let $K = \mathbb{F}_q(x, y)$ be a cubic function field in standard form given by* (4.2) *with D given by* (4.1). *Let $u \in \overline{\mathbb{F}}_q$ be a primitive cube root of unity and P a finite place of $\mathbb{F}_q(x)$. If $v_P(D)$ is even and D is a square modulo P, let $Q \in \mathbb{F}_q(u)[x]$ be any square root of $-3D$ modulo P. Set $R = -3(9B + Q)/2$ and $S = R/P^{v_P(R)}$ $(R, S \in \mathbb{F}_q(u)[x])$. Then $K/\mathbb{F}_q(x)$ has P-signature*

- $(1, 1; 1, 1; 1, 1)$ *if*
  - $v_P(A) = 0 < v_P(B)$, *and A is a square modulo P;*
  - $v_P(A) > 0 = v_P(B)$, $q^{\deg(P)} \equiv 1 \pmod 3$, *and B is a cube modulo P;*
  - $v_P(A) = v_P(B) = 0$, $v_P(D)$ *is even, $D/P^{v_P(D)}$ is a square modulo P, and S is a cube modulo P in $\mathbb{F}_q(u)[x]$;*
- $(1, 1; 1, 2)$ *if*
  - $v_P(A) = 0 < v_P(B)$, *and A is not a square modulo P;*
  - $v_P(A) > 0 = v_P(B)$, *and* $q^{\deg(P)} \equiv -1 \pmod 3$*;*
  - $v_P(A) = v_P(B) = 0$, $v_P(D)$ *is even, and $D/P^{v_P(D)}$ is not a square modulo P;*
- $(1, 3)$ *if*
  - $v_P(A) > 0 = v_P(B)$, $q^{\deg(P)} \equiv 1 \pmod 3$, *and B is not a cube modulo P;*
  - $v_P(A) = v_P(B) = 0$, *and $v_P(D)$ is even, $D/P^{v_P(D)}P$ is a square modulo P, and S is not a cube modulo P in $\mathbb{F}_q(u)[x]$;*
- $(1, 1; 2, 1)$ *if $v_P(D)$ is odd;*
- $(3, 1)$ *if* $1 \le v_P(B) \le v_P(A)$.

Proof The restriction that $K/\mathbb{F}_q(x)$ is in standard form immediately implies the following:

- $3v_P(A) < 2v_P(B)$ and $v_P(A)$ even if and only if $v_P(A) = 0 < v_P(B)$;
- $3v_P(A) > 2v_P(B)$ and $v_P(B) \equiv 0 \pmod 3$ if and only if $v_P(A) > 0 = v_P(B)$;
- $3v_P(A) > 2v_P(B)$ and $v_P(B) \not\equiv 0 \pmod 3$ if and only if $1 \le v_P(B) \le v_P(A)$;
- $3v_P(A) = 2v_P(B)$ if and only if $v_P(A) = v_P(B) = 0$.

The proof is now completely analogous to that of Theorem 8.1, if everywhere in that proof we replace x^{-1} by P and $\mathbb{F}_q$ by $\mathbb{F}_{q^d}$ in every field of Laurent series, as well as s by S, $\deg(\alpha)$ by $-v_P(\alpha)$, and $\operatorname{sgn}(\alpha)$ by $G/P^{v_P(\alpha)} \pmod P$ for $\alpha \in \{D, \delta_+, \delta_-\}$. ■

Once again, if $\mathbb{F}$ is a finite extension of $\mathbb{F}_q$ of cardinality $r \equiv 1 \pmod 6$, and $G, P \in \mathbb{F}[x]$ with P irreducible of degree d and $P \nmid G$, then G is a square modulo P if and only if $G^{(r^d-1)/2} \equiv 1 \pmod P$, and G is a cube modulo P if and only if $G^{(r^d-1)/3} \equiv 1 \pmod P$. Furthermore, if $v_P(D)$ is even and D is a square modulo P, then we need to compute a square root of D modulo P in $\mathbb{F}_q[x]$, which amounts to computing a square root in the field $\mathbb{F}_{q^d}$. Again, if $v_P(D)$ is even and $v_P(A) = v_P(B) = 0$, then the congruence $t^3 - At + B \equiv 0 \pmod P$ has three solutions in $\mathbb{F}_q[x]$ if $D/P^{v_P(D)}$ is a square modulo P in $\mathbb{F}_q[x]$ and S is a cube modulo P in $\mathbb{F}_q(u)[x]$, no solutions in $\mathbb{F}_q[x]$

if $D/P^{v_P(D)}$ is a square modulo P in $\mathbb{F}_q[x]$ and S is not a cube modulo P in $\mathbb{F}_q(u)[x]$, and exactly one solution in $\mathbb{F}_q[x]$ if $D/P^{v_P(D)}$ is not a square modulo P in $\mathbb{F}_q[x]$.

We now provide two applications of the signature computations discussed in the previous section, namely computing the class number of a function field, and obtaining information about the distribution of the zeros of the zeta function. Both are explained in more detail in [22].

9 Application 1: Class Number Computation

The places of any algebraic function field $K/\mathbb{F}_q$ of genus g generate a free Abelian group $\mathcal{D}_K$ known as the group of *divisors* of $K/\mathbb{F}_q$. The notion of degree of a place of K then extends homomorphically to divisors, *i.e.,* for any divisor $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{a_{\mathfrak{p}}} \in \mathcal{D}_K$, the degree of $\mathfrak{a}$ is $\deg(\mathfrak{a}) = \sum_{\mathfrak{p}} a_{\mathfrak{p}} \deg(\mathfrak{p})$. Let $\mathcal{D}_K^0$ be the subgroup of $\mathcal{D}_K$ of divisors of degree zero, and $\mathcal{P}_K$ the subgroup of $\mathcal{D}_K^0$ of *principal* divisors; these are divisors of the form $\operatorname{div}(\alpha) = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha)}$ with $\alpha \in K^*$. Then the factor group $\mathrm{Pic}_K^0 = \mathcal{D}_K^0/\mathcal{P}_K$ is a finite Abelian group, known as the (*degree zero*) *divisor class group* (or *Jacobian*) of $K/\mathbb{F}_q$, whose order h_K is the *divisor class number* of K. The computation of h_K is an important problem in number theory and arithmetic geometry. It also has applications to cryptography, since cryptographic schemes based on algebraic curves require that h_K be known.

One way of computing h_K can be described at a high level as follows:

(i) Compute an approximation $E \in \mathbb{N}$ of h_K and an error $U \in \mathbb{N}$ such that $|h_K - E| < U$.
(ii) Search through the open interval $]E - U, E + U[$ to find h_K.

While in principle, this idea applies in any algebraic function field [22], it has been most extensively researched for application to hyperelliptic, *i.e.,* quadratic, function fields [26–29], and to some extent for cubic function fields [24].

We comment briefly on item (ii) above. The search can be performed using Shanks' baby-step giant-step or Pollard's kangaroo method. This procedure requires an efficient arithmetic framework on divisors of K. For quadratic extensions, there is a large volume of literature on the subject, starting with [4]; we simply refer to the sources cited in the previous paragraph. Arithmetic in purely cubic function fields was provided in [2, 14, 20, 21]; work on arbitrary cubic function fields as considered in this paper is in progress. The number of operations required to conduct a search using baby-step giant-step or Pollard kangaroo is essentially the square root of the length of the interval. The interval $]E - U, E + U[$ has length $2U - 1$, so step (ii) of the above method requires $c\sqrt{U}$ operations on divisors of K for some constant c that depends on the cost of the arithmetic, *i.e.,* on the size q of the base field and the genus g of $K/\mathbb{F}_q$.

We now elaborate further on step (i) of the algorithm above as it is a direct application of the work on signatures provided here. The *zeta function* of $K/\mathbb{F}_q$ is the power series

$$\zeta_K(s) = \sum_{\mathfrak{a} \geq 0} q^{-\deg(\mathfrak{a})s} \quad (\Re(s) > 1),$$

where $\Re(s)$ is the real part of the complex variable s, and the summation is over all *effective* divisors $\mathfrak{a} \geq 0$ of K, *i.e.,* divisors $\mathfrak{a}$ for which $\nu_{\mathfrak{p}}(\mathfrak{a}) \geq 0$ for all places $\mathfrak{p}$ of K. It is known that $\zeta_K(s)$ is periodic with period $2\pi i/\log q$ and analytic in the entire complex plane with the exception of simple poles at $s \equiv 0, 1 \pmod{2\pi i/\log(q)}$. We have

$$\zeta_K(s) = \frac{L_K(q^{-s})}{(1-q^{-s})(1-q^{1-s})}, \tag{9.1}$$

where $1/(1-q^{-s})(1-q^{1-s}) = \zeta_{\mathbb{F}_q(x)}(s)$ is the zeta function of the rational function field $\mathbb{F}_q(x)$, and $L_K(t) \in \mathbb{Z}[t]$ is a polynomial of degree $2g$ in t that is referred to as the *L-polynomial* of $K/\mathbb{F}_q(x)$. The *analytic class number formula* connects the class number with the zeta function and asserts that $h_K = L_K(1)$. We have

$$L_K(t) = \prod_{j=1}^{2g}(1-\omega_j t), \tag{9.2}$$

where the ω_j are algebraic integers of absolute value $\sqrt{q}$. This latter statement is known as the *Riemann hypothesis for function fields* and is in fact not a hypothesis, but a theorem that was first proved in full generality in 1948 by A. Weil [34, 35].

The zeta function has an Euler product representation

$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1-q^{-\deg(\mathfrak{p})s}},$$

where the product ranges over all places $\mathfrak{p}$ of K. A truncated version of this product, using only finitely many terms, can be used to explicitly compute a value E' such that $h_K = E'e^B$. Here B is determined by the "tail" of the product, and the cut-off point in the product is large enough such that $|B| < \psi$ for some bound ψ that is significantly less than one and can be computed explicitly. If we define $E \in \mathbb{N}$ to be the nearest integer to E', *i.e.,* $E \in \mathbb{N}$ with $-1/2 < |E - E'| \leq 1/2$, and set $U = \lceil E'(e^{\psi}-1) + 1/2 \rceil \in \mathbb{N}$, then

$$|h_K - E| = |E'(e^B-1) + (E'-E)| \leq |E'(e^B-1)| + |E'-E| < E'(e^{\psi}-1) + \frac{1}{2} \leq U.$$

Thus, E and U are the desired parameters for our class number algorithm. If we write $K = \mathbb{F}_q(x,y)$, then

$$\zeta_K(s) = \prod_{\mathfrak{p}|P_\infty} \frac{1}{1-q^{-f(\mathfrak{p}|P_\infty)s}} \prod_{P \neq P_\infty} \prod_{\mathfrak{p}|P} \frac{1}{1-q^{-f(\mathfrak{p}|P)\deg(P)s}}.$$

The first product requires knowledge of the P_∞-signature of $K/\mathbb{F}_q(x)$, or at least of the residue degrees of all the places of K lying above P_∞. The second product ranges over all monic irreducible polynomials in $\mathbb{F}_q[x]$. A truncated version of this product requires the computation of the signatures of all the finite places of $\mathbb{F}_q(x)$ up to a

certain degree bound λ. Thus, efficient signature computation is an essential tool in computing the class number of K.

To optimize the algorithm, the running times of the two steps of the class number algorithm should be balanced, *i.e.,* roughly equal. By our remarks above, the computation of E and U thus should take time $c'\sqrt{U}$ for some constant c'. This determines the cut-off point λ for truncation of the Euler product. The best choice is to let λ be the nearest integer to $(2g-1)/5$, giving an overall running time of $O(q^{(2g-1)/5})$ for fixed genus g and $q \to \infty$. Details for cubic function field extensions can be found in [24]. The case of arbitrary function fields was discussed in [22].

10 Application 2: Distribution of Class Numbers and Zeros of Zeta Functions

The quantities E and U, and thus the signature computations performed to obtain them, have further uses in the analysis of the distribution of the zeros of zeta functions. In the interest of space, we can only give an overview of the underlying ideas, which are rather sophisticated. By (9.1) and (9.2), the values $\log_q(\omega_j)$ $(1 \le j \le 2g)$ are zeros of the zeta function $\zeta_K(s)$ of $K/\mathbb{F}_q$. Write $\omega_j = \sqrt{q}e^{i\varphi_j}$ with $\varphi_j \in [0, 2\pi[$. Since it is well known that $\overline{\omega_j} = \omega_{g+j}$, we have $\varphi_{j+g} \equiv -\varphi_j \pmod{2\pi}$ for $1 \le j \le g$, and we can enumerate the φ_j such that $0 \le \varphi_j \le \pi$ and $\varphi_{j+g} \equiv -\varphi_j \pmod{2\pi}$ for $1 \le j \le g$. Now define the quantity

$$S(n) = \Big|\sum_{j=1}^{g} e^{ni\varphi_j}\Big| = 2\Big|\sum_{j=1}^{g} \cos(ni\varphi_j)\Big|.$$

The mean of $S(n)$ over all function fields of fixed genus g provides information on the distribution behavior of the φ_j, and hence of the zeros of zeta functions $\zeta_K(s)$ of function fields $K/\mathbb{F}_q$ of genus g as $q \to \infty$.

We now relate the quantity $S(n)$ to the results in the previous section. The two are connected through the question of how good a bound U is on the "error" $|h_K - E|$. Let $\alpha(q,g)$ be the average of the quotient $|h_K - E|/U$ over all function fields $K/\mathbb{F}_q$ of genus g; the quantity $\alpha(g,q)$ measures how well U bounds $|h_K - E|$ in general for function fields $K/\mathbb{F}_q$ of genus g. If we let $\alpha(g) = \lim_{q\to\infty} \alpha(g,q)$, then we see that the bound U on $|h_K - E|$ is on average by a factor of $\alpha(g)^{-1}$ too large.

Recall that $e^t - 1 \approx t$ for $|t|$ significantly less than one. Since $E' \approx E$ and $|B|, \psi$ are much smaller than one for large q, we thus have $|h_K - E| \approx E'|e^B - 1| \approx E|B|$; similarly, $U \approx E\psi$. It follows that $|h_K - E|/U \approx |B|/\psi$, and hence one would expect that

$$\alpha(g,q) \approx \mathrm{Mean}\Big(\frac{|B|}{\psi}\Big).$$

It can be shown [22] that in many cases, the dominant term in the quotient $|B|/\psi$ is $S(\lambda+1)$ where λ is the nearest integer to $(2g-1)/5$ as discussed in the previous section. For example, this always holds if λ is even and in some other cases as well; otherwise, a certain correction term needs to be added to obtain the correct limit. Hence, if we can determine the mean of $S(\lambda+1)$, then we can find $\alpha(g,q)$ and thus

$\alpha(g)$, at least heuristically. Using results by Katz and Sarnak [10, 11], this mean was numerically computed for hyperelliptic function fields in [26]. Unfortunately, this mean appears to be very difficult to compute for other types of fields.

However, the above argument could be turned around as follows. If one had access to a fast class number algorithm, then it would be possible to compute the quotients $|h_K - E|/U$ for a large number of function fields $K/\mathbb{F}_q$ for fixed q and g. Taking the numerical average of all these quotients could give an idea of the value of $\alpha(q, g)$. Repeating this process for many large prime powers q might ultimately shed light on the value of the limit $\alpha(g)$. Each of the quotients $|h_K - E|/U$ requires the computation of the residue degrees of a large number of places, so once again, an efficient way of determining signatures is a necessary ingredient here.

11 Open Problems

A number of open problems arise from this work. For example, it is unclear how some of the results in this paper can be extended to cubic extensions of characteristic 2 or even 3. An investigation of certain characteristic 3 fields is currently being undertaken by the fourth author; work on the characteristic 2 case is also in progress.

Our proofs of Theorems 8.1 and 8.2 rely heavily on Cardano's formulae as given in Lemma 7.2. While similar techniques may extend to other function fields with solvable minimal polynomials, they are clearly not generalizable to arbitrary function fields. Moreover, algorithms for computing the field discriminant and integral bases of function field extensions of arbitrary degree exist, but they are less efficient than methods that rely on the simple types of ingredients used here, such as square-free factorizations or extracting roots over finite fields.

The class number algorithm described above requires efficient arithmetic on divisors in any cubic function field K. While such arithmetic was provided for purely cubic extensions in [2, 14, 20, 21], it has not yet been developed for arbitrary cubic fields. In contrast to the hyperelliptic case, explicit formulae for divisor addition, or equivalently, ideal multiplication, in purely cubic function fields as described in [2, 20] are already quite intricate. The case of arbitrary cubic function fields is even more complicated. The level of complexity only increases as one considers function fields of higher degree. There is discussion of divisor arithmetic for arbitrary function fields in [9, 33], and a more geometric approach was taken in [12], but it remains to be seen how efficient these methods are when implemented and applied to extensions of large degree.

Acknowledgments This work began as a student research project conducted during the Rocky Mountain Mathematics Consortium Graduate Summer School on Computational Number Theory and Applications to Cryptography, held June 19–July 7, 2006, at the University of Wyoming. The authors wish to thank an anonymous referee for a thorough review of this work and for a number of very helpful suggestions that led to significant improvements to this paper.

References

[1] A. A. Albert, *A determination of the integers of all cubic fields.* Ann. of Math. **31**(1930), no. 4, 550–566. doi:10.2307/1968153

[2] M. L. Bauer, *The arithmetic of certain cubic function fields.* Math. Comp. **73**(2004), no. 245, 387–413. (electronic) doi:10.1090/S0025-5718-03-01559-X

[3] J. A. Buchmann and H. W. Lenstra, Jr., *Approximating rings of integers in number fields.* J. Théor. Nombres Bordeaux **6**(1994), no. 2, 221–260.

[4] D. G. Cantor, *Computing in the Jacobian of a hyperelliptic curve.* Math. Comp. **48**(1987), no. 177, 95–101. doi:10.2307/2007876

[5] A. L. Chistov, *The complexity of constructing the ring of integers in a global field.* Soviet. Math. Dokl. **39**(1989), no. 5, 597–600.

[6] H. Cohen, *A Course in Computational Algebraic Number Theory*. Graduate Texts in Mathematics 138. Springer-Verlag, Berlin, 1993.

[7] B. N. Delone and K. Faddeev, *The Theory of Irrationalities of the Third Degree.* Translations of Mathematical Monographs 10. American Mathematical Society, Providence, RI, 1964.

[8] H. Hasse, *Number Theory*. Classics in Mathematics, Springer-Verlag, Berlin, 2002.

[9] F. Hess, *Computing Riemann-Roch spaces in algebraic function fields and related topics.* J. Symbolic Comput. **33**(2002), no. 4, 425–445. doi:10.1006/jsco.2001.0513

[10] N. M. Katz and P. Sarnak. *Random Matrices, Frobenius Eigenvalues and Monodromy.* American Mathematical Society Colloquium Publications 45. Amererican Mathematical Society, Providence, RI, 1999.

[11] ———, *Zeroes of zeta functions and symmetry.* Bull. Amer. Math. Soc. **36**(1999), no. 1, 1–26. doi:10.1090/S0273-0979-99-00766-1

[12] K. Khuri-Makdisi, *Linear algebra algorithms for divisors on an algebraic curve.* Math. Comp. **73**(2004), no. 245, 333–357. (electronic) doi:10.1090/S0025-5718-03-01567-9

[13] Y. Lee, *The unit rank classification of a cubic function field by its discriminant.* Manuscripta Math. **116**(2005), no. 2, 173–181. doi:10.1007/s00229-004-0530-5

[14] Y. Lee, R. Scheidler, and C. Yarrish, *Computation of the fundamental units and the regulator of a cyclic cubic function field.* Experiment. Math. **12**(2003), no. 2, 211–225.

[15] D. H. Lehmer, *Computer technology applied to the theory of numbers.* In: Studies in Number Theory. Math. Assoc. Amer., 1969, pp. 117–151.

[16] P. Llorente and E. Nart, *Effective determination of the decomposition of the rational primes in a cubic field.* Proc. Amer. Math. Soc. **87**(1983), no. 4, 579–585. doi:10.2307/2043339

[17] D. Lorenzini, *An Invitation to Arithmetic Geometry.* Graduate Studies in Mathematics 9. American Mathematical Society, Providence, RI, 1996.

[18] M. Pohst and H. Zassenhaus, *Algorithmic Algebraic Number Theory*. Revised reprint. Encyclopedia of Mathematics and its Applications 30. Cambridge University Press, Cambridge, 1997.

[19] M. Rosen, *Number Theory in Function Fields.* Graduate Texts in Mathematics 210. Springer-Verlag, New York, 2002.

[20] R. Scheidler, *Ideal arithmetic and infrastructure in purely cubic function fields.* J. Théorie Nombres Bordeaux, **13**(2001), no. 2, 609–631

[21] ———, *Algorithmic aspects of cubic function fields.* In: Algorithmic Number Theory. Lecture Notes in Comput. Sci. 3076. Springer-Verlag, Berlin, 2004, pp. 395–410.

[22] R. Scheidler and A. Stein, *Approximating Euler products and class number computation in algebraic function fields.* To appear in Rocky Mountain J. Math.

[23] ———, *Voronoi's algorithm in purely cubic congruence function fields of unit rank* 1. Math. Comp. **69**(2000), no. 231, 1245–1266. doi:10.1090/S0025-5718-99-01136-9

[24] ———, *Class number approximation in cubic function fields.* Contr. Discrete Math. **2**(2007), no. 2, 107–132. (electronic)

[25] D. Shanks. *Five number-theoretic algorithms.* In: Proc. Second Manitoba Conference on Numerical Mathematics. Congres 1973. Utilitas Math., Winnipeg, 1973, pp. 51–70.

[26] A. Stein and E. Teske, *Explicit bounds and heuristics on class numbers in hyperelliptic function fields.* Math. Comp. **71**(2002), no. 238, 837–861. (electronic) doi:10.1090/S0025-5718-01-01385-0

[27] ———, *The parallelized Pollard kangaroo method in real quadratic function fields.* Math. Comp. **71**(2002), no. 238, 793–814. (electronic) doi:10.1090/S0025-5718-01-01343-6

[28] ———, *Optimized baby-step giant-step methods.* J. Ramanujan Math. Soc. **20**(2005), no. 1, 1–32.

[29] A. Stein and H. C. Williams, *Some methods for evaluating the regulator of a real quadratic function field.* Experiment. Math. **8**(1999), no. 2, 119–133.

[30] H. Stichtenoth, *Algebraic Function Fields and Codes*. Springer-Verlag, Berlin, 1993.

[31] L. Tornheim, *Minimal basis and inessential discriminant divisors for a cubic field.* Pacific J. Math. **5**(1955), 623–631.
[32] E. von Żyliński, *Zur Theorie der außerwesentlichen Diskriminantenteiler algebraischer Körper.* Math. Ann. **73**(1913), no. 2, 273–274. doi:10.1007/BF01456716
[33] E. Volcheck, *Computing in the Jacobian of a plane algebraic curve.* In: Algorithmic Number Theory. Lecture Notes in Comput. Sci. 877. Springer, Berlin, 1994, pp. 221–233.
[34] A. Weil, *Sur les courbes algébraiques et les variétés qui s'en déduisent*. Hermann, Paris, 1948.
[35] ———, *Variétés abéliennes et courbes algébraiques*. Hermann, Paris, 1948.
[36] Q. Wu and R. Scheidler, *An explicit treatment of biquadratic function fields.* Contrib. Discrete Math. **2**(2007), no. 1, 43–60. (electronic)

Department of Mathematics, Kutztown University of Pennsylvania, Kutztown, PA 19530, USA
e-mail: elandqui@kutztown.edu

Department of Mathematics and Statistics, University of Calgary, Calgary, AB T2N 1N4
e-mail: pieter@math.ucalgary.ca
rscheidl@math.ucalgary.ca
quwu@math.ucalgary.ca

Department of Mathematics, Bates College, Lewiston, ME 04240, USA
e-mail: jwebster@bates.edu