International Journal of Number Theory
Vol. 11, No. 6 (2015) 1839–1885
© World Scientific Publishing Company
DOI: 10.1142/S1793042115500803

World Scientific
www.worldscientific.com

Construction of all cubic function fields of a given square-free discriminant

M. J. Jacobson, Jr.

Department of Computer Science
University of Calgary, 2500 University Drive NW
Calgary, Alberta, Canada T2N 1N4
jacobs@ucalgary.ca

Y. Lee

Department of Mathematics
Ewha Womans University, Seodaemoonku
Seoul 120-750, South Korea
yoonjinl@ewha.ac.kr

R. Scheidler[*] and H. C. Williams[†]

Department of Mathematics and Statistics
University of Calgary, 2500 University Drive NW
Calgary, Alberta, Canada T2N 1N4
[*]*rscheidl@ucalgary.ca*
[†]*hwilliam@ucalgary.ca*

Received 4 November 2013
Accepted 27 October 2014
Published 14 May 2015

For any square-free polynomial D over a finite field of characteristic at least 5, we present an algorithm for generating all cubic function fields of discriminant D. We also provide a count of all these fields according to their splitting at infinity. When $D' = D/(-3)$ has even degree and a leading coefficient that is a square, i.e. D' is the discriminant of a real quadratic function field, this method makes use of the infrastructures of this field. This infrastructure method was first proposed by Shanks for cubic number fields in an unpublished manuscript from the late 1980s. While the mathematical ingredients of our construction are largely classical, our algorithm has the major computational advantage of finding very small minimal polynomials for the fields in question.

Keywords: Cubic function field; quadratic function field; discriminant; signature; quadratic generator; reduced ideal.

Mathematics Subject Classification 2010: 11Y40, 11R58, 11R16, 11R11, 11-04

1. Introduction and Motivation

It is well-known that any quadratic field, or more generally, any order in a quadratic field, is uniquely determined by its discriminant. However, for global fields of higher degree, this is no longer true, and there are generally several non-conjugate fields of any given discriminant. This raises a number of questions: How many such fields are there — either for any one fixed discriminant or asymptotically, counting all absolute discriminants up to a given bound — and how can all these fields be constructed efficiently?

1.1. *Cubic number fields*

For cubic number fields, the above questions have all been answered. Let $N_3^{\pm}(X)$ denote the number of non-conjugate cubic fields of positive, respectively negative discriminant D with $|D| \leq X$. Davenport and Heilbronn [10, 11] determined explicit constants $c^{\pm}$ such that $N_3^{\pm}(X) \sim c^{\pm}X$, and a number of results on the error term have been established since then [5, 43, 44]. An analogous count for relative cubic number field extensions with a fixed quadratic resolvent field was provided in [8]. A very efficient algorithm for determining all $N_3^{\pm}(X)$ cubic fields for any bound X is due to Belabas [3], who was able to find all non-conjugate cubic fields of absolute discriminant bounded above by $X = 10^{11}$.

The cubic number field count for any *fixed* discriminant was established by Hasse [16]:

Theorem 1.1 ([16, Satz 7, p. 578]). *Let K be a quadratic number field of discriminant D, and r the 3-rank of the ideal class group of K. Then the number of non-conjugate cubic fields of discriminant D is $m = (3^r - 1)/2$.*

For example, the imaginary quadratic field $\mathbb{Q}(\sqrt{-4027})$ has 3-rank 2, so there are $m = (3^2-1)/2 = 4$ non-conjugate cubic fields of discriminant -4027. Unfortunately, Hasse's result is not constructive and therefore does not provide an efficient method of determining these m fields. Even Belabas' fast algorithm is impractical here: In order to find the m fields of discriminant D, his method must generate all cubic fields of absolute discriminant *up to* $|D|$, and this requires too many possible generating polynomials to be inspected.

A basic idea for constructing all cubic fields of a fixed square-free discriminant D goes back to Berwick [4]. The *dual* discriminant to D, defined to be $D' = -3D/\gcd(3, D)^2$, plays a crucial role here. Berwick's observation, expressed in modern terminology, was that every cubic field arises from a 3-*virtual unit* in the quadratic field $\mathbb{Q}(\sqrt{D'})$, i.e. a generator of a principal ideal that is the cube of some ideal. Suppose $\lambda = (A + B\sqrt{D'})/2$, with $A, B \in \mathbb{Z}$ non-zero, is a 3-virtual unit that is not itself a cube in $\mathbb{Q}(\sqrt{D'})$, but whose norm is a cube, say $\lambda\overline{\lambda} = Q^3$ with $Q \in \mathbb{Z}$. Then $F(Z) = Z^3 - 3QZ + A$ is the minimal polynomial of a cubic field of discriminant D or $-27D'$, and every cubic field of discriminant D can be obtained in this fashion. Moreover, two 3-virtual units $\lambda_1, \lambda_2 \in \mathbb{Q}(\sqrt{D'})$ give rise to the same triple of conjugate cubic fields if and only if one of the quotients λ_1/λ_2 or $\lambda_1/\overline{\lambda}_2$ is a cube in $\mathbb{Q}(\sqrt{D'})$. Cubic fields can therefore be constructed from quadratic 3-virtual units, or more exactly, via the ideal cube roots of such 3-virtual units. Care must be taken that this construction generates the complete collection of triples of conjugate cubic fields of discriminant D, that it generates each such field exactly once, and that any fields of discriminant $-27D'$ are detected and discarded.

A major problem with this technique is that the minimal polynomials thus produced can have extremely large coefficients, particularly when $D < 0$, in which case $\mathbb{Q}(\sqrt{D'})$ is a real quadratic field. In the late 1980s, Shanks showed how to circumvent this problem. Although he never published a complete account of his research in this direction, he did give talks [33, 35] about it and left behind an unfinished 52 page handwritten manuscript [34] which is in the possession of the last author. He also mentioned his work briefly in [36]. Shanks gave his technique the FORTRAN designator CUFFQI, an acronym derived from the phrase *Cubic Fields From Quadratic Infrastructure*.

In addition to Hasse's Theorem (Theorem 1.1), a second important result required for Shanks' method is due to Scholz [31], which establishes the relationship between the 3-ranks of the dual quadratic fields $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}(\sqrt{D'})$:

Theorem 1.2 (Scholz [31]). *Let D and D' be dual fundamental discriminants with $D < 0$, and let r and r' denote the respective 3-ranks of the ideal class groups of the imaginary quadratic field $\mathbb{Q}(\sqrt{D})$ and the real quadratic field $\mathbb{Q}(\sqrt{D'})$. Then $r = r'$ or $r = r' + 1$.*

The first of these two cases is called *non-escalatory*, whereas the second case is referred to as *escalatory* [37]. For example, recall that the imaginary quadratic field $\mathbb{Q}(\sqrt{-4027})$ has 3-rank 2. Its dual field $\mathbb{Q}(\sqrt{12081})$ has 3-rank 1; hence, this field belongs to the escalatory case.

Shanks' idea was to construct all the non-conjugate complex cubic fields of fundamental discriminant $D < 0$ by performing all the computations in the real quadratic field $\mathbb{Q}(\sqrt{D'})$. For example, the four non-conjugate cubic fields of discriminant $D = -4027$ can be constructed by performing the CUFFQI algorithm in the quadratic field $\mathbb{Q}(\sqrt{12081})$. The main ingredient required in the development of CUFFQI is what Shanks termed the *infrastructure* of an ideal class in a real quadratic field [32]. The key advantage of his method is that it produces minimal polynomials with small coefficients for all the cubic fields in question.

Shanks did not present his algorithm in a form which is suitable for implementation on a computer. This was done later by Fung [14]. Unfortunately, Fung's method was never published because Shanks wanted to publish his work on CUFFQI first (but never did). Evidence of the efficiency of Fung's version of CUFFQI is provided by his impressive (for the late 1980s) computation of all the non-conjugate complex cubic fields of the 19 digit discriminant $D = -3161659186633662283$. As Quer [23] had already determined that the 3-rank of $\mathbb{Q}(\sqrt{D})$ is 6, we know that there must be exactly $(3^6 - 1)/2 = 364$ such fields. Fung was able to find all of these fields in less than 3 CPU minutes on an Amdahl 5870 mainframe computer.

1.2. *Cubic function fields*

We now turn to the tasks of counting, constructing and tabulating cubic extensions of the rational function field $\mathbb{F}_q(t)$ where $\mathbb{F}_q$ is a finite field of characteristic at least 5. A class field theoretic approach was recently employed to construct all non-Galois cubic function fields of a fixed discriminant $D \in \mathbb{F}_q[t]$ [22], and subsequently their Galois counterparts [12]. These techniques compute the appropriate ray class group of $\mathbb{Q}(\sqrt{D})$, the class fields of all its index 3 subgroups, and finally, all their cubic subfields. Kummer theory was used in [45, 46] for constructing and tabulating a much more general class of function fields which in particular includes non-Galois cubics. The first of these two sources additionally generalized the technique of [22], and implementations in MAGMA established that it is significantly slower than the Kummer theoretic method. The Davenport–Heilbronn asymptotics [10, 11] were extended to arbitrary global base fields by Datskovsky and Wright [9]; their generalization includes in particular the case of cubic function fields. Belabas' tabulation technique [3] was successfully extended to cubic function fields in [26, 27, 29].

This paper presents a method for constructing small defining equations for all non-conjugate cubic function fields of a *fixed square-free* discriminant $D \in \mathbb{F}_q[t]$. It follows the same general ideas as outlined for cubic number fields in Sec. 1.1, but note that the function field scenario exhibits some subtle differences to the number field setting. In particular, our method distinguishes between *imaginary*, *unusual* and *real* quadratic function fields of discriminant D, according to whether D has odd degree, even degree with a non-square leading coefficient, or even degree with a square leading coefficient. Following Berwick and Shanks, all our computations are performed in the quadratic (i.e. hyperelliptic) function field $K' = \mathbb{F}_q(t, \sqrt{D'})$ where $D' = D/(-3)$, but note that in contrast to the number field situation, D' may define the same field as D here. When D' is imaginary, the computations are straightforward. When D' is unusual, our technique makes use of Artin's arithmetic [1] for unusual binary quadratic forms over $\mathbb{F}_q[t]$, adapted to quadratic ideals; this scenario has no number field analogue. Finally, when D' is real, we adapt Shanks' ideas and Fung's version of CUFFQI — both significantly streamlined — to function fields, performing arithmetic in infrastructures of the real quadratic function field K'.

The key to our construction is the relationship between cubic function fields of discriminant D and ideal classes of K' of order dividing 3. If K' is imaginary or unusual, then every ideal class of order 3, paired with its inverse, gives rise to a unique triple of conjugate cubic function fields of discriminant D. When the field is real, the principal class gives rise to one such triple, and every ideal class of order 3, again paired with its inverse, generates three such distinct triples. On input q and a square-free polynomial $D(t) \in \mathbb{F}_q[t]$, our algorithm outputs minimal polynomials for all triples of conjugate cubic function fields of discriminant D. It first computes a basis of the 3-torsion of the ideal class group of K' and, in the case when K' is real, the regulator of K'. When K' is imaginary or unusual, the method then obtains a reduced or (in the unusual setting) almost reduced representative in each basis ideal class. When K' is real, the technique identifies three suitable reduced ideals in each basis ideal class, along with one suitable reduced principal ideal; these ideals are carefully selected for computational suitability. Finally, the algorithm finds appropriately normalized generators of the cubes of all these reduced and almost reduced ideals. From the norm and trace in $K'/\mathbb{F}_q(t)$ of each of these generators, a certain monic irreducible cubic polynomial over $\mathbb{F}_q[t]$ can be easily derived. These polynomials define distinct triples of conjugate cubic function fields of discriminant D, and cover the entire collection of such fields.

Just as for CUFFQI, our method provides very small generating polynomials in all cases; "small" here refers to the fact that the degrees of the coefficients in $\mathbb{F}_q[t]$ of these polynomials are linearly bounded in the degree of the discriminant (and hence the genus) of the function field. Similar to the algorithm of [22], the bottleneck of our technique is class group computation. However, in addition to producing small minimal polynomials, our technique significantly outperforms the algorithms of [22, 45, 46].

In addition to our construction, we give a refined function field version of Hasse's Theorem and relate our field counts to this result; in fact, we provide exact expressions for the number of non-conjugate cubic function fields of discriminant D according to how the infinite place of $\mathbb{F}_q(t)$ splits in the cubic extension. In addition, we include a complexity analysis of our algorithms as well as numerical results generated using many of the quadratic function fields of high 3-rank identified in Bauer *et al.* in [2]; two large examples are provided in Appendix A. Finally, we compare the performance of our construction technique with that of the tabulation method for cubic function fields given in [27] — which also produces very small defining equations — showing definitively that our algorithm is more efficient for constructing fields of a single discriminant.

2. Preliminaries: Algebraic Function Fields

We begin by establishing notation and summarizing a few useful facts about algebraic function fields; see [25, 41] for sources on this subject.

2.1. *Algebraic function fields*

Let $\mathbb{F}_q$ be a finite field with q elements, $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$, and $k = \mathbb{F}_q(t)$ the field of rational functions in the variable t with coefficients in $\mathbb{F}_q$. For any non-zero $G \in \mathbb{F}_q[t]$, denote by $\deg(G)$ the degree of G, by $\operatorname{sgn}(G)$ the leading coefficient of G, and by $v_H(G)$ the highest power of H that divides G for any non-constant polynomial $H \in \mathbb{F}_q[t]$. The completion of k with respect to its infinite place is the field of Puiseux series over $\mathbb{F}_q$ in t^{-1}, denoted by $\mathbb{F}_q\langle t^{-1}\rangle$. Non-zero elements in this field have the form $\alpha = \sum_{i \le m} a_i t^i$, with $m = \deg(\alpha) \in \mathbb{Z}$, $a_i \in \mathbb{F}_q$ for $i \le m$, and $a_m = \operatorname{sgn}(\alpha) \neq 0$.

We generally write an algebraic function field in the form $M = k(x)$ where $F(t, x) = 0$ and $F(t, X) \in \mathbb{F}_q[t][X]$ is the minimal polynomial of x over k. We will always assume that $\mathbb{F}_q$ is the full constant field of M. Let $\Delta \in \mathbb{F}_q[t]$ denote the discriminant of F when considered as a polynomial in X, or equivalently, the discriminant of x. We assume that M/k is separable, so $\Delta \neq 0$. Then $\Delta = I^2D$ where $I \in \mathbb{F}_q[t]$ is the *index* of x in M and D is the discriminant of M/k; note that we will speak of *the* index and discriminant even though I and D are only unique up to non-zero constant factors. We have $I \in \mathbb{F}_q^*$ if and only if the curve $F(t, x) = 0$ is non-singular.

The maximal order $\mathcal{O}$ of M/k is the integral closure of $\mathbb{F}_q[t]$ in M/k, or equivalently, the set of functions in M that are regular at all finite places. We write (fractional) principal ideals of $\mathcal{O}$ as $\mathfrak{a} = (\alpha)$ with $\alpha \in M$ ($\alpha \in \mathcal{O}$ if $\mathfrak{a}$ is integral). Two non-zero ideals are *equivalent* if they differ by a factor that is a fractional principal ideal. Under ideal multiplication, the equivalence classes form the *ideal class group* of M/k, which is a finite abelian group whose order h is the *ideal class number* of K/k. For any ideal $\mathfrak{a}$ of $\mathcal{O}$, we denote by $[\mathfrak{a}]$ its ideal class. Henceforth, the term “ideal” will be assumed to be synonymous with non-zero integral ideal. An ideal of $\mathcal{O}$ is *primitive* if it is not contained in (or equivalently, not a multiple of) any principal ideal of $\mathcal{O}$ that is generated by a non-constant polynomial in $\mathbb{F}_q[t]$.

Let $\infty_1, \ldots, \infty_s$ be the infinite places of M/k, i.e. the poles of t. If e_i and f_i denote the ramification index and relative degree of ∞_i for $1 \leq i \leq s$, then the $2s$-tuple $(e_1, f_1; e_2, f_2; \ldots; e_s, f_s)$, with the pairs (e_i, f_i), $1 \leq i \leq s$ ordered lexicographically, is the *signature* of M/k. The group of units $\mathcal{O}^*$ of $\mathcal{O}$ is an infinite abelian group of rank $s - 1$ (the *unit rank* of M/k) whose torsion part is $\mathbb{F}_q^*$.

2.2. *Quadratic function fields*

A *quadratic* (or *hyperelliptic*) function field is a quadratic extension of $k = \mathbb{F}_q(t)$. If q is odd, which we henceforth assume, then every such extension is of the form $K = k(y)$ where $y^2 = D$ with $D(t) \in \mathbb{F}_q[t]$ non-constant. We may assume that D is square-free. Then the discriminant of K/k is D, and the genus of K is $g = \lfloor (\deg(D) - 1)/2 \rfloor$, so $\deg(D) = 2g + 1$ or $2g + 2$ depending on whether $\deg(D)$ is odd or even. The maximal order of K/k is $\mathcal{O} = k[t, y]$.

The extension K/k, or its discriminant D, are said to be *imaginary*, *unusual*, or *real*, according to whether $\deg(D)$ is odd, $\deg(D)$ is even and $\operatorname{sgn}(D)$ is a non-square in $\mathbb{F}_q$, or $\deg(D)$ is even and $\operatorname{sgn}(D)$ is a square in $\mathbb{F}_q$. The above terminology stems from quadratic number fields: imaginary and real quadratic function fields behave much like their number field counterparts in terms of their structure and arithmetic; in particular, they have signature $(2, 1)$ and $(1, 1; 1, 1)$, respectively (see for example [25, Proposition 14.6, p. 248]). Unusual quadratic function fields are of signature $(1, 2)$ and have no number field analogue; moreover, they become real when considered over a quadratic extension of $\mathbb{F}_q$. Referring to the decomposition of the infinite place of k in K, the three types of hyperelliptic function fields are also termed *ramified*, *inert* and *split*.

We point out that every imaginary quadratic function field K/k can be converted to a real quadratic extension of k, for example by virtue of a variable transformation of the form $t \to (t-a)^{-1}$ where $a \in \mathbb{F}_q$ with $D(a) \neq 0$. However, such a transformation obviously changes the discriminant. For the context of this paper, we will always assume that discriminants are given *a priori*.

If K/k is real, then the two infinite places of K yield two embeddings of K into the completion $\mathbb{F}_q\langle t^{-1}\rangle$. So if we fix $\operatorname{sgn}(y)$, then the notions of degree and sign are well-defined for elements in K. If ϵ is a fundamental unit of K/k, i.e. a generator of $\mathcal{O}^*/\mathbb{F}_q^*$, then $R = |\deg(\epsilon)|$ is the *regulator* of K/k; it is independent of the choice of fundamental unit. To facilitate a unified treatment, set $R = 1$ when K is not real. Then the degree zero divisor class number of K is the product hR/f where h is the ideal class number of K/k, $f = 2$ if K/k is unusual, and $f = 1$ otherwise (see [30] or [25, Proposition 14.1(b), p. 243]). The Hasse–Weil interval now yields the bounds

$$(\sqrt{q}-1)^{2g} \leq hR/f \leq (\sqrt{q}+1)^{2g}; \tag{2.1}$$

see [25, Proposition 5.11, p. 55].

For any $\alpha = a + by \in K$ $(a, b \in k)$, we write the conjugate of α as $\overline{\alpha} = a - by$, so the trace of α is $\operatorname{Tr}(\alpha) = \alpha + \overline{\alpha} = 2a$ and the norm of α is $N(\alpha) = \alpha\overline{\alpha} = a^2 - b^2 D$. The norm of an ideal $\mathfrak{a}$ of $\mathcal{O}$ is the unique monic polynomial $N(\mathfrak{a})$ with $\mathfrak{a}\overline{\mathfrak{a}} = (N(\mathfrak{a}))$ where $\overline{\mathfrak{a}} = \{\overline{\alpha} \,|\, \alpha \in \mathfrak{a}\}$ is the conjugate ideal of $\mathfrak{a}$. A primitive ideal $\mathfrak{a}$ of $\mathcal{O}$ is *reduced* if $\deg(N(\mathfrak{a})) \leq g$ and *almost reduced* if $\deg(N(\mathfrak{a})) = g + 1$. The number n of reduced ideals in each ideal class of K is finite and varies with the type of field. If K is imaginary, then $n = 1$ for every ideal class. If K is unusual, then $n = 0$ or 1, and ideal classes with $n = 0$ contain $q + 1$ equivalent almost reduced ideals [1]. For real fields K, the set of reduced ideals in any ideal class is referred to as the *infrastructure* of that class. Each infrastructure has a different cardinality n, but one always has $n \approx R$.

The following normalization on K^* will turn out to be useful later on.

Definition 2.1. An element $\alpha \in K^*$ is *normalized* if $\operatorname{sgn}(N(\alpha))$ is a cube in $\mathbb{F}_q^*$.

Note that if $q \equiv -1$ (3), then every element in K^* is normalized, since every element in $\mathbb{F}_q$ is a cube (the unique cube root of $a \in \mathbb{F}_q$ is $a^{(2q-1)/3}$).

Lemma 2.2. *If* $\alpha \in K^*$, *then* $\beta = \operatorname{sgn}(N(\alpha))\alpha$ *is normalized.*

Proof. $N(\beta) = \operatorname{sgn}(N(\alpha))^2 N(\alpha)$, so $\operatorname{sgn}(N(\beta)) = \operatorname{sgn}(N(\alpha))^3$. □

Lemma 2.2 implies in particular that every principal ideal of $\mathcal{O}$ has a normalized generator.

Definition 2.3 ([6, Definition 5.2.4, p. 231]). Let $n \in \mathbb{N}$ and $\mathfrak{a}$ an ideal of $\mathcal{O}$ whose nth power is principal. Then any generator λ of $\mathfrak{a}^n$ is an *n-virtual unit* of $\mathcal{O}$.

An n-virtual unit λ is *primitive*, *reduced*, or *almost reduced* if $\mathfrak{a}$ is primitive, reduced, or almost reduced, respectively.

Normalized primitive, and especially reduced or almost reduced, 3-virtual units will play a crucial role in our construction.

We conclude our discussion of quadratic extensions with a function field analogue of Scholz' Theorem (Theorem 1.2). Let D be unusual, $a \in \mathbb{F}_q^*$, $D' = a^{-1}D$, and $K' = k(y')$ with $(y')^2 = D'$. If a is a square in $\mathbb{F}_q$, then obviously $K = K'$, and the two hyperelliptic curves $y^2 = D(t)$ and $(y')^2 = D'(t)$ are isomorphic. If a is a non-square in $\mathbb{F}_q$, then D' and D are said to be *dual* discriminants, and K and K' are *dual* quadratic function fields. In this case, the hyperelliptic curve $y^2 = D(t)$ is the quadratic twist by a of the hyperelliptic curve $(y')^2 = D'(t)$. The following generalization of Scholz' Theorem (Theorem 1.2) to function fields is due to Rosen [24] and the second author [20]:

Theorem 2.4 ([20, Theorem 3.1], function field version of Theorem 1.2). *Let ℓ be an odd prime dividing $q+1, k = \mathbb{F}_q(t), K/k$ an unusual quadratic function field, and K'/k the corresponding dual real quadratic function field. If r and r' denote the respective ℓ-ranks of the ideal class groups of K/k and K'/k, then $r = r'$ or $r = r' + 1$. In the latter case, the regulator of K'/k is a multiple of ℓ.*

Analogous to quadratic number fields, the cases $r = r'+1$ and $r = r'$ are referred to as *escalatory* and *non-escalatory*, respectively.

2.3. *Cubic function fields*

Recall that $\mathbb{F}_q$ is a finite field of characteristic at least 5. A cubic equation of the form

$$z^3 - 3Qz + 2A = 0 \tag{2.2}$$

with $Q, A \in \mathbb{F}_q[t]$ has *quadratic resolvent* equation $x^2 - 2Ax + Q^3 = 0$. So any cubic equation (2.2) defines a unique unordered pair of elements $\{\lambda, \overline{\lambda}\}$ in some quadratic extension of k with $\lambda + \overline{\lambda} = 2A$ and $\lambda\overline{\lambda} = Q^3$, namely the roots of its resolvent polynomial. The roots $z^{(0)}, z^{(1)}, z^{(2)}$ of (2.2) are given by Cardano's well-known formula

$$z^{(i)} = u^i\delta + u^{-i}\overline{\delta} \qquad (i = 0, 1, 2), \tag{2.3}$$

where u is a primitive cube root of unity, $\delta^3 = \lambda$, $\overline{\delta}^3 = \overline{\lambda}$, and the cube roots are taken[a] so that $\delta\overline{\delta} = Q$. Over the extension $k(\lambda)$ of $k = \mathbb{F}_q(t)$, the quantities $z^{(i)}$ and $u^i\delta$ generate the same function field:

Proposition 2.5. *Let $K' = k(\lambda)$. Then $K'(u^i\delta) = K'(z^{(i)})$ for $i = 0, 1, 2$.*

[a] This still leaves three choices for the cube root δ of λ, but different choices for δ only lead to a different ordering of the roots $z^{(0)}, z^{(1)}, z^{(2)}$.

Proof. By (2.3), $z^{(i)} = u^i\delta + Q/u^i\delta \in k(u^i\delta) \subseteq K'(u^i\delta)$. On the other hand, $(u^i\delta)^2 - z^{(i)}(u^i\delta) + Q = 0$ and $(u^i\delta)^3 \in K' \subseteq K'(z^{(i)})$, so $u^i\delta$ satisfies both a quadratic and a cubic equation over $K'(z^{(i)})$, forcing $u^i\delta \in K'(z^{(i)})$. □

A *cubic function field* is a (separable) cubic extension of k. Assume henceforth that k has characteristic at least 5. Then every cubic function field can be written as $L = k(z)$ with z given by (2.2) and $F(Z) = Z^3 - 3QZ + 2A$ irreducible over k. The three cubic fields $L = k(z^{(0)})$, $L' = k(z^{(1)})$ and $L'' = k(z^{(2)})$ with $z^{(i)}$ given by (2.3) for $i = 0, 1, 2$ are *conjugate* cubic function fields.

The discriminant of $F(Z)$ is $\Delta = 108(Q^3 - A^2)$. Write $\Delta = (6B)^2D$ where D is the discriminant of L/k, and $6B \in \mathbb{F}_q[t]$ is the index of z in L. Then the roots λ and $\overline{\lambda}$ of the quadratic resolvent equation of (2.2) are given by $\lambda = A + By'$ and $\overline{\lambda} = A - By'$, where y' is a square root of $D' = D/(-3)$. If Δ is not constant and not a square in $\mathbb{F}_q[t]$, then $K' = k(\lambda) = k(y')$ is a quadratic function field, namely the resolvent field of L or its dual. In this case, the pair $\{\lambda, \overline{\lambda}\}$ of resolvent roots is said to be a pair of *quadratic generators* of the unordered triple of conjugate cubic function fields $\{L, L', L''\}$; see Berwick [4].

Equation (2.2) is said to be in *standard form* if no non-constant polynomial $G \in \mathbb{F}_q[t]$ satisfies $v_G(Q) \geq 2$ and $v_G(A) \geq 3$. It is easy to compute the discriminant D of L/k from the discriminant $\Delta = 108(Q^3 - A^2)$ of z as follows.

Proposition 2.6 ([18, Lemma 5.1], function field version of [21, Theorem 2]). *Let $L = k(z)$ be a cubic function field in standard form with z defined by* (2.2). *Set $\Delta = 108(Q^3 - A^2)$, and let D be the discriminant of L/k. Then any irreducible factor $P \in \mathbb{F}_q[t]$ of Δ satisfies*

$v_P(D) = 2$ *if and only if* $v_P(Q) \geq v_P(A) \geq 1$;
$v_P(D) = 1$ *if and only if* $v_P(\Delta)$ *is odd*;
$v_P(D) = 0$ *otherwise.*

We have the following signature characterization for cubic function fields:

Proposition 2.7 ([18, Corollary 7.4]). *Let $L = k(z)$ be a cubic function field with z defined by* (2.2). *Set $\Delta = 108(Q^3 - A^2)$, let u be a primitive cube root of unity, and let $\{\lambda, \overline{\lambda}\}$ be a pair of quadratic generators of $\{L, L', L''\}$. Then the signature of L/k is*

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

If $\deg(\lambda) = \deg(\overline{\lambda})$, then $\deg(\lambda) = 3\deg(Q)/2$ is divisible by 3. So signature $(3, 1)$ forces $\deg(\lambda) \neq \deg(\overline{\lambda})$, and hence

$$\deg(A^2) = 2\deg(\lambda + \overline{\lambda}) = 2\max\{\deg(\lambda), \deg(\overline{\lambda})\} > \deg(\lambda) + \deg(\overline{\lambda}) = \deg(Q^3).$$

Thus, $\operatorname{sgn}(\Delta) = \operatorname{sgn}(108A^2) = -3\operatorname{sgn}(6A)^2$, which immediately yields the following:

Corollary 2.8. *Let L/k be a cubic extension of discriminant D. Then the following hold*:

- *If D is imaginary, then L/k has signature* $(1, 1; 2, 1)$.
- *Suppose $q \equiv 1 \pmod 3$. Then*
  if D is unusual, then L/k has signature $(1, 1; 1, 2)$;
  if D is real, then L/k has signature $(1, 1; 1, 1; 1, 1)$ *or* $(1, 3)$ *or* $(3, 1)$.
- *Suppose $q \equiv -1 \pmod 3$. Then*
  if D is unusual, then L/k has signature $(1, 1; 1, 2)$ *or* $(3, 1)$;
  if D is real, then L/k has signature $(1, 1; 1, 1; 1, 1)$ *or* $(1, 3)$.

2.4. *Hasse's theorem for function fields*

It has long been known that there are strong ties between cubic and quadratic number fields. The same is true for cubic and quadratic function fields, as already evidenced by (2.3) and Corollary 2.8. A further connection is Hasse's Theorem (Theorem 1.1) which extends to function fields:

Theorem 2.9 (Function field version of Theorem 1.1). *Let $k = \mathbb{F}_q(t)$, K/k a quadratic extension of discriminant D and characteristic at least* 5, *and let r be the* 3*-rank of the ideal class group of K/k. Then the number of non-conjugate cubic function fields L/k of discriminant D and unit rank at least one is* $(3^r - 1)/2$.

Proof sketch. We only sketch the proof, as it proceeds analogously to Hasse's class field theoretic proof of Theorem 1.1, with some minor changes due to the adaptation to the function field scenario. Hasse proved in [16] that if K is a quadratic number field of discriminant D whose class group has 3-rank r, then the triples of conjugate cubic number fields of discriminant D are in one-to-one correspondence with the $(3^r - 1)/2$ distinct index 3 subgroups of the 3-torsion of the ideal class group of K. All these fields are contained in the Hilbert class field of K whose Galois group is the ideal class group of K.

The modifications in the function field proof arise from the slightly different definition of the Hilbert class field. The Hilbert class field of the quadratic function field K/k is the maximal unramified abelian extension H of K in some separable closure of K in which every infinite place of K splits completely; the last condition distinguishes the function field situation from the one for number fields and guarantees that H/K is a finite extension. Then we have the exact same correspondence between triples $\{L, L', L''\}$ of conjugate cubic function fields of discriminant D that are contained in H and index 3 subgroups of the 3-torsion of the ideal class group of K/k. However, not all cubic function fields of discriminant D are contained in H. More exactly, $L \subset H$ if and only if the Galois closure N of L is contained in H, which is the case if and only if every infinite place of K splits completely in N. By [19, Lemmas 2.2 and 2.3], these cubic function fields are exactly those with more than one infinite place. □

The Hasse count of $(3^r - 1)/2$ for cubic function fields does not include the fields with just one infinite place, i.e. those of unit rank zero. This scenario is impossible for cubic number fields as every irreducible cubic polynomial over the rationals has at least one real root. We provide a complete count for cubic function fields in Corollaries 4.3 and 4.5 below.

3. Quadratic Generators

The concept of quadratic generators as defined in Sec. 1.2 is a crucial ingredient for generating all triples of conjugate cubic function fields of a given square-free discriminant. So it is important to understand the exact relationship between cubic fields, quadratic generators, and the quadratic ideals they generate.

As before, let $\mathbb{F}_q$ be a finite field of characteristic at least 5, and set $k = \mathbb{F}_q(t)$. Fix a square-free non-constant polynomial $D \in \mathbb{F}_q[t]$, and let $D' = D/(-3)$. Define $K = k(y)$ and $K' = k(y')$ via $y^2 = D$ and $(y')^2 = D'$. Henceforth, all norms and traces are taken with respect to the extension K'/k. Let $\mathcal{O}'$ denote the maximal order of K'; we will only consider ideals of $\mathcal{O}'$.

For brevity, define the following four sets:

$$\begin{aligned}
\mathcal{L} &= \{\{L, L', L''\} \mid [L : k] = 3, L/k \text{ has discriminant } D\},\\
\mathcal{L}^* &= \{\{L, L', L''\} \in \mathcal{L} \mid L/k \text{ has unit rank at least } 1\},\\
\mathcal{I} &= \{\{[\mathfrak{a}], [\overline{\mathfrak{a}}]\} \mid \ \mathfrak{a} \text{ is an ideal of } \mathcal{O}' \text{ with } [\mathfrak{a}]^3 = [\mathcal{O}']\},\\
\mathcal{I}^* &= \mathcal{I} \backslash \{\{[\mathcal{O}'], [\mathcal{O}']\}\} = \{\{[\mathfrak{a}], [\overline{\mathfrak{a}}]\} \in \mathcal{I} \mid [\mathfrak{a}] \text{ has order } 3\}.
\end{aligned}$$

Then by Theorem 2.9, $\#\mathcal{L}^* = (3^r - 1)/2$, where r is the 3-rank of K/k. Furthermore by Corollary 2.8, $\mathcal{L}^* = \mathcal{L}$ if D is imaginary, or if D is unusual and $q \equiv 1 \pmod 3$, whereas $\mathcal{L}^* \subsetneq \mathcal{L}$ is possible otherwise.

In this section, we provide a description of quadratic generators as 3-virtual units, and characterize for each triple of fields $\{L, L', L''\} \in \mathcal{L}$ the complete collection of 3-virtual units that give rise to quadratic generators of $\{L, L', L''\}$. Later on, in Sec. 5, we devise methods for generating small 3-virtual units, which will in turn help to produce minimal polynomials with small coefficients for every triple of fields in $\mathcal{L}$. In Sec. 4, we determine the cardinality of $\mathcal{L}$, i.e. we refine the result of Theorem 2.9 to include totally inert and totally ramified cubic extensions. To achieve all this, we construct a map Φ from $\mathcal{L}$ to $\mathcal{I}$ in such a way that pre-images under Φ are explicitly computable via small quadratic generators. The map Φ will turn out to be a bijection onto $\mathcal{I}^*$ if D' is imaginary or unusual, and a surjection onto $\mathcal{I}$ that is three-to-one onto $\mathcal{I}^*$ and one-to-one onto the pair $\{[\mathcal{O}'], [\mathcal{O}']\}$ if D' is real. We can then generate all of $\mathcal{L}$ by simply computing the pre-images $\Phi^{-1}(\mathcal{I}^*)$ if D' is imaginary or unusual and $\Phi^{-1}(\mathcal{I})$ if D' is real. A straightforward counting argument, together with Theorem 2.9, will yield the exact number of triples in $\mathcal{L}$ of any given signature.

Theorem 3.1. *Let $\lambda \in \mathcal{O}'$. Then $\{\lambda, \overline{\lambda}\}$ is a pair of quadratic generators of a triple $\{L, L', L''\} \in \mathcal{L}$ in standard form if and only if λ is a normalized primitive* 3*-virtual unit of $\mathcal{O}'$ that is not a cube in $\mathcal{O}'$.*

Proof. Let $\{\lambda, \overline{\lambda}\}$ be a pair of quadratic generators of a triple $\{L, L', L''\} \in \mathcal{L}$. Write $L = k(z)$ with z given by (2.2) in standard form. Then $A \neq 0$ due to irreducibility, and $Q \neq 0$ by Proposition 2.6 as D is non-constant and square-free. Writing $\Delta = 108(Q^3 - A^2) = (6B)^2 D$, we have $\lambda = A + By'$ with $N(\lambda) = Q^3$, so λ is normalized.

To establish that λ generates the cube of a primitive ideal, set $G = \gcd(A, Q)$. We claim that

$$v_G(D) = v_G(Q) = v_G(B) = 1 < v_G(A). \tag{3.1}$$

To that end, let $P \in \mathbb{F}_q[t]$ be a prime divisor of G. Then $P \mid \Delta$, $v_P(A) \geq 1$ and $v_P(Q) \geq 1$. By Proposition 2.6, $v_P(Q) < v_P(A)$ as D is square-free. It follows that $v_P(Q) = 1$, as otherwise L is not in standard form. Thus, $v_P(G) = 1$ and $v_P(\Delta) = 3$ is odd. By Proposition 2.6, $v_P(D) = 1$. Also, $v_P(B) = (v_P(\Delta) - v_P(D))/2 = 1$, which proves (3.1).

Since $G \mid \gcd(A, B)$ by (3.1), it follows that $G \mid \lambda$. Consider the ideal $\mathfrak{a} = (Q, \lambda/G)$, i.e. the $\mathcal{O}'$-module generated by Q and λ/G. Then $\mathfrak{a}$ is primitive as $\gcd(Q, A/G, B/G) = 1$ by (3.1). Since $\lambda\overline{\lambda} = N(\lambda) = Q^3$, we see that $\mathfrak{a}\overline{\mathfrak{a}} = (Q)\mathfrak{b}$ where

$$\mathfrak{b} = (Q, \lambda/G, \overline{\lambda}/G, Q^2/G^2) = (Q, A/G, By'/G, Q^2/G^2).$$

Now (3.1) implies that $\gcd(Q, A/G, (Q/G)^2) = 1$, so $1 \in \mathfrak{b}$, and hence $\mathfrak{b} = \mathcal{O}'$. Thus, $N(\mathfrak{a}) = \operatorname{sgn}(Q)^{-1}Q$.

Note that $\lambda^2 = A^2 + B^2D' + ABy'$ is a multiple of G^3. Thus, $\mathfrak{a}^3 = (\lambda)\mathfrak{c}$ where $\mathfrak{c} = (\overline{\lambda}, Q^2/G, Q\lambda/G^2, \lambda^2/G^3)$. Since $(N(\mathfrak{a})^3) = (Q^3) = (N(\lambda))$, we see that $\mathfrak{c} = \mathcal{O}'$, so $(\lambda) = \mathfrak{a}^3$ with $\mathfrak{a}$ a primitive ideal of $\mathcal{O}'$.

Finally, let δ be a cube root of λ. If λ were a cube in $\mathcal{O}'$, then $u^i\delta \in \mathcal{O}'$ for some $i \in \{0, 1, 2\}$. It would follow from Proposition 2.5 that $K' = K'(u^i\delta) = K'(z^{(i)})$, so $z^{(i)} \in K' \cap k(z^{(i)}) = k$, contradicting $[L : k] = 3$.

Conversely, let λ be a normalized 3-virtual unit of $\mathcal{O}'$ that is not a cube in $\mathcal{O}'$. Write $\lambda = A + By'$ with $A, B \in \mathbb{F}_q[t]$, and write $(\lambda) = \mathfrak{a}^3$ where $\mathfrak{a}$ is a primitive ideal. Then $N(\lambda) = aN(\mathfrak{a})^3$ for some $a \in \mathbb{F}_q^*$. Since λ is normalized and $N(\mathfrak{a})$ is monic, a is a cube in $\mathbb{F}_q^*$, so $N(\lambda) = Q^3$ for some non-zero $Q \in \mathbb{F}_q[t]$. Note that $B \neq 0$, as otherwise $\lambda = \lambda^3/\lambda^2 = \lambda^3/N(\lambda) = (A/Q)^3$ is a cube in $\mathbb{F}_q(t)$, which would force it to be a cube in $\mathcal{O}'$.

Set $F(Z) = Z^3 - 3QZ + 2A \in \mathbb{F}_q[t]$. Then $F(Z)$ has discriminant $\Delta = 108(Q^3 - A^2) = (6B)^2 D$. By (2.3), $F(Z)$ has a zero $z = \delta + \overline{\delta}$, where $\delta^3 = \lambda$, $\overline{\delta}^3 = \overline{\lambda}$, and $\delta\overline{\delta} = Q$. Since δ is a root of the polynomial $G(T) = (T^3 - \lambda)(T^3 - \overline{\lambda}) = T^6 - 2AT^3 + Q^3 \in \mathbb{F}_q[t, T]$, it is integral over $\mathbb{F}_q[t]$. Thus, $\delta \notin K'$, as otherwise $\delta \in \mathcal{O}'$, contradicting the fact that λ is not a cube in $\mathcal{O}'$. It follows that $[K'(\delta) : K'] = 3$, so $[K'(z) : K'] = 3$ by Proposition 2.5.

Now z is a zero of the monic cubic polynomial $F(Z) \in K'[Z]$, which must therefore be the minimal polynomial of z over K'. So $F(Z)$ is irreducible over K' and hence over k. It follows that $F(Z)$ is the minimal polynomial of a cubic extension $L = k(z)$ where z satisfies (2.2). To see that F is in standard form, suppose by way of contradiction that there exists an irreducible polynomial $P \in \mathbb{F}_q[t]$ with $P^2 \mid Q$ and $P^3 \mid A$. Then $P^6 \mid A^2 - Q^3 = B^2 D'$, so $P^5 \mid B^2$ since D' is square-free, and hence $P^3 \mid B$. Thus, $P^3 \mid \lambda$. Since $(\lambda) = \mathfrak{a}^3$, P must divide $\mathfrak{a}$, contradicting the fact that $\mathfrak{a}$ is primitive.

It remains to show that L/k has discriminant D, which is the square-free kernel of Δ. Let d be the discriminant of L/k. Then $d \mid \Delta = (6B)^2 D$, so D is also the square-free kernel of d. By way of contradiction, suppose that there exists a prime polynomial $P \in \mathbb{F}_q[t]$ with $v_P(d) \geq 2$. Then $P \mid B$ as D is square-free. By Proposition 2.6, $v_P(d) = 2$ and $v_P(Q) \geq v_P(A) \geq 1$. It follows that $P \mid \lambda$.

Since d/D is a square and $v_P(d) = 2$, P cannot divide D. Hence, P cannot divide D' and thus does not ramify in K'. If P is inert in $\mathcal{O}'$, then $P \mid (\lambda) = \mathfrak{a}^3$ implies $P \mid \mathfrak{a}$, contradicting the fact that $\mathfrak{a}$ is primitive. If P splits in $\mathcal{O}'$, say $(P) = \mathfrak{p}\overline{\mathfrak{p}}$ with $\mathfrak{p}, \overline{\mathfrak{p}}$ conjugate prime ideals in $\mathcal{O}'$, then $\mathfrak{p}, \overline{\mathfrak{p}} \mid \mathfrak{a}^3$ implies $\mathfrak{p}, \overline{\mathfrak{p}} \mid \mathfrak{a}$. Since $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ are coprime, $(P) = \mathfrak{p}\overline{\mathfrak{p}} \mid \mathfrak{a}$, again contradicting the fact that $\mathfrak{a}$ is primitive.

So we conclude that d is square-free, and hence $d = D$ up to a constant square factor. It follows that L/k has discriminant D, and so $\{\lambda, \overline{\lambda}\}$ is a pair of quadratic generators of $\{L, L', L''\} \in \mathcal{L}$. □

Next, we investigate under what conditions different pairs of quadratic generators correspond to the same triple of fields in $\mathcal{L}$.

Theorem 3.2. *For $j = 1, 2$, let $\{\lambda_j, \overline{\lambda}_j\}$ be a pair of quadratic generators of a triple $\{L_j, L'_j, L''_j\} \in \mathcal{L}$. Then $\{L_1, L'_1, L''_1\} = \{L_2, L'_2, L''_2\}$ if and only if $\lambda_1 = \alpha^3 \lambda_2$ or $\lambda_1 = \alpha^3 \overline{\lambda}_2$ for some non-zero $\alpha \in K'$.*

Proof. For $j = 1, 2$, write $L_j = k(z_j)$ with $z_j^3 - 3Q_j z_j + 2A_j = 0$, and let $z_j^{(i)}$ be the conjugates of z_j for $i = 0, 1, 2$. By (2.3), $z_j^{(i)} = u^i \delta_j + u^{-i} \overline{\delta}_j$ where u is a primitive cube root of unity, $\delta_j^3 = \lambda_j$, $\overline{\delta}_j^3 = \overline{\lambda}_j$, and $\delta_j \overline{\delta}_j = Q_j \in \mathbb{F}_q[t]$.

Suppose first that $\{L_1, L'_1, L''_1\} = \{L_2, L'_2, L''_2\}$, so $L_1 = k(z_2^{(i)})$ for some $i \in \{0, 1, 2\}$. Then $K'(z_1) = K'(z_2^{(i)})$, and hence $K'(\delta_1) = K'(u^i \delta_2)$ by Proposition 2.5. It follows that $\delta_1 \in K'(u^i \delta_2)^3$. Also $\delta_1^3 = \lambda_1 \in K'$ and $(u^i \delta_2) = \lambda_2 \in K'$. Standard results on generators of radical extensions now force $\delta_1 = \beta u^i \delta_2$ or $\delta_1 = \beta (u^i \delta_2)^2$

for some $\beta \in K'$. In the former case, $\lambda_1 = \beta^3\lambda_2$; in the latter case, $\lambda_1 = \beta^3\lambda_2^2 = (\beta\lambda_2/Q_2)^3\,\overline{\lambda}_2$.

Conversely, suppose that $\lambda_1 = \alpha^3\lambda_2$ or $\lambda_1 = \alpha^3\overline{\lambda_2}$ for some non-zero $\alpha \in K'$. Then $\delta_1 = u^i\alpha\delta_2$ or $\delta_1 = \alpha u^i\overline{\delta}_2 = \alpha Q/u^{-i}\delta_2$. It follows that $K'(\delta_1) = K'(u^i\delta_2)$ for some $i \in \{0,1,2\}$. By Proposition 2.5, $K'(z_1) = K'(z_2^{(i)})$. Intersecting both sides with L_1 shows that $L_1 \subseteq K'(z_2^{(i)})$. Now $K'(z_2^{(i)})$ is an extension of degree at most 6 over k that contains the cubic extension L_1/k, which forces $[K'(z_2^{(i)}) : L_1] \leq 2$. So $z_2^{(i)}$ is at most quadratic over L_1 and is also a root of the cubic polynomial $F_2(Z) = Z^3 - 3Q_2Z + 2A_2 \in L_1[Z]$. It follows that $z_2^{(i)} \in L_1$, and hence $k(z_2^{(i)}) \subseteq L_1$. Since both extensions are cubic over k, they must be equal, so $\{L_1, L_1', L_1''\} = \{L_2, L_2', L_2''\}$. □

Corollary 3.3. *For $j = 1, 2$, let $\{\lambda_j, \overline{\lambda}_j\}$ be two pairs of quadratic generators of a triple $\{L, L', L''\} \in \mathcal{L}$, and let $\mathfrak{a}_j$ be the primitive ideal in $\mathcal{O}'$ such that $(\lambda_j) = \mathfrak{a}_j^3$. Then $\mathfrak{a}_1$ is equivalent to $\mathfrak{a}_2$ or $\overline{\mathfrak{a}}_2$.*

Proof. By Theorem 3.2, we have $\mathfrak{a}_1 = (\alpha)\mathfrak{a}_2$ or $\mathfrak{a}_1 = (\alpha)\overline{\mathfrak{a}}_2$ for some non-zero $\alpha \in K'$. □

4. Count of Cubic Fields of Discriminant D by Signature

In this section, we determine the cardinality of $\mathcal{L}$, and count the number of triples in $\mathcal{L}$ by signature. Consider the map

$$\Phi : \mathcal{L} \to \mathcal{I} \text{ via } \{L, L', L''\} \mapsto \{[\mathfrak{a}], [\overline{\mathfrak{a}}]\},$$

where $(\lambda) = \mathfrak{a}^3$ for some pair $\{\lambda, \overline{\lambda}\}$ of quadratic generators of $\{L, L', L''\}$. Then Φ is well-defined, because if $\{[\mathfrak{a}], [\overline{\mathfrak{a}}]\}, \{[\mathfrak{b}], [\overline{\mathfrak{b}}]\} \in \mathcal{I}$ such that $\mathfrak{a}^3 = (\lambda)$, $\mathfrak{b}^3 = (\mu)$ and both $\{\lambda, \overline{\lambda}\}$ and $\{\mu, \overline{\mu}\}$ are pairs of quadratic generators of the same triple of fields in $\mathcal{L}$, then $\mathfrak{b}$ is equivalent to $\mathfrak{a}$ or $\overline{\mathfrak{a}}$ by Corollary 3.3, so $\{[\mathfrak{b}], [\overline{\mathfrak{b}}]\} = \{[\mathfrak{a}], [\overline{\mathfrak{a}}]\}$.

We will prove that Φ is a bijection onto $\mathcal{I}^*$ if D' is imaginary or unusual. When D' is real, we will see that Φ is a three-to-one map onto $\mathcal{I}^*$ and one-to-one onto the principal class pair $\{[\mathcal{O}'], [\mathcal{O}']\}$.

Lemma 4.1. *Suppose that D' is imaginary or unusual. Then the following hold*:

(1) *No element of $\mathcal{L}$ maps to the pair $\{[\mathcal{O}'], [\mathcal{O}']\}$ under Φ.*
(2) *If $[\mathfrak{a}]$ is any ideal class of $\mathcal{O}'$ of order* 3, *then the pre-image of the pair $\{[\mathfrak{a}], [\overline{\mathfrak{a}}]\} \in \mathcal{I}^*$ under Φ contains exactly one element.*

Proof. Every normalized generator λ of $\mathcal{O}'$ belongs to $(\mathcal{O}')^* = \mathbb{F}_q^*$, so $\lambda^2 = \operatorname{sgn}(N(\lambda))$ is a cube in $\mathbb{F}_q^*$. Then $\lambda = \lambda^3/\lambda^2$ is itself a cube in $\mathbb{F}_q^*$. The result of part (1) now follows from Theorem 3.1.

For part (2), assume without loss of generality that $\mathfrak{a}$ is primitive, and let λ be a normalized generator of $\mathfrak{a}^3$. Then λ is not a cube in $\mathcal{O}'$ as $\mathfrak{a}$ is non-principal.

By Theorem 3.1, $\{\lambda, \overline{\lambda}\}$ is a pair of quadratic generators of some triple of fields $\{L, L', L''\}$ in the pre-image of $\{[\mathfrak{a}], [\overline{\mathfrak{a}}]\}$ under Φ.

To see that this triple of fields is unique, let $\{M, M', M''\}$ be another triple of fields in $\mathcal{L}$ that maps to $\{[\mathfrak{a}], [\overline{\mathfrak{a}}]\}$ under Φ, with a pair of quadratic generators $\{\mu, \overline{\mu}\}$. By Theorem 3.1, μ is normalized. Write $(\mu) = \mathfrak{b}^3$ with $\mathfrak{b} \in [\mathfrak{a}]$, and let $\alpha \in K'$ with $\mathfrak{b} = (\alpha)\mathfrak{a}$. Then $\mu = \eta\alpha^3\lambda$ for some $\eta \in (\mathcal{O}')^* = \mathbb{F}_q^*$. Since μ and λ are normalized, η is a cube in $\mathbb{F}_q^*$. By Theorem 3.2, $\{M, M', M''\} = \{L, L', L''\}$. □

Lemma 4.2. *Suppose that D' is real. Then the following hold*:

(1) *The pre-image of the pair $\{[\mathcal{O}'], [\mathcal{O}']\}$ under Φ contains exactly one element.*
(2) *If $[\mathfrak{a}]$ is any ideal class of $\mathcal{O}'$ of order 3, then the pre-image of the pair $\{[\mathfrak{a}], [\overline{\mathfrak{a}}]\} \in \mathcal{I}^*$ under Φ contains exactly three elements.*

Proof. Let ϵ be a normalized fundamental unit of K'. Then by Theorem 3.1, $\{\epsilon, \overline{\epsilon}\}$ is a pair of quadratic generators of some triple of fields $\{L, L', L''\}$ in the pre-image of $\{[\mathcal{O}'], [\mathcal{O}']\}$ under Φ.

Let $\{M, M', M''\}$ be another triple of fields in $\mathcal{L}$ that maps to $\{[\mathcal{O}'], [\mathcal{O}']\}$ under Φ, with a pair of quadratic generators $\{\mu, \overline{\mu}\}$. By Theorem 3.1, μ is normalized and not a cube in $\mathcal{O}'$. Write $(\mu) = \mathfrak{b}^3$ for some $\mathfrak{b} \in [\mathcal{O}']$, and let α be a generator of $\mathfrak{b}$. Then $\mu = a\epsilon^i\alpha^3$ with $a \in \mathbb{F}_q^*$ and $i \in \mathbb{Z}$. Since μ and ϵ are normalized, a is a cube in $\mathbb{F}_q^*$. Without loss of generality, set $a = 1$. Also, since μ is not a cube in $\mathcal{O}'$, i cannot be divisible by 3. If $i \equiv 1 \pmod 3$, then $\mu = (\alpha\epsilon^{(i-1)/3})^3\epsilon$, and if $i \equiv 2 \pmod 3$, then $\mu = N(\epsilon)^{-1}(\alpha\epsilon^{(i+1)/3})^3\overline{\epsilon}$. Noting that $N(\epsilon)$ is a cube in $\mathbb{F}_q^*$, we obtain $\{M, M', M''\} = \{L, L', L''\}$ by Theorem 3.2. This proves part (1).

Part (2) uses the same reasoning as in the proof of Lemma 4.1 to establish that $\Phi^{-1}(\{[\mathfrak{a}], [\overline{\mathfrak{a}}]\})$ is non-empty and thus contains some triple $\{L, L', L''\} \in \mathcal{L}$ with a pair of quadratic generators $\{\lambda, \overline{\lambda}\}$.

Let $\{M, M', M''\}$ be another triple of fields in $\mathcal{L}$ that maps to $\{[\mathfrak{a}], [\overline{\mathfrak{a}}]\}$ under Φ, with a pair of quadratic generators $\{\mu, \overline{\mu}\}$. Then $(\mu) = \mathfrak{b}^3$ for some $\mathfrak{b} \in [\mathfrak{a}]$. Write $\mathfrak{b} = (\alpha)\mathfrak{a}$ with $\alpha \in \mathcal{O}'$. Then $\mu = a\epsilon^i\alpha^3\lambda$ for some $a \in \mathbb{F}_q^*$ and $i \in \mathbb{Z}$ where ϵ is a normalized fundamental unit of K'. As before, we may again assume that $a = 1$.

Now $\epsilon^i\alpha^3\lambda$ and $\epsilon^j\alpha^3\lambda$ differ by a factor that is a cube in K' if and only if ϵ^{i-j} is a cube in K', which can only happen if $i \equiv j \pmod 3$ since ϵ is a fundamental unit. Also $\epsilon^i\alpha^3\lambda$ and $\overline{\epsilon}^j\overline{\alpha}^3\overline{\lambda}$ cannot differ by a factor that is a cube in K', as otherwise $\mathfrak{a}$ and $\overline{\mathfrak{a}}$ would be equivalent ideals, contradicting the assumption that $[\mathfrak{a}]$ has order 3.

So the pairs of quadratic generators of every triple of fields $\{L_i, L_i', L_i''\} \in \Phi^{-1}(\{[\mathfrak{a}], [\overline{\mathfrak{a}}]\})$ are of the form $\{\mu_i, \overline{\mu}_i\}$ where $\mu_i = \epsilon^i\alpha_i^3\lambda$ with $\alpha_i \in \mathcal{O}'$ and $i \in \{0, 1, 2\}$. By Theorem 3.2, $\{L_0, L_0', L_0''\} = \{L, L', L''\}$, and the triples $\{L_i, L_i', L_i''\}$ are pairwise distinct for $i = 0, 1, 2$. □

Corollary 4.3. *Let r' denote the 3-rank of the ideal class group of K'/k. If D' is imaginary or unusual, then $\#\mathcal{L} = (3^{r'} - 1)/2$. If D' real, then $\#\mathcal{L} = (3^{r'+1} - 1)/2$.*

Proof. Using Lemma 4.1, this statement follows from the fact that the class group of K'/k has $(3^{r'}-1)/2$ pairs of distinct conjugate ideal classes of order 3, and from the simple calculation $3\cdot(3^{r'}-1)/2+1=(3^{r'+1}-1)/2$. □

Corollary 4.4. *Let r and r' denote the respective 3-ranks of the ideal class groups of K/k and K'/k. If D is imaginary, or D is unusual and $q \equiv 1 \pmod 3$, then $r = r'$.*

Proof. By Theorem 2.9, $\#\mathcal{L}^* = (3^r-1)/2$, and by Corollary 4.3, $\#\mathcal{L} = (3^{r'}-1)/2$. Finally, if D is imaginary, or D is unusual and $q \equiv 1 \pmod 3$, then $\mathcal{L} = \mathcal{L}^*$ by Corollary 2.8. □

We can now determine the exact number of triples in $\mathcal{L}$ of any given signature in terms of the 3-rank of K, which is more natural than expressing it in terms of the 3-rank of K'. The following is a refinement of Theorem 2.9.

Corollary 4.5. *Let r denote the 3-rank of the ideal class group of K/k.*

- *If D is imaginary, then all $(3^r-1)/2$ triples of conjugate cubic fields of discriminant D have signature $(1,1;2,1)$; no other signatures occur.*
- *If D is unusual, then the following hold:*
  - *If $q \equiv 1 \pmod 3$, then all $(3^r-1)/2$ triples of conjugate cubic fields of discriminant D have signature $(1,1;1,2)$; no other signatures occur.*
  - *If $q \equiv -1 \pmod 3$, in the escalatory case, all $(3^r-1)/2$ triples of conjugate cubic fields of discriminant D have signature $(1,1;1,2)$; no other signatures occur.*
  - *If $q \equiv -1 \pmod 3$, in the non-escalatory case, $(3^r-1)/2$ triples of conjugate cubic fields of discriminant D have signature $(1,1;1,2), 3^r$ such triples have signature $(3,1)$, and no other signatures occur.*
- *If D is real, then the following hold:*
  - *If $q \equiv 1 \pmod 3$, then $(3^r-1)/2$ triples of conjugate cubic fields of discriminant D have signature $(1,1;1,1;1,1), 3^r$ such triples have signature $(1,3)$ or $(3,1))$, and no other signatures occur.*
  - *If $q \equiv -1 \pmod 3$, in the escalatory case, $(3^r-1)/2$ triples of conjugate cubic fields of discriminant D have signature $(1,1;1,1;1,1), 3^r$ such triples have signature $(1,3)$, and no other signatures occur.*
  - *If $q \equiv -1 \pmod 3$, in the non-escalatory case, all $(3^r-1)/2$ triples of conjugate cubic fields of discriminant D have signature $(1,1;1,1;1,1)$; no other signatures occur.*

Proof. If D is imaginary, or D is unusual and $q \equiv 1 \pmod 3$, then the claim is a simple consequence of Corollaries 2.8 and 4.4 together with Theorem 2.9.

Assume now that D is unusual and $q \equiv -1 \pmod 3$, so D' is real. In the escalatory case, $r = r'+1$, so by Corollary 4.3, $\#\mathcal{L} = (3^r-1)/2 = \#\mathcal{L}^*$, and the only possible signature is $(1, 1; 1, 2)$ by Corollary 2.8. In the non-escalatory case, $r = r'$ and hence $\#(\mathcal{L}\backslash\mathcal{L}^*) = (3^{r+1} - 1)/2 - (3^r - 1)/2 = 3^r$. By Corollary 2.8, $(3^r - 1)/2$ of the triples of fields in $\mathcal{L}$ have signature $(1, 1; 1, 2)$ and the remaining 3^r triples have signature $(3, 1)$.

Next, assume that D is real. If $q \equiv 1 \pmod 3$, then D' is real and $r = r'$. So as before, $\#\mathcal{L} = (3^{r+1} - 1)/2$ and $\#\mathcal{L}^* = (3^r - 1)/2$. By Corollary 2.8, the $(3^r - 1)/2$ elements in $\mathcal{L}^*$ have signature $(1, 1; 1, 1; 1, 1)$ and the remaining 3^r elements in $\mathcal{L}\backslash\mathcal{L}^*$ have signature $(1, 3)$ or $(3, 1)$.

Finally, assume that D is real and $q \equiv -1 \pmod 3$, so D' is unusual. In the escalatory case, $r' = r + 1$. So $\#\mathcal{L} = (3^{r+1} - 1)/2$, in which case there are once again 3^r elements in $\mathcal{L}$ outside $\mathcal{L}^*$. The possible signatures can again be inferred from Corollary 2.8. In the non-escalatory case, $r = r'$, so $\#\mathcal{L} = \#\mathcal{L}^*$, and the only possible signature permitted by Corollary 2.8 is $(1, 1; 1, 1; 1, 1)$. □

5. Small 3-Virtual Units

The proof of part (1) of Lemma 4.2 revealed that when D' is real, a normalized fundamental unit ϵ of K' produces the triple of fields in $\mathcal{L}$ that maps to the principal class pair under Φ. The proof of part (2) was similarly constructive: if $[\mathfrak{a}]$ is an ideal class of order 3 and λ any normalized generator of $\mathfrak{a}^3$, then the three elements $\lambda, \epsilon\lambda, \epsilon^2\lambda \in \mathcal{O}'$ give rise to the three triples in the pre-image of the pair $\{[\mathfrak{a}], [\overline{\mathfrak{a}}]\} \in \mathcal{I}^*$ under Φ. From a computational point of view, however, these generators tend to be very poor choices to represent a triple of fields since they are generally very large. For example, the constant coefficient in the minimal polynomial $F(Z) = Z^3 - 3N(\epsilon)Z + \mathrm{Tr}(\epsilon)$ has degree R, the regulator of K'. If K'/k has small ideal class group, which is typically the case [13], then this degree is exponentially large in the size of D by (2.1).

This section is devoted to finding small 3-virtual units of $\mathcal{O}'$ that are not cubes in $\mathcal{O}'$. "Small" here means that their norm and trace, or equivalently, their coefficients in $\mathbb{F}_q[t]$ with respect to 1 and y', have small degree. By virtue of Theorem 3.1, after suitable normalization, these 3-virtual units give rise to defining equations (2.2) for each triple of fields in $\mathcal{L}$ whose coefficients Q and A have low degree.

More specifically, for each ideal class $[\mathfrak{a}]$ of order dividing 3, with $\mathfrak{a}$ non-principal if D' is imaginary or unusual, we first find one ideal (if D is imaginary or unusual) or three ideals (if D' is real) in $[\mathfrak{a}]$ whose cubes have small generators that are not themselves cubes in $\mathcal{O}'$, and then find these generators λ. Then the pairs $\{\lambda, \overline{\lambda}\}$ represent pairs of small quadratic generators for every triple of fields in the pre-image of $\{[\mathfrak{a}], [\overline{\mathfrak{a}}]\}$ under Φ, so this process enumerates all of $\mathcal{L}$. For D' imaginary or unusual, the procedure turns out to be straightforward. However, when D' is real, the computations become significantly more complicated; this is where infrastructures come to the rescue. Before we provide an explicit description of the algorithms involved, we summarize the necessary basic facts about ideals in quadratic function fields and their arithmetic; for details, consult [17].

5.1. *Ideal arithmetic in quadratic function fields*

Let K'/k be a quadratic function field of discriminant D' and genus $g = \lfloor(\deg(D')-1)/2\rfloor$, with maximal order $\mathcal{O}'$. If K' is real, then fix a normalized fundamental unit of ϵ of K'/k of positive degree, so $N(\epsilon)$ is a cube in $\mathbb{F}_q^*$ and $R = \deg(\epsilon)$ is the regulator of K'/k.

Primitive ideals $\mathfrak{a}$ of $\mathcal{O}'$ are $\mathbb{F}_q[t]$-modules of rank 2 and will always be represented in terms of an $\mathbb{F}_q[t]$-basis $\{Q, P+y'\}$ with $Q, P \in \mathbb{F}_q[t]$. Here $Q = N(\mathfrak{a})$, $Q \mid D' - P^2$ and P is unique modulo Q. Note that $\overline{\mathfrak{a}}$ has $\mathbb{F}_q[t]$-basis $\{Q, -P+y'\}$.

For any two equivalent ideals $\mathfrak{a}, \mathfrak{b}$ of $\mathcal{O}'$, a (*relative*) *generator of* $\mathfrak{b}$ *with respect to* $\mathfrak{a}$ is an element $\theta \in K'$ with $\mathfrak{b} = (\theta)\mathfrak{a}$; for $\mathfrak{a} = \mathcal{O}'$, this is simply a generator of $\mathfrak{b}$. If K' is real and $0 \leq \deg(\theta) < R$, then θ is a *minimal non-negative* generator of $\mathfrak{b}$ with respect to $\mathfrak{a}$. Given any primitive ideal $\mathfrak{a}$ of $\mathcal{O}'$, an iterative *reduction* procedure produces a specific ideal $\mathfrak{r}$ equivalent to $\mathfrak{a}$ and a relative generator θ of $\mathfrak{r}$ with respect to $\mathfrak{a}$. Here, $\mathfrak{r}$ is the unique reduced ideal in $[\mathfrak{a}]$ if D' is imaginary, the unique reduced ideal or any of the $q+1$ almost reduced ideals in $[\mathfrak{a}]$ is D' is unusual, and the first reduced ideal in $[\mathfrak{a}]$ obtained through the iterative reduction procedure if D' is real. This can be accomplished efficiently using for example one of the reduction methods described in [17], and requires $O(g \max\{g, \deg(N(\mathfrak{a}))\})$ operations[b] in $\mathbb{F}_q$. If the ideal $\mathfrak{a}$ is the primitive part of the product of two reduced or almost reduced ideals $\mathfrak{r}_1$ and $\mathfrak{r}_2$, then the process of computing $\mathfrak{r}$ and θ from $\mathfrak{r}_1$ and $\mathfrak{r}_2$ is called a *giant step* and requires $O(g^2)$ operations in $\mathbb{F}_q$.

For the remainder of Sec. 5.1, assume that K'/k is real, and recall that the collection of reduced ideals in any ideal class comprises the *infrastructure* of that class. For two equivalent reduced ideals $\mathfrak{a}, \mathfrak{b}$, the *distance* from $\mathfrak{a}$ to $\mathfrak{b}$ is $\delta(\mathfrak{b}, \mathfrak{a}) = \deg(\theta)$ where θ is a minimal non-negative generator of $\mathfrak{b}$ with respect to $\mathfrak{a}$. Distances exhibit a number of symmetries; specifically, $\delta(\mathfrak{b}, \mathfrak{a}) = \delta(\overline{\mathfrak{a}}, \overline{\mathfrak{b}})$, and $\delta(\mathfrak{b}, \mathfrak{a}) = R - \delta(\mathfrak{a}, \mathfrak{b})$ when $\mathfrak{a} \neq \mathfrak{b}$. The distance gives rise to an ordering of the ideals in the infrastructure of $\mathfrak{a}$ via increasing distance from $\mathfrak{a}$. A *baby step* generates from any reduced ideal $\mathfrak{b}$ the next ideal $\mathfrak{b}_+$ in this ordering in a cyclic fashion, along with the distance advance $\delta(\mathfrak{b}_+, \mathfrak{b})$, or alternatively, a generator of $\mathfrak{b}_+$ with respect to $\mathfrak{b}$. We have $1 \leq \delta(\mathfrak{b}_+, \mathfrak{b}) \leq g$ for $\mathfrak{b} \neq \mathcal{O}'$, and $\delta(\mathcal{O}'_+, \mathcal{O}') = g+1$. In particular, this implies the lower bound $R \geq g+1$. A baby step requires $O(g)$ operations in $\mathbb{F}_q$.

For any integer N with $0 \leq N < R$ and any reduced ideal $\mathfrak{a}$, the *reduced ideal below* N *with respect to* $\mathfrak{a}$ is the reduced ideal $\mathfrak{b} \in [\mathfrak{a}]$ with $\delta(\mathfrak{b}, \mathfrak{a}) \leq N < \delta(\mathfrak{b}_+, \mathfrak{a})$. Clearly, $0 \leq N - \delta(\mathfrak{b}, \mathfrak{a}) \leq g$. The *reduced ideal closest to* N *with respect to* $\mathfrak{a}$ is the reduced ideal $\mathfrak{b} \in [\mathfrak{a}]$ with $|\delta(\mathfrak{b}, \mathfrak{a}) - N|$ minimal (with ties between $\mathfrak{b}$ and $\mathfrak{b}_+$ broken by $\mathfrak{b}$). We have $|\delta(\mathfrak{b}, \mathfrak{a}) - N| \leq g/2$.

Let $\mathfrak{r} \in [\mathfrak{b}]$ be the ideal obtained by performing a giant step on a reduced ideal $\mathfrak{b}$ and a reduced principal ideal $\mathfrak{a}$. Then $\delta(\mathfrak{r}, \mathfrak{b}) = \delta(\mathfrak{a}, \mathcal{O}') - d$ with $0 \leq d \leq 2g$

[b] All our complexity results are to be considered functions of g, so the O-notation refers to $g \to \infty$. Moreover, all O-constants are independent of q.

(see [40, Theorem 3.7]). Now at most $d \leq 2g$ baby steps applied to $\mathfrak{r}$ yield the reduced ideal $\mathfrak{c}$ below $\delta(\mathfrak{a}, \mathcal{O}')$ with respect to $\mathfrak{b}$, along with the error $\delta(\mathfrak{c}, \mathfrak{b}) - \delta(\mathfrak{a}, \mathcal{O}')$. Using a technique analogous to binary exponentiation on $\mathfrak{a}$, we can now compute for any $n \in \mathbb{N}$ the reduced ideal $\mathfrak{d}$ below $n\delta(\mathfrak{a}, \mathcal{O}')$ with respect to $\mathfrak{b}$ and the error $e = \delta(\mathfrak{d}, \mathfrak{b}) - n\delta(\mathfrak{a}, \mathcal{O}')$. This requires at most $O(g^2 \log n)$ operations in $\mathbb{F}_q$. For any $N \in \mathbb{N}$ with $N < R$, applying this technique to a principal ideal $\mathfrak{a}$ of known distance $\delta(\mathfrak{a}, \mathcal{O}')$ and the exponent $n = \lfloor N/\delta(\mathfrak{a}, \mathcal{O}')\rfloor$, we can thus obtain the ideal closest to $n\delta(\mathfrak{a}, \mathcal{O}')$ with respect to $\mathfrak{b}$, and no more than $\delta(\mathfrak{a}, \mathcal{O}')$ baby steps yield the ideal $\mathfrak{d}$ closest to N with respect to $\mathcal{O}'$. If we choose $\mathfrak{a}$ so that $\delta(\mathfrak{a}, \mathcal{O}') \in O(g \log n)$ — a typical choice for our purpose is $\mathfrak{a} = \mathcal{O}'_+$ and $\delta(\mathfrak{a}, O') = g + 1$ — then we can find $\mathfrak{d}$ in $O(g^2 \log n)$ operations in $\mathbb{F}_q$. None of these computations require knowledge of any actual distances, with the exception of $\delta(\mathfrak{a}, \mathcal{O}')$.

5.2. *Small 3-virtual units for D' imaginary or unusual*

Let D' be an imaginary or unusual discriminant, and $\lambda = A + By' \in \mathcal{O}'$ ($A, B \in \mathbb{F}_q[t]$). Then λ is said to be *small* if

$$\deg(A) \leq \begin{cases} \lfloor 3g/2 \rfloor & \text{if } D' \text{ is imaginary,} \\ \lfloor 3(g+1)/2 \rfloor & \text{if } D' \text{ is unusual,} \end{cases}$$

and

$$\deg(B) \leq \begin{cases} \lfloor (g-1)/2 \rfloor & \text{if } D' \text{ is imaginary,} \\ \lfloor (g+1)/2 \rfloor & \text{if } D' \text{ is unusual.} \end{cases}$$

Since any polynomial of degree d can be represented by the $(d+1)$-tuple of its coefficients, a small element in $\mathcal{O}'$ can be represented by $\deg(A) + \deg(B) + 2$ elements in $\mathbb{F}_q$. For D' imaginary, this number is at most $2g + 1 = \deg(D')$. If D' is unusual, then an upper bound is $2g + 4 = \deg(D') + 2$ if g is odd, and $2g + 3 = \deg(D') + 1$ if g is even.

It is easy to see that reduced or almost reduced ideals produce small 3-virtual units:

Lemma 5.1. *If D' is an imaginary discriminant, then every reduced* 3*-virtual unit is small. If D' is an unusual discriminant, then every reduced or almost reduced* 3*-virtual unit is small.*

Proof. Let $\lambda = A + By'$ ($A, B \in \mathbb{F}_q[t]$) be any generator of $\mathfrak{r}^3$ where $\mathfrak{r}$ is reduced if D' is imaginary, and r is reduced or almost reduced if D' is unusual. Then $A^2 - B^2D' = N(\lambda) = N(\mathfrak{r})^3$, so $\deg(A^2 - B^2D') \leq 3\deg(N(\mathfrak{r}))$. If D' is imaginary, then $\deg(A^2) \neq \deg(B^2D)$ as $\deg(D')$ is odd. If D' is unusual, then the leading terms of A^2 and B^2D' cannot cancel each other as $\operatorname{sgn}(D')$ is a non-square. So either way, $\max\{\deg(A^2), \deg(B^2D)\} \leq 3\deg(N(\mathfrak{r}))$ by the triangle equality for degrees.

If D' is imaginary, then $\deg(D') = 2g + 1$ and $\deg(N(\mathfrak{r})) \leq g$. If D' is unusual, then $\deg(D') = 2g + 2$ and $\deg(N(\mathfrak{r})) \leq g + 1$. The desired bounds are now easy to derive. □

It is straight-forward to find a small 3-virtual units as specified in Lemma 5.1:

Algorithm 5.2 (Small 3-virtual units, D' imaginary or unusual).
Input: A reduced or, if D' is unusual, almost reduced ideal $\mathfrak{a}$ in $\mathcal{O}'$ whose ideal class has order 3.
Output: A small generator λ of $\mathfrak{a}^3$.
Algorithm:

```
(1) Compute a primitive ideal $\mathfrak{b}$ and a polynomial $S \in \mathbb{F}_q[t]$ such that $(S)\mathfrak{b} = \mathfrak{a}^3$.
(2) Apply reduction to $\mathfrak{b}$ to obtain $\theta \in \mathcal{O}'$ with $\mathfrak{b} = (\theta)$.
(3) Output $\lambda = S\theta$.
```

Theorem 5.3. *Algorithm* 5.2 *is correct and requires $O(g^2)$ operations in $\mathbb{F}_q$.*

Proof. Since $\mathcal{O}'$ is the only reduced principal ideal, $\mathfrak{a}^3$ is equivalent to $\mathcal{O}'$. A generator θ of the primitive part $\mathfrak{b}$ of $\mathfrak{a}^3$ can be obtained by applying reduction to $\mathfrak{b}$. Then $\mathfrak{a}^3 = (S)\mathfrak{b} = (S\theta)$, so $\lambda = S\theta$ is a generator of $\mathfrak{a}^3$, which by Lemma 5.1 is small. The computational work required to compute λ is dominated by the cost of computing $\mathfrak{a}^3$ and θ, so the asymptotic field operations count follows from the remarks in Sec. 5.1. □

5.3. *Small 3-virtual units for D' real and small regulator*

The result of Lemma 5.1 is no longer true for real discriminants D'; in fact, most reduced 3-virtual units $\lambda = A + By'$ have coefficients A, B of very large degree. Hence we need to identify among the many reduced ideals in any ideal class one (for the principal class) or three (for ideal classes of order 3) whose cubes have small generators. For the principal class, the reduced ideal in question will lie at about one third of the total circumference of the infrastructure, i.e. at approximate distance $R/3$. For each non-principal class, we choose three roughly equally spaced reduced ideals at approximate distances 0, $R/3$ and $2R/3$ from some reduced starting ideal.

Henceforth, assume that D' is a real discriminant. Then an element $\lambda \in \mathcal{O}'$ is said to be *small* if $\deg(\lambda), \deg(\overline{\lambda}) \leq 3g + 1$. If $\lambda = A + By'$ with $A, B \in \mathbb{F}_q[t]$, then λ is small if and only if $\deg(A) \leq 3g + 1$ and $\deg(B) \leq 2g$, so λ can be represented by at most $(3g + 1) + 2g + 2 = 5g + 3 = 5\deg(D')/2 - 2$ elements in $\mathbb{F}_q$.

Fix a fundamental unit ϵ of K' of positive degree $R = \deg(\epsilon)$. We split our computational task of finding a pair of small quadratic generators into two steps. First, we determine a reduced principal ideal whose cube has a small generator, and three distinct reduced ideals in each ideal class of order 3 whose cubes have small generators. When R is small, specifically $R \leq 3g + 1$, then this step will also yield small generators of the cubes of all these ideals. In the generic case, when R is large, the second computation step will take as input the $\mathbb{F}_q[t]$-basis of any of these reduced ideals and find a small generator of its cube.

If $x \in \mathbb{R}$, then $\lceil x \rfloor$ will denote the nearest integer to x, i.e the unique integer such that $-1/2 \le x - \lceil x \rfloor < 1/2$.

Theorem 5.4. *Let $\mathfrak{a}$ be the reduced principal ideal closest to $N = \lceil R/3 + g/2 \rfloor$ with respect to $\mathcal{O}'$, and α a minimal non-negative generator of $\mathfrak{a}$. Then $\lambda = \alpha^3 \epsilon^{-1}$ is a small generator of $\mathfrak{a}^3$. Furthermore, if $R \ge 3g + 2$, then $\mathfrak{a} \ne \mathcal{O}'$.*

Proof. It is obvious that λ is a generator of $\mathfrak{a}^3$. Moreover, $N \ge \lceil 1/3 + 1/2 \rfloor = 1$, and since $R \ge g + 1$, we have

$$N \le \lceil R/3 + (R-1)/2 \rfloor \le 5R/6 < R.$$

Now $|\delta(\mathfrak{a}, \mathcal{O}') - N| \le g/2$ implies

$$3\delta(\mathfrak{a}, \mathcal{O}') \le 3\left(N + \frac{g}{2}\right) \le 3\left(\frac{R}{3} + \frac{g}{2} + \frac{1}{2} + \frac{g}{2}\right) = R + 3g + \frac{3}{2}, \tag{5.1}$$

$$3\delta(\mathfrak{a}, \mathcal{O}') \ge 3\left(N - \frac{g}{2}\right) \ge 3\left(\frac{R}{3} + \frac{g}{2} - \frac{1}{2} - \frac{g}{2}\right) = R - \frac{3}{2}. \tag{5.2}$$

In particular, if $R \ge 3g + 2$, then

$$\delta(\mathfrak{a}, \mathcal{O}') \ge \frac{R}{3} - \frac{1}{2} \ge \left(g + \frac{2}{3}\right) - \frac{1}{2} = g + \frac{1}{6},$$

so $\delta(\mathfrak{a}, \mathcal{O}') \ge g + 1 = \delta(\mathcal{O}'_+, \mathcal{O}')$, and hence $\mathfrak{a} \ne \mathcal{O}'$. Furthermore, (5.1) and (5.2) imply $-1 \le 3\delta(\mathfrak{a}, \mathcal{O}') - R \le 3g+1$. Since $\delta(\mathfrak{a}, \mathcal{O}') = \deg(\alpha)$, we have $\deg(\lambda) = 3\delta(\mathfrak{a}, \mathcal{O}') - R$, so $-1 \le \deg(\lambda) \le 3g + 1$. Since $\mathfrak{a}$ is reduced, we have $\deg(\lambda\overline{\lambda}) = \deg(N(\mathfrak{a})^3) \le 3g$, so $\deg(\overline{\lambda}) = \deg(\lambda\overline{\lambda}) - \deg(\lambda) \le 3g + 1$. □

Theorem 5.5. *Let $\mathfrak{r}$ be any reduced ideal whose class has order 3. Let $\mathfrak{c}$ be a reduced principal ideal equivalent to $\mathfrak{r}^3, \theta$ a generator of $\mathfrak{c}$ with respect to $\mathfrak{r}^3, \gamma$ a minimal non-negative generator of $\mathfrak{c}$, and write $\deg(\theta) - \deg(\gamma) = nR + m$ with $-3(g+1)/2 \le m < R - 3(g+1)/2$. For $i = 0, 1, 2$, set $N_i = \lceil (m + iR)/3 + g/2 \rfloor$, define $\mathfrak{a}_i$ to be the reduced ideal closest to N_i with respect to $\mathfrak{r}$, and let α_i be a minimal non-negative generator of $\mathfrak{a}_i$ with respect to $\mathfrak{r}$. Then $\lambda_i = \alpha_i^3 \epsilon^{n-i} \gamma / \theta$ is a small generator of $\mathfrak{a}_i^3$ for $i = 0, 1, 2$.*

Proof. Clearly $N_0 = \lceil m/3 + g/2 \rfloor \ge \lceil -1/2 \rfloor = 0$, and since

$$2m \le 2R - 3(g+1) - 1 = 2R - 3g - 4,$$

we have

$$N_2 \le \left\lceil \frac{1}{3}\left(R - \frac{3g}{2} - 2 + 2R\right) + \frac{g}{2} \right\rfloor \le \left\lceil R - \frac{2}{3} \right\rfloor = R - 1,$$

so $0 \leq N_0 \leq N_1 \leq N_2 < R$. Analogous to the proof of Theorem 5.4, we have

$$3\delta(\mathfrak{a}_i, \mathfrak{r}) \leq 3\left(N_i + \frac{g}{2}\right) \leq 3\left(\frac{m+iR}{3} + \frac{g}{2} + \frac{1}{2} + \frac{g}{2}\right) = m + iR + 3g + \frac{3}{2},$$

$$3\delta(\mathfrak{a}_i, \mathfrak{r}) \geq 3\left(N_i - \frac{g}{2}\right) \geq 3\left(\frac{m+iR}{3} + \frac{g}{2} - \frac{1}{2} - \frac{g}{2}\right) = m + iR - \frac{3}{2},$$

so $-1 \leq 3(\mathfrak{a}_i, \mathfrak{r}) - (m + iR) \leq 3g + 1$.

Now $\mathfrak{a}_i^3 = (\alpha_i)^3\mathfrak{r}^3 = (\alpha_i^3/\theta)\mathfrak{c} = (\alpha_i^3\gamma/\theta) = (\lambda_i)$, so λ_i is a generator of $\mathfrak{a}_i^3$. Moreover, since $\delta(\mathfrak{a}_i, \mathfrak{r}) = \deg(\alpha_i)$, we have

$$\begin{aligned} \deg(\lambda_i) &= 3\deg(\alpha_i) + (n-i)R + \deg(\gamma) - \deg(\theta) \\ &= 3\delta(\mathfrak{a}_i, \mathfrak{r}) + (n-i)R - (nR + m) \\ &= 3\delta(\mathfrak{a}_i, \mathfrak{r}) - (m + iR), \end{aligned}$$

so $-1 \leq \deg(\lambda_i) \leq 3g + 1$, and $\deg(\overline{\lambda_i}) = 3\deg(N(\mathfrak{a}_i)) - \deg(\lambda_i) \leq 3g + 1$. □

Note that in order to compute the ideals given in Theorems 5.4 and 5.5, we must know the regulator R, which can be pre-computed using the method of [39], for example.

Theorem 5.6. *If the regulator R is known, then the ideals $\mathfrak{a}$ of Theorem* 5.4 *and $\mathfrak{a}_0, \mathfrak{a}_1, \mathfrak{a}_2$ of Theorem* 5.5 *can be computed in $O(g^3 \log q)$ operations in $\mathbb{F}_q$. If R is linearly bounded in g, then computing the small generators λ of Theorem* 5.4 *and $\lambda_0, \lambda_1, \lambda_2$ of Theorem* 5.5 *requires another $O(g^2)$ operations in $\mathbb{F}_q$.*

Proof. Since $\log R \leq 2g\log(\sqrt{q} + 1) \in O(g \log q)$ by (2.1), the ideals in question can be found in $O(g^3 \log q)$ operations in $\mathbb{F}_q$. The fundamental unit ϵ, the generator α of $\mathfrak{a}$ as given in Theorem 5.4, and the elements γ, θ, and α_i for $i = 0, 1, 2$ as given in Theorem 5.5 can all be obtained by executing no more than R baby steps in the appropriate infrastructure. If R is linearly bounded in g, this requires $O(g^2)$ operations in $\mathbb{F}_q$. □

5.4. *Small 3-virtual units for D' real and large regulator*

Recall that by [13], the ideal class number K'/k is typically very small, so R is of magnitude q^g by (2.1). In this case, any fundamental unit ϵ as well as the quantity γ of Theorem 5.5 will have exponentially large coefficients (of order R) with respect to 1 and y', so the expressions for the 3-virtual units given in Theorems 5.4 and 5.5 are no longer suitable for computation. Not surprisingly, computing small 3-virtual units when K' has large regulator using only $O(g^2)$ field operations is significantly more complicated. In this case, we make use of the following idea. Suppose $\mathfrak{a}$ is a reduced ideal whose cube is principal and has a small generator λ, as determined in Theorems 5.4 and 5.5 for example; we wish to determine such a small generator λ of $\mathfrak{a}^3$. Then $\overline{\lambda}$ is a small generator of $\overline{\mathfrak{a}}^3$, so we can search for λ in the infrastructure of $\mathfrak{a}$ and for $\overline{\lambda}$ in the infrastructure of $\overline{\mathfrak{a}}$ simultaneously as follows. Square $\mathfrak{a}$ and apply reduction to the primitive part of the product ideal $\overline{\mathfrak{a}}^2 \in [\mathfrak{a}]$ to obtain a reduced ideal $\mathfrak{c}$ equivalent to $\mathfrak{a}$. Now apply baby steps simultaneously to $\mathfrak{c}$ and $\overline{\mathfrak{c}}$ until either $\mathfrak{a}$ or $\overline{\mathfrak{a}}$ is found. The various relative generators found in the process are efficiently computable and not too large and will lead to two possible generators of $\mathfrak{a}^3$. At least one of these can be shown to be small, and we can detect which of the two is small.

Theorem 5.7. *Let $\mathfrak{a}$ be a reduced ideal whose cube is principal, and set $\mu = SN(\mathfrak{b})\alpha$ and $\nu = SN(\mathfrak{b})\overline{\beta}$ where $S, \mathfrak{b}, \alpha, \beta$ are given as follows:*

- $\mathfrak{a}^2 = (S)\mathfrak{b}$ *with $S \in \mathbb{F}_q[t]$ and $\mathfrak{b}$ a primitive ideal;*
- $\mathfrak{c} = (\gamma)\overline{\mathfrak{b}}$ *where $\mathfrak{c}$ is the first reduced ideal encountered when applying reduction steps to $\overline{\mathfrak{b}}$;*
- $\alpha = \gamma\theta$ *where $\mathfrak{a} = (\theta)\mathfrak{c}$, obtained by applying baby steps to $\mathfrak{c}$ until $\mathfrak{a}$ is obtained;*
- $\beta = \overline{\gamma}\psi$ *where $\overline{\mathfrak{a}} = (\psi)\overline{\mathfrak{c}}$, obtained by applying baby steps to $\overline{\mathfrak{c}}$ until $\overline{\mathfrak{a}}$ is obtained.*

Then the following hold:

(1) *μ and ν are generators of $\mathfrak{a}^3$.*
(2) *If $\mathfrak{c} = \mathfrak{a}$, then $\mu = \nu$, which is a small generator of $\mathfrak{a}^3$.*
(3) *If $\mathfrak{c} \neq \mathfrak{a}$, then $\mu = u\nu\epsilon$ for some $u \in \mathbb{F}_q^*$, and the following hold:*
   (a) *Suppose that $R \leq 3g+1$. If $\deg(\mu) < R$, then μ is a small generator of $\mathfrak{a}^3$, else ν is a small generator of $\mathfrak{a}^3$.*
   (b) *Suppose $R > 3g+1$. If $\deg(\alpha) \leq \deg(\beta)$, then μ is a small generator of $\mathfrak{a}^3$; else ν is a small generator of $\mathfrak{a}^3$.*

Proof. $S, \mathfrak{b}, \alpha$ and β are all well-defined, since $\mathfrak{a}$ is equivalent to $\overline{\mathfrak{a}}^2$ and hence to $\overline{\mathfrak{b}}$. Furthermore, $\mathfrak{a} = (\alpha)\overline{\mathfrak{b}}$ and $\overline{\mathfrak{a}} = (\beta)\mathfrak{a}$. It follows that $\mathfrak{a}^3 = (S)\mathfrak{a}\mathfrak{b} = (S\alpha)\mathfrak{b}\overline{\mathfrak{b}} = (\mu)$ and $\mathfrak{a}^3 = (S)\mathfrak{a}\mathfrak{b} = (S\overline{\beta})\overline{\mathfrak{b}}\mathfrak{b} = (\nu)$, so μ and ν both generate $\mathfrak{a}^3$.

Note that $\gamma\overline{\gamma} = N(\gamma) = N(\mathfrak{c})/N(\mathfrak{b})$, so $\mu = \theta S\gamma N(\mathfrak{b}) = \theta SN(\mathfrak{c})/\overline{\gamma}$ and $\overline{\nu} = S\psi\overline{\gamma}N(\mathfrak{b}) = \psi N(\mathfrak{c})/(\gamma/S)$. By Lemma 3.4 and Theorem 3.7 of [40], we have $\deg(\overline{\gamma}) \leq 0$ and $-2g \leq \deg(\gamma/S) \leq 0$. Furthermore, $\deg(N(\mathfrak{c})) \leq g$ and $\deg(N(\mu)) = \deg(N(\nu)) = 3\deg(N(\mathfrak{a})) \leq 3g$ as $\mathfrak{a}$ and $\mathfrak{c}$ are reduced ideals. This yields the following bounds on the degrees of μ, ν and their conjugates:

$$\deg(\mu) = \deg(\theta) + \deg(S) + \deg(N(\mathfrak{c})) - \deg(\overline{\gamma}) \geq 0,$$

$$\deg(\overline{\nu}) = \deg(\psi) + \deg(N(\mathfrak{c})) - \deg(\gamma/S) \geq 0,$$

$$\deg(\overline{\mu}) = \deg(N(\mu)) - \deg(\mu) \leq 3g,$$

$$\deg(\nu) = \deg(N(\nu)) - \deg(\overline{\nu}) \leq 3g.$$

If $\mathfrak{c} = \mathfrak{a}$, then $\theta = \psi = 1$, so $\mu = \nu$, and the above bounds immediately force μ to be a small generator of $\mathfrak{a}^3$. So suppose for the remainder of this proof that $\mathfrak{c} \neq \mathfrak{a}$.

Then $\mu/\nu = \theta/\overline{\psi} = \theta\psi/N(\psi)$ and $\deg(\theta) + \deg(\psi) = \delta(\mathfrak{a}, \mathfrak{c}) + \delta(\overline{\mathfrak{a}}, \overline{\mathfrak{c}}) = R$, so

$$\deg(\mu) - \deg(\nu) = R - \deg(N(\psi)) = R - \deg(N(\mathfrak{c})) + \deg(N(\mathfrak{a})).$$

Since $\mathfrak{a}$ is reduced and $R \geq g + 1$, we have $0 \leq \deg(N(\mathfrak{a})) \leq g < R$; similarly for $\mathfrak{c}$. Thus, $0 < R - g \leq \deg(\mu) - \deg(\nu) \leq R + g < 2R$. Now μ and ν generate the same ideal, so they must differ by a unit. Thus, their degrees must differ by a multiple of R. This forces $\deg(\mu) - \deg(\nu) = R$, and hence $\mu = u\nu\epsilon$ for some $u \in \mathbb{F}_q^*$.

Suppose first that $R \leq 3g + 1$. If $\deg(\mu) < R$, then $\deg(\mu) \leq 3g$ and $\deg(\overline{\mu}) \leq 3g$ from the bounds above, so μ is a small generator of $\mathfrak{a}^3$. If $\deg(\mu) \geq R$, then $\deg(\nu) = \deg(\mu) - R \geq 0$. It follows that $\deg(\nu) \leq 3g$ from above and $\deg(\overline{\nu}) = \deg(N(\nu)) - \deg(\nu) \leq 3g$, so ν is a small generator of $\mathfrak{a}^3$.

Now suppose that $R > 3g + 1$, and let λ be a small generator of $\mathfrak{a}^3$. Then there exists $v \in \mathbb{F}_q^*$ and $m \in \mathbb{Z}$ such that $\lambda = v\mu\epsilon^{m-1} = uv\nu\epsilon^m$. Then

$$(m - 1)R = \deg(\lambda) - \deg(\mu) \leq \deg(\lambda) \leq 3g + 1 < R, \tag{5.3}$$

$$mR = \deg(\overline{\nu}) - \deg(\overline{\lambda}) \geq -\deg(\overline{\lambda}) \geq -(3g + 1) > -R \tag{5.4}$$

so $m \in \{0, 1\}$.

Assume that $\deg(\alpha) \leq \deg(\beta)$, so $\deg(\mu) \leq \deg(\overline{\nu})$. If ν is a small generator of $\mathfrak{a}^3$, then $\deg(\mu) \leq \deg(\overline{\nu}) \leq 3g + 1$ and $\deg(\overline{\mu}) \leq 3g$, so μ is also a small generator of $\mathfrak{a}^3$. If ν is not a small generator of $\mathfrak{a}^3$, then $m = 1$, so $\mu = v^{-1}\lambda$ is a small generator of $\mathfrak{a}^3$. A similar argument shows that ν is a small generator of $\mathfrak{a}^3$ when $\deg(\alpha) \geq \deg(\beta)$. □

Note that when $R \leq 3g + 1$, then part (3)(a) of Theorem 5.7 can be used to find a small generator of $\mathfrak{a}^3$ as an alternative to Theorems 5.4 and 5.5.

We formulate the above theorem as an algorithm:

Algorithm 5.8 (Small 3-virtual units, D' real, $R \geq 3g + 2$).

Input: A reduced ideal $\mathfrak{a}$ whose cube is principal and has a small generator.
Output: A small generator λ of $\mathfrak{a}^3$.
Algorithm:

```
(1) Compute a primitive ideal $\mathfrak{b}$ and a polynomial $S \in \mathbb{F}_q[t]$ such that $\mathfrak{a}^2 = (S)\mathfrak{b}$.
(2) Apply reduction steps to $\overline{\mathfrak{b}}$ until the first reduced ideal $\mathfrak{c}$ is encountered. Set $\gamma$
    to be the relative generator of $\mathfrak{c}$ with respect to $\overline{\mathfrak{b}}$ obtained in this process.
(3) If $\mathfrak{c} = \mathfrak{a}$, then output $\lambda = SN(\mathfrak{b})\gamma$.
(4) Else, simultaneously apply baby steps to $\mathfrak{c}$ and $\overline{\mathfrak{c}}$, keeping track of the respective
    ideals $\mathfrak{r}, \mathfrak{s}$ thus encountered and the respective relative generators $\rho, \sigma$ with
    $\mathfrak{r} = (\rho)\mathfrak{c}$ and $\mathfrak{s} = (\sigma)\overline{\mathfrak{c}}$, until $\mathfrak{r} = \mathfrak{a}$ or $\mathfrak{s} = \overline{\mathfrak{a}}$.
```

(5) Suppose $\mathfrak{r} = \mathfrak{a}$ is encountered first. While $\mathfrak{s} \neq \overline{\mathfrak{a}}$ and $\deg(\overline{\gamma}\sigma) < \deg(\gamma\rho)$, apply baby steps to $\mathfrak{s}$. If $\deg(\overline{\gamma}\sigma) \geq \deg(\gamma\rho)$ is found first, output $\lambda = SN(\mathfrak{b})\gamma\rho$. Otherwise, in the case that $\mathfrak{s} = \overline{\mathfrak{a}}$ is found first, output $\lambda = SN(\mathfrak{b})\gamma\overline{\sigma}$.

(6) Suppose $\mathfrak{s} = \overline{\mathfrak{a}}$ is encountered first. While $\mathfrak{r} \neq \mathfrak{a}$ and $\deg(\gamma\rho) < \deg(\overline{\gamma}\sigma)$, apply baby steps to $\mathfrak{r}$. If $\deg(\gamma\rho) < \deg(\overline{\gamma}\sigma)$ is found first, output $\lambda = SN(\mathfrak{b})\gamma\overline{\sigma}$. Otherwise, in the case that $\mathfrak{r} = \mathfrak{a}$ is found first, output $\lambda = SN(\mathfrak{b})\gamma\rho$.

Theorem 5.9. *Algorithm* 5.8 *produces a small generator λ of $\mathfrak{a}^3$ and requires $O(g^2)$ operations in $\mathbb{F}_q$.*

Proof. As before, set $\mu = SN(\mathfrak{b})\alpha$ and $\nu = SN(\mathfrak{b})\overline{\beta}$, where α and β (as well as θ, ψ and $\mathfrak{c}$) are given as in Theorem 5.7. By the same theorem, μ and ν generate $\mathfrak{a}^3$.

If $\mathfrak{c} = \mathfrak{a}$, then by part (2) of Theorem 5.7, $\mu = SN(\mathfrak{b})\gamma$ is a small generator of $\mathfrak{a}^3$. So assume that $\mathfrak{c} \neq \mathfrak{a}$.

Suppose we enter step (5). Then $\gamma\rho = \alpha$ in the context of Theorem 5.7. Also, as baby steps to $\mathfrak{s}$ cause $\deg(\sigma)$ to increase strictly, we always have $\deg(\overline{\gamma}\sigma) \leq \deg(\beta)$, with equality occurring exactly when $\mathfrak{s} = \overline{\mathfrak{a}}$. Now, if the while loop terminates with the condition $\deg(\overline{\gamma}\sigma) \geq \deg(\gamma\rho)$, then we know that $\deg(\alpha) \leq \deg(\beta)$, and by part (3)(b) of Theorem 5.7, $\lambda = SN(\mathfrak{b})\gamma\rho$ is a small generator of $\mathfrak{a}^3$. Otherwise, the while loop terminates with $\mathfrak{s} = \overline{\mathfrak{a}}$ and $\deg(\beta) = \deg(\overline{c}\sigma) < \deg(\gamma\rho) = \deg(\alpha)$, so again by part (3)(b) of Theorem 5.7, $\lambda = SN(\mathfrak{b})\gamma\overline{\sigma}$ is a small generator of $\mathfrak{a}^3$. A symmetric argument can be used if step (5) is passed and step (6) is entered instead.

The number of field operations required to compute λ is dominated by the costs of the baby steps. Notice that since λ is a small generator, $\deg(\lambda)$ is linear in g. As a single baby step increases the degree of the corresponding relative generator by at least 1, the total number of baby steps required to compute both ρ and σ is also in $\mathcal{O}(g)$. Finally, each baby step requires $O(g)$ field operations, so the total cost is $O(g^2)$ field operations. □

6. Computing the Set $\mathcal{L}$: Algorithms and Results

In this section, we present our construction of all cubic function fields of a given discriminant. We also briefly discuss our implementation and some numerical results, and compare our technique to the cubic function field tabulation method of [26, 27].

6.1. *Construction of $\mathcal{L}$*

We now have all the ingredients for generating the set $\mathcal{L}$ by computing small minimal polynomials for the entire pre-image of $\mathcal{I}^*$ under Φ for D' imaginary or unusual and of $\mathcal{I}$ under Φ for D' real. Our construction requires access to machinery for obtaining a basis for the 3-torsion of the class group of K'/k as well as the regulator R when K' is real. Once these quantities are found, the set $\mathcal{L}$ can be computed via straightforward calls to the algorithms in Sec. 5.

Algorithm 6.1 (Computing $\mathcal{L}$ when $D/(-3)$ is imaginary or unusual).

Input:

- A prime power q with $\gcd(q, 6) = 1$;
- A square-free polynomial $D \in \mathbb{F}_q[t]$ so that $D' = D/(-3)$ is imaginary or unusual.

Output: Minimal polynomials for the $(3^{r'} - 1)/2$ distinct triples of conjugate cubic fields of discriminant D.

Algorithm:

```
(1) Compute a basis $\mathcal{B}$ for the 3-torsion of the ideal class group of the quadratic function field $K'$ of discriminant $D'$.
(2) For each pair $\{[\mathfrak{a}], [\overline{\mathfrak{a}}]\}$ with $\mathfrak{a} \in \langle \mathcal{B} \rangle$ non-principal do
    (a) Compute the reduced or an almost reduced ideal $\mathfrak{r}$ in the class of $\mathfrak{a}$.
    (b) Compute a small generator $\lambda$ of $\mathfrak{r}^3$ using Algorithm 5.2.
    (c) Set $a = \mathrm{sgn}(N(\lambda))$.
    (d) Output $F(Z) = Z^3 - 3aN(\mathfrak{r})Z + \mathrm{Tr}(a\lambda)$.
```

Theorem 6.2. *Algorithm* 6.1 *is correct.*

Proof. Step (2)(a) produces reduced or almost reduced representatives for all the $(3^{r'} - 1)/2$ distinct ideal classes of order 3 of K'. For each ideal $\mathfrak{r}$ thus produced, $a\lambda$ is a generator of $\mathfrak{r}^3$ which is normalized by Lemma 2.2. Furthermore $\alpha\lambda$ is not a cube in $\mathcal{O}'$ as $\mathfrak{r}$ is not principal. We have $\mathrm{sgn}(N(a\lambda)) = a^3$, so $N(a\lambda) = \mathrm{sgn}(N(a\lambda))N(\mathfrak{r})^3 = (aN(\mathfrak{r}))^3$. By Theorem 3.1, the polynomial $F(Z)$ of step (2)(d) is a minimal polynomial for the triple of cubic fields $\{L, L', L''\} \in \mathcal{L}$ for which $\{a\lambda, a\overline{\lambda}\}$ is a pair of quadratic generators. By Corollary 3.3, all these fields are distinct, and by Corollary 4.3, all triples of fields in $\mathcal{L}$ are produced by the algorithm. □

Theorem 3.1 rules out cubes in $\mathcal{O}'$ as quadratic generators. When D' is real, restricting to small reduced 3-virtual units ensures this requirement:

Lemma 6.3. *Suppose that D' is real. Then no small reduced* 3*-virtual unit in $\mathcal{O}' \backslash \mathbb{F}_q$ is an $\mathbb{F}_q^*$-multiple of a cube in $\mathcal{O}'$.*

Proof. Let $\lambda \in \mathcal{O}'$ be small so that $(\lambda) = \mathfrak{r}^3$ with $\mathfrak{r}$ reduced, and suppose that $\lambda = a\mu^3$ for some $a \in \mathbb{F}_q^*$ and $\mu \in \mathcal{O}'$. Then $\mathfrak{r} = (\mu)$, so $\mathfrak{r}$ is principal. Now $3g + 1 \geq \deg(\lambda) = 3\deg(\mu)$, so $\deg(\mu) \leq g$; similarly $\deg(\overline{\mu}) \leq g$.

If $\deg(\mu) \geq 0$, then $0 \leq \deg(\mu) \leq g < R$, so μ is a minimal non-negative generator of $\mathfrak{r}$. It follows that $\delta(\mathfrak{r}, \mathcal{O}') = \deg(\mu)$. Since $\delta(\mathfrak{a}, \mathcal{O}') \geq \delta(\mathcal{O}'_+, \mathcal{O}') \geq g + 1 > \delta(\mathfrak{r}, \mathcal{O}')$ for all reduced principal ideals $\mathfrak{a} \neq \mathcal{O}'$, this forces $\mathfrak{r} = \mathcal{O}'$. If $\deg(\mu) < 0$, then $\deg(\overline{\mu}) = \deg(N(\mu)) - \deg(\mu) \geq -\deg(\mu) > 0$, which as before forces $\overline{\mathfrak{r}} = \mathcal{O}'$, and hence again $\mathfrak{r} = \mathcal{O}'$.

It follows that $\mu = b\epsilon^i$ for some $b \in \mathbb{F}_q^*$ and $i \in \mathbb{Z}$. Then $iR = \deg(\mu) \leq g < R$ forces $i \leq 0$, and $-iR = \deg(\overline{\mu}) \leq g < R$ implies $i \geq 0$. Hence $\mu = b$ and $\lambda = ab^3 \in \mathbb{F}_q$. □

Algorithm 6.4 (Computing $\boldsymbol{\mathcal{L}}$ when $\boldsymbol{D/(-3)}$ is real).

Input:

- A prime power q with $\gcd(q, 6) = 1$;
- A square-free polynomial $D \in \mathbb{F}_q[t]$ so that $D' = D/(-3)$ is real.

Output: Minimal polynomials for the $(3^{r'+1} - 1)/2$ distinct triples of conjugate cubic fields of discriminant D.

Algorithm:

```
(1) Compute the regulator $R$ of $K'$.
(2) If $R \leq 3g + 1$ then compute a fundamental unit $\epsilon$ of $K'$.
(3) Compute the ideal $\mathfrak{a}$ of Theorem 5.4.
(4) If $R \leq 3g + 1$ then
          If $\mathfrak{a} = \mathcal{O}'$, then set $\lambda = \epsilon$,
          Else compute a small generator $\lambda$ of $\mathfrak{a}^3$ as described in Theorem 5.4 or in
          part (3)(a) of Theorem 5.7,
    Else    $//R \geq 3g + 2$
          Compute a small generator $\lambda$ of $\mathfrak{a}^3$ as described in Algorithm 5.8.
(5) Set $a = \mathrm{sgn}(N(\lambda))$.
(6) Output $F(Z) = Z^3 - 3aN(\mathfrak{a})Z + \mathrm{Tr}(a\lambda)$.
(7) Compute a basis $\mathcal{B}$ for the 3-torsion of the ideal class group of the quadratic
    function field $K'$ of discriminant $D'$.
(8) For each pair $\{[\mathfrak{a}], [\overline{\mathfrak{a}}]\}$ with $\mathfrak{a} \in \langle \mathcal{B} \rangle$ non-principal do
    (a) Compute a reduced ideal $\mathfrak{r}$ in the class of $\mathfrak{a}$.
    (b) Compute the three ideals $\mathfrak{a}_0, \mathfrak{a}_1, \mathfrak{a}_2$ of Theorem 5.5 from $\mathfrak{r}$.
    (c) For $i = 0, 1, 2$ do
          (i) If $R \leq 3g + 1$ then
                    Compute a small generator $\lambda_i$ of $\mathfrak{a}_i$ as described in Theorem 5.5 or
                    in part (3)(a) of Theorem 5.7,
              Else    $// R \geq 3g + 2$
                    Compute a small generator $\lambda_i$ of $\mathfrak{a}_i$ as described in Algorithm 5.8.
         (ii) Set $a_i = \mathrm{sgn}(N(\lambda_i))$.
        (iii) Output $F_i(Z) = Z^3 - 3a_iN(\mathfrak{a}_i)Z + \mathrm{Tr}(a_i\lambda_i)$.
```

Theorem 6.5. *Algorithm* 6.4 *is correct.*

Proof. Step (3) produces a reduced principal ideal $\mathfrak{a}$ that has a small generator, and step (4) computes such a small generator λ. If $R \leq 3g + 1$, then $\lambda = \epsilon$ or

$\lambda = \alpha^3\epsilon^{-1}$ for some $\alpha \in \mathcal{O}'$, so no $\mathbb{F}_q^*$-multiple of λ is a cube in $\mathcal{O}'$. If $R \geq 3g+2$, then $\mathfrak{a} \neq \mathcal{O}'$ by Theorem 5.4, so $\lambda \notin \mathbb{F}_q^*$. By Lemma 6.3, again no $\mathbb{F}_q^*$-multiple of λ is a cube in $\mathcal{O}'$.

Similarly, step (8)(b) produces three distinct reduced representatives in each of the $(3^{r'}-1)/2$ distinct ideal classes of order 3 of K' that have small generators, and step (8)(c)(i) computes all these small generators. Since none of these ideals is principal, no $\mathbb{F}_q^*$-multiple of any of the small generators is a cube in $\mathcal{O}'$ by Lemma 6.3.

For each small 3-virtual unit λ thus produced, $a\lambda$ with $a = \operatorname{sgn}(N(\lambda))$ is normalized by Lemma 2.2 and is not a cube. Once again, by Theorem 3.1, each polynomial $F(Z)$ of steps (6) and (8)(c)(iii) is a minimal polynomial for the triple of cubic fields $\{L, L', L''\} \in \mathcal{L}$ for which $\{a\lambda, a\overline{\lambda}\}$ is a pair of quadratic generators. By Theorem 3.2 and Corollary 3.3, all these fields are distinct, and by Corollary 4.3, all triples of fields in $\mathcal{L}$ are produced by the algorithm. □

6.2. *Computational considerations*

Each minimal polynomial $F(Z) = Z^3 - 3QZ + 2A$ output by Algorithm 6.1 or Algorithm 6.4 requires storage of $\deg(Q) + \deg(A) + 2$ elements in $\mathbb{F}_q$. We have $\deg(Q) \leq g$ for D' imaginary or real, and $\deg(Q) \leq g+1$ for D' unusual. Similarly, we see that $\deg(A) \leq \lfloor 3g/2 \rfloor$ for D' imaginary, $\deg(A) \leq \lfloor 3(g+1)/2 \rfloor$ for D' unusual, and $\deg(A) \leq 3g+1$ for D' real. This yields the following space requirement for $F(Z)$:

- $\lfloor 5g/2 \rfloor + 2 = \lfloor (5\deg(D)+3)/4 \rfloor$ field elements when D' is imaginary,
- $\lfloor 5(g+1)/2 \rfloor + 2 = \lfloor 5\deg(D)/4 \rfloor + 2$ field elements when D' is unusual,
- $4g+3 = 2\deg(D) - 1$ field elements when D' is real.

The run time of our construction algorithms (Algorithms 6.1 and 6.4) is determined by the computation of the 3-torsion of the class group of K', along with the regulator if K'/k is real, and the generation of the $(3^{r'}-1)/2$ minimal polynomials of all cubic function fields of discriminant D. The structure of any finite abelian group G can be computed using $O(\sqrt{\#G})$ group operations; see for example [42] and the references therein. In our context, $\#G \leq 2(\sqrt{q}+1)^{2g}$ by (2.1), so the basis $\mathcal{B}$ in step (1) of Algorithm 6.1 or step (7) of Algorithm 6.4 can be found in $O(g^2(\sqrt{q}+1)^g)$ operations in $\mathbb{F}_q$. This dominates the regulator computation in step (1) of Algorithm 6.4 if R is computed using for example the algorithm of [39].

The loops in step (2) of Algorithm 6.1 and step (8) of Algorithm 6.4 are each executed $(3^{r'}-1)/2$ times. The most naïve way of generating the ideals $\mathfrak{r}$ in step (2)(a) of Algorithm 6.1 or step (8)(a) of Algorithm 6.4 requires $O(g^2)$ field operations. By Theorem 5.3, step (2)(b) of Algorithm 6.1 requires $O(g^2)$ operations in $\mathbb{F}_q$. By Theorems 5.6 and 5.9, steps (3)–(6) as well as each iteration of step (8) of Algorithm 6.4 require $O(g^3 \log q)$ operations in $\mathbb{F}_q$.

Note that all the $O()$ estimates above apply to both $q \to \infty$ and $g \to \infty$, and the constants are independent of q and g. Since $r' \leq 2g$ (see for example [25, Corollary, p. 180]), it follows that the number of field operations required by Algorithms 6.1 and 6.4 is bounded above by

$$C \max\{g^2(\sqrt{q}+1)^g, g^2 3^{r'}\} \leq C g^2 (\max\{\sqrt{q}+1, 9\})^g \tag{6.1}$$

and

$$C \max\{g^2(\sqrt{q}+1)^g, \log(q) g^3 3^{r'}\} \leq C g^2 \max\{(\sqrt{q}+1)^g, \log(q^g) 3^{2g}\}, \tag{6.2}$$

respectively, for some positive constant C that is independent of q and g but depends on the signature of K' (imaginary, unusual, real).

Restricting our computation to just the 3-torsion of the class group of K' may be faster than finding the complete structure; moreover, for large genus, Hammell's index calculus algorithm [15] might be more efficient than square root methods. Furthermore, r' is expected to be small compared to $2g$, so step (1) of Algorithm 6.1 and step (7) of Algorithm 6.4 generally dominate the overall running time in practice. Once $\mathcal{B}$ is found, along with the regulator R if D' is real, the remaining portions of Algorithms 6.1 and 6.4 tend to be very efficient.

To test our constructions, we implemented both Algorithms 6.1 and 6.4 in C++, using NTL [38] for finite field and polynomial arithmetic; our computer code is available from the first author upon request. The computationally most interesting scenario is the case when D is an unusual discriminant with dual real discriminant D', so we focus our discussion on this case. Here, we require in particular that $q \equiv -1 \pmod 3$, and the computations are performed in the infrastructure of the real quadratic field K'. Our implementations were tested on 209 388 unusual discriminants D, taken from [2], for which the corresponding quadratic function fields have 3-ranks ranging from 2 to 4, as well as their dual real discriminants D'. The discriminants were defined over $\mathbb{F}_q$ with $q \in \{5, 11, 17, 23\}$ and the corresponding quadratic function fields had genus $g \in \{3, 4, 5, 7, 8, 9, 11\}$. In order to distinguish the escalatory from the non-escalatory examples, we computed the class groups for both the unusual and the dual real quadratic fields. In total, 81 736 of the quadratic fields were escalatory and 127 652 were non-escalatory. The computations were done on a 2.8 GHz Intel Pentium 4 processor running Linux, and were completed in just seven days; this includes the time required to compute the class groups and (in the case when D is unusual) the regulator of K'.

In all cases, our implementations produced the correct number of cubic fields with the appropriate signatures as determined in Corollary 4.5, and all of them corresponded to small quadratic generators. Once the structure of the ideal class group was computed, our algorithms were very efficient. Over all the examples of both unusual and real discriminants, the maximum running time to compute the cubic fields of a single discriminant was less than 2 s, and on average was less than 1 s.

In order to test our implementations further, we employed the technique of [2] to construct an example with larger 3-rank by lifting the base field. The unusual discriminant $D = 2t^{12} + 3t^9 + t^3 + 1$, when defined over $\mathbb{F}_{5^3}$, corresponds to a quadratic function field of 3-rank 5 and is non-escalatory — the dual real discriminant $D' = D/(-3) = t^{12} + 4t^9 + 3t^3 + 3$ corresponds to a field that also has 3-rank 5. We ran Algorithms 6.4 and 6.1 on this pair of dual discriminants. On input D, Algorithm 6.4 produced exactly $(3^5 - 1)/2 = 121$ triples of conjugate cubic fields of signature $(1, 1; 1, 2)$ and $3^5 = 243$ of signature $(3, 1)$. Once the class group was computed, these 364 triples of fields were computed in only 8.39 s, and the total computation required 3.5 min. On input D', Algorithm 6.1 produced 121 triples of conjugate fields of signature $(1, 1; 1, 1; 1, 1)$ in 37.42 s after the class group was computed, and the total computation required 5.66 h. The second computation was slower because, as discussed in [2], ideal arithmetic in unusual quadratic function fields over large base fields is currently more cumbersome than ideal arithmetic in the imaginary and real cases. The complete list of cubic function fields produced for these two examples can be found in Appendix A.

6.3. *Construction versus tabulation*

We also compared our algorithm to the tabulation procedure for cubic function fields of [27]. This method computes small minimal polynomials for all cubic function fields of square-free discriminant D up to a given degree bound B so that $D' = D/(-3)$ is imaginary or unusual; unlike our method, the technique does not apply to real discriminants D'. The tabulation algorithm is an adaptation to function fields of Belabas' algorithm [3] for tabulating cubic number fields and makes use of the Davenport–Heilbronn map. This map is an explicit discriminant preserving one-to-one correspondence between triples of conjugate cubic function fields and a certain efficiently computable set $\mathcal{U}$ of equivalence classes of binary cubic forms over $\mathbb{F}_q[t]$, given by their unique reduced representatives. Every reduced form $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3 \in \mathbb{F}_q[t, x, y]$ of discriminant

$$D = D(f) = 18abcd + b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 \tag{6.3}$$

representing a class in $\mathcal{U}$ corresponds bijectively to the minimal polynomial $f(x, 1)$ of a triple of conjugate cubic function fields of the same discriminant D. Moreover, $f(x, y)$ satisfies the coefficient bounds

$$\deg(a), \deg(b) \le \deg(D)/4, \quad \deg(ac), \deg(ad), \deg(bc) \le \deg(D)/2, \tag{6.4}$$

together with some simple normalization conditions. The algorithm loops over all quadruples $(a, b, c, d) \in \mathbb{F}_q[t]^4$ that satisfy said normalization conditions as well as (6.4) (with $\deg(D)$ replaced by the degree bound B). For each such quadruple, it checks that the corresponding binary cubic form is reduced and represents a class in $\mathcal{U}$; if yes, then the method outputs $f(x, 1)$.

If the input bound B to the tabulation algorithm is the degree of our target discriminant D, and all the fields of discriminant different from D are suppressed, then the output is a list of minimal polynomials of all cubic function fields of discriminant D, as desired. Unfortunately, there is no way of knowing in advance when D is encountered in the tabulation process. Even worse, numerical data show that the triples of cubic function fields of discriminant D are interspersed with all the other fields in an unpredictable manner. However, one significant improvement is possible here: one can simply let a, b, c loop over the bounds (6.4) and attempt to solve for d by applying the quadratic formula to (6.3).

Using techniques analogous to [28], it is straightforward to show that for any $s \in \mathbb{N}$, the number of appropriately normalized polynomials a of degree at most $\lfloor s/4 \rfloor$ is at least $C_a q^{\lfloor s/4 \rfloor + 1}$, and the number of polynomial pairs (b, c) with $\deg(b) \leq \lfloor s/4 \rfloor$ and $\deg(bc) \leq \lfloor s/2 \rfloor$ is at least $C_{bc} s q^{\lfloor s/2 \rfloor + 2}$, for suitable positive constants C_a, C_{bc} that are independent of s and q. Taking into account the polynomial arithmetic performed in each loop iteration, it follows that the running time of this improved tabulation algorithm (turned construction algorithm) is at least

$$C \sum_{s=1}^{\deg(D)} s^3 q^{\lfloor s/4 \rfloor + \lfloor s/2 \rfloor + 3} \geq C \deg(D)^3 q^{\lfloor \deg(D)/4 \rfloor + \lfloor \deg(D)/2 \rfloor + 3} \geq 8Cg^3 q^{(3g+5)/2},$$

where $\deg(D) = 2g+1$ or $2g+2$ depending on the type of D' (imaginary or unusual), and C is some positive constant that is independent of D and q.

When the discriminant degree is odd and small, it might be possible to improve this lower bound, since the possibilities for the degrees of the coefficients of a reduced form $f(x, y)$ are more limited, and the choices for their leading coefficients may be subject to further restrictions. For example, when $\deg(D) = 3$ or 5, then the number of choices for triples (a, b, c) can be established as $q^2(q-1)$ and $q^2(q-1)/2$, respectively. For $\deg(D) = 7$, there are $q^5(q-1)/2$ possible such triples (a, b, c). However, when $\deg(D)$ becomes large or is even, such counting arguments become exceedingly complicated or yield no further improvement.

We now compare the run time of the modified tabulation algorithm with that of Algorithm 6.1. The rather coarse estimate $r' \leq 2g$ will suffice for our analysis. Consider the ratio

$$F(g, q) = \frac{g^3 \sqrt{q}^{3g+5}}{g^2 (\max\{\sqrt{q}+1, 9\})^g} = gq^{5/2} \left(\frac{q^{3/2}}{\max\{\sqrt{q}+1, 9\}} \right)^g, \tag{6.5}$$

whose numerator is a lower bound on the run time of the tabulation algorithm and whose denominator represents an upper bound on the run time of our construction algorithm by (6.1) (up to constant factors that are independent of q and g). For $q \geq 64$, we have $9 \leq \sqrt{q} + 1 = \sqrt{q}(1 + 1/\sqrt{q}) \leq 9\sqrt{q}/8 = 9 \max\{\sqrt{q}/8, 1\}$. So

$$F(q, g) \geq gq^{5/2} \left(\frac{q^{3/2}}{9 \max\{\sqrt{q}/8, 1\}} \right)^g = gq^{5/2} \left(\frac{q \min\{\sqrt{q}, 8\}}{9} \right)^g,$$

and we see that $F(q, g)$ grows at least exponentially in $\log(q^g)$ as $g \to \infty$ or $q \to \infty$. So one expects that our method outperforms the revised tabulation method even for quadratic function fields of modest size, including the cases of small odd discriminant degree discussed above. Computations confirm these theoretical estimates: recall that it took under 6 h to construct all 121 triples of conjugate cubic function fields of the real discriminant $D'(t) = t^{12} + 4t^9 + 3t^3 + 3$ over $\mathbb{F}_{125}$. Based on the numerical results of [28], we predict that the modified tabulation algorithm (using only three loops) would run a few days just on inputs $B = 12$ and $q = 5$. Inputs of $B = 12$ and $q = 125$ would be completely infeasible for this method.

7. Conclusion and Further Work

The algorithms described in this paper generate all triples of conjugate cubic function fields of any fixed square-free discriminant D over a finite field of characteristic at least 5, represented by small defining polynomials. Once the structure (or at least the 3-torsion) of the ideal class group — and for D' real also the regulator — of the quadratic function field K' of discriminant $D' = D/(-3)$ is known, our method is very efficient. Our technique makes use of ideal arithmetic in K'. When D' is imaginary or unusual, this is straightforward, although somewhat slow and cumbersome in the latter case. In the more interesting scenario when D' is real, infrastructure arithmetic in the real field K' is utilized; this idea is originally due to Shanks.

In addition to computing all the cubic function fields of discriminant D, we also provided a characterization of exactly which signatures can occur for these fields, as well as an *a priori* count for them, split up according to signature. The count is determined by the type of discriminant (D imaginary, unusual, or real), the congruence class of $q \pmod 3$, the 3-rank of the ideal class group of the quadratic function field of discriminant D and, where applicable, the distinction between escalatory and non-escalatory. This count by signature is much more interesting than the corresponding situation in number fields, where one has the very simple correspondence of real, respectively, imaginary quadratic fields corresponding to real, respectively, complex cubic fields of the same (fundamental) discriminant. Moreover, among a pair of dual quadratic fields, one is always real and the other always imaginary, whereas in the function field scenario, they can be identical, or both are imaginary, or one is real and the other unusual.

Our worst case complexity comparison in Sec. 6.3 shows that our algorithm outperforms the tabulation method of [27]. It would be interesting to see how the two techniques compare in terms of average performance. The average complexity of our construction is clearly determined by the expected run time of class group computation. On the other hand, the average performance of the tabulation algorithm seems to be very hard to analyze since it is difficult to predict when the target discriminant is encountered in the course of the tabulation. Insight into this problem might aid in improving the performance of the tabulation method when one is interested in only one particular discriminant, as in the construction procedure.

As in the number field setting, our technique can be extended to non-square-free discriminants. In this scenario, just as in the approach taken in [22], simple class field theory must be replaced by ray class field theory, and more Kummer theory is needed. In this vein, motivated by [7], a technique for constructing all non-cyclic cubic function fields (and more generally, all dihedral extensions of prime degree) with a given quadratic resolvent field was presented in [45, 46], along with an implementation of the corresponding tabulation algorithm in MAGMA. However, this method produces quadratic generators in a more ad hoc fashion: if a given quadratic generator λ is somewhat large, it and its square are multiplied by cubes in K' to see if a smaller generator can be found. It would be interesting to combine the approach of [45, 46] with the computational advantages of using arithmetic of reduced or almost reduced ideals presented here.

Finally, it is worth noting that our results do not extend to base fields of characteristic 2 or even 3; these cases would require a completely different theory and treatment.

Acknowledgments

This work was inspired by, and is dedicated to, the late Dan Shanks. The first, third and fourth authors are supported by NSERC of Canada. The second author is the corresponding author and supported by the LG Yonam Foundation. The authors thank Pieter Rozenhart for discussions and some test computations that aided in our algorithm comparisons of Sec. 6.3. We are also grateful to an anonymous referee for his or her careful review and constructive suggestions for improvement of our paper.

Appendix A. Examples

We present minimal polynomials for the 121 triples of conjugate cubic function fields with the real discriminant $D' = 3 + 3t^3 + 4t^9 + t^{12}$ over $\mathbb{F}_{5^3}$, as well as the 364 triples of conjugate cubic function fields with the dual unusual discriminant $D = -3D' = 1 + t^3 + 3t^9 + 2t^{12}$, separated by signature. The class group of the quadratic function field of discriminant D' is isomorphic to $\mathbb{Z}/3556350\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and its regulator is $R = 18$. The class group of the function field of discriminant D is isomorphic to $\mathbb{Z}/21338100\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. As the 3-rank is 5 in both cases, we are in the non-escalatory situation.

The field $\mathbb{F}_{5^3}$ was constructed as $\mathbb{F}_{5^3} = \mathbb{F}_5[w]/(3 + 4w + w^2 + w^3)$ in our computations. In the tables below, the coefficients of polynomials in $\mathbb{F}_{5^3}[t]$ are given as integers in $\{0, \ldots, 124\}$ via the map

$$\nu : \mathbb{F}_{5^3} \to \{0, \ldots, 124\}$$

$$a_2 w^2 + a_1 w + a_0 \mapsto a_2 5^2 + a_1 5 + a_0.$$

Polynomials in $\mathbb{F}_{5^3}[t]$ are given as vectors, so the polynomial $b_d t^d + b_{d-1} t^{d-1} + \cdots + b_1 t + b_0$ appears as $[\nu(b_0), \nu(b_1), \ldots, \nu(b_{d-1}), \nu(b_d)]$.

Minimal polynomials for the cubic function fields of discriminant D' are listed in Table A.1, and those for cubic function fields of discriminant D in Tables A.2 and A.3.

Table A.1. Minimal polynomials $F(z) = z^3 - 3Q_i z + 2A_i$ for the 121 cubic fields of real discriminant $D' = 3 + 3t^3 + 4t^9 + t^{12}$; all have signature $(1, 1; 1, 1; 1, 1)$.

i	Q_i	A_i
0	$[0, 2, 2, 1, 4, 0, 3]$	$[1, 0, 1, 1, 3, 4, 3, 4, 4, 1]$
1	$[1, 4, 2, 3, 0, 1, 1]$	$[2, 2, 2, 3, 2, 0, 2, 4, 3, 2]$
2	$[0, 0, 0, 0, 3]$	$[2, 0, 0, 1, 0, 0, 1]$
3	$[4, 0, 2, 1, 3, 0, 2]$	$[0, 2, 0, 2, 3, 4, 1, 1, 0, 2]$
4	$[0, 1, 0, 0, 2]$	$[3, 0, 0, 3]$
5	$[1, 1, 0, 1, 0, 2, 2]$	$[0, 2, 1, 3, 4, 0, 4, 3, 1, 2]$
6	$[0, 2, 3, 0, 0, 0, 4]$	$[1, 0, 4, 1, 2, 1, 2, 2, 3, 2]$
7	$[2, 1, 2, 0, 2]$	$[4, 1, 3, 1, 0, 1]$
8	$[0, 1, 0, 0, 1]$	$[4, 0, 0, 0, 0, 0, 4]$
9	$[2, 1, 2, 1, 3]$	$[1, 4, 2, 3, 2, 1, 4]$
10	$[0, 2, 2, 4, 2, 3, 3]$	$[3, 3, 1, 0, 3, 3, 4, 2]$
11	$[1, 0, 2, 2, 1]$	$[0, 3, 0, 0, 1, 3, 4]$
12	$[3, 0, 0, 0, 0, 0, 4]$	$[3, 0, 0, 0, 0, 0, 0, 0, 0, 2]$
13	$[65, 91, 10, 106, 1, 101, 101]$	$[82, 74, 24, 11, 90, 56, 37, 1, 84, 78]$
14	$[101, 61, 60, 66, 81, 106, 106]$	$[61, 50, 0, 34, 105, 111, 114, 10, 50, 114]$
15	$[14, 122, 120, 97, 18, 52, 52]$	$[65, 77, 8, 119, 82, 115, 9, 24, 55, 5]$
16	$[34, 123, 16, 110, 98, 8, 122]$	$[16, 56, 121, 47, 45, 24, 37, 14, 18, 62]$
17	$[41, 49, 79, 124, 30, 0, 31]$	$[99, 65, 14, 65, 77, 97, 19, 18, 65, 44]$
18	$[93, 102, 2, 40, 70, 62, 62]$	$[84, 31, 4, 79, 46, 86, 21, 99, 78, 80]$
19	$[74, 30, 48, 92, 68, 86, 86]$	$[42, 92, 41, 8, 44, 33, 89, 74, 70]$
20	$[115, 52, 124, 101, 46, 118, 118]$	$[72, 25, 96, 111, 11, 1, 78, 68, 11, 52]$
21	$[98, 77, 69, 70, 95, 0, 71]$	$[124, 77, 107, 35, 15, 15, 60, 83, 0, 87]$
22	$[26, 14, 108, 115, 54, 0, 23]$	$[99, 11, 47, 86, 114, 72, 79, 85, 76, 28]$
23	$[8, 93, 6, 63, 0, 0, 17]$	$[66, 34, 69, 36, 102, 80, 67, 58, 63, 11]$
24	$[11, 61, 76, 17, 121, 119, 72]$	$[107, 122, 91, 48, 23, 80, 78, 7, 66, 70]$
25	$[15, 110, 29, 91, 88, 37, 30]$	$[79, 42, 65, 14, 116, 60, 104, 13, 19, 124]$
26	$[27, 89, 29, 41, 97, 0, 95]$	$[39, 104, 112, 37, 24, 86, 40, 96, 106, 41]$
27	$[40, 49, 81, 124, 80, 0, 70]$	$[40, 2, 108, 89, 53, 80, 21, 81, 106, 23]$
28	$[42, 115, 6, 51, 92, 0, 120]$	$[116, 114, 0, 104, 91, 83, 98, 85, 67, 104]$
29	$[118, 78, 74, 46, 1, 0, 4]$	$[18, 52, 56, 34, 13, 60, 31, 75, 48, 3]$
30	$[106, 72, 62, 28, 5, 52, 52]$	$[9, 108, 77, 83, 42, 56, 82, 93, 16, 65]$
31	$[24, 110, 68, 93, 25, 51, 51]$	$[100, 90, 48, 80, 85, 11, 99, 96, 61, 122]$
32	$[74, 7, 103, 82, 50, 106, 106]$	$[37, 31, 122, 86, 55, 109, 47, 56, 9, 106]$
33	$[81, 89, 25, 42, 47, 0, 115]$	$[118, 61, 18, 115, 70, 22, 32, 118, 96, 86]$
34	$[72, 26, 76, 88, 114, 48, 100]$	$[8, 120, 50, 110, 83, 41, 62, 83, 96, 14]$
35	$[11, 81, 113, 39, 41, 0, 1]$	$[1, 103, 23, 99, 69, 8, 95, 23, 71, 93]$
36	$[122, 109, 81, 91, 96, 0, 52]$	$[84, 53, 15, 69, 37, 10, 77, 93, 106, 109]$
37	$[73, 4, 65, 42, 111, 21, 21]$	$[106, 61, 13, 38, 81, 58, 66, 119, 68, 18]$
38	$[54, 46, 83, 88, 73, 0, 66]$	$[37, 56, 5, 58, 27, 101, 103, 75, 76, 118]$
39	$[35, 95, 73, 57, 97, 55, 11]$	$[49, 77, 20, 46, 65, 93, 88, 87, 58, 98]$
40	$[84, 103, 33, 110, 32, 0, 123]$	$[84, 2, 29, 51, 16, 32, 106, 33, 27, 108]$
41	$[79, 91, 108, 120, 67, 109, 59]$	$[60, 116, 32, 85, 67, 123, 105, 47, 106, 81]$

Table A.1. (*Continued*)

i	Q_i	A_i
42	[21, 51, 23, 80, 119, 0, 117]	[63, 5, 73, 61, 109, 53, 84, 118, 27, 80]
43	[27, 120, 55, 22, 45, 15, 15]	[49, 29, 14, 30, 81, 39, 34, 95, 86, 78]
44	[43, 77, 77, 56, 84, 0, 103]	[61, 13, 70, 13, 6, 48, 45, 18, 3, 67]
45	[94, 10, 122, 100, 1, 0, 4]	[88, 15, 39, 43, 68, 58, 40, 12, 102, 3]
46	[66, 59, 13, 87, 112, 90, 120]	[28, 113, 98, 102, 108, 32, 10, 47, 79, 123]
47	[20, 69, 29, 91, 17, 0, 108]	[116, 66, 101, 53, 70, 120, 11, 52, 13, 22]
48	[48, 95, 46, 56, 0, 0, 87]	[79, 43, 77, 60, 8, 32, 75, 36, 56, 66]
49	[113, 25, 33, 98, 118, 0, 15]	[31, 16, 85, 77, 61, 65, 14, 95, 27, 25]
50	[39, 114, 54, 95, 111, 13, 2]	[43, 57, 0, 86, 34, 100, 121, 72, 41, 116]
51	[66, 33, 74, 63, 80, 0, 1]	[1, 9, 108, 116, 77, 48, 117, 108, 124, 95]
52	[124, 50, 117, 26, 123, 99, 55]	[90, 0, 66, 20, 117, 102, 27, 66, 15, 34]
53	[121, 4, 78, 81, 72, 106, 106]	[27, 59, 68, 62, 33, 36, 79, 90, 76, 88]
54	[17, 100, 30, 50, 121, 0, 79]	[61, 39, 45, 36, 21, 7, 9, 12, 13, 94]
55	[33, 51, 24, 81, 101, 0, 91]	[94, 59, 88, 91, 123, 107, 41, 94, 118, 53]
56	[109, 71, 76, 95, 24, 19, 19]	[6, 97, 102, 32, 52, 66, 116, 118, 59, 113]
57	[122, 47, 9, 34, 18, 27, 27]	[61, 40, 113, 53, 38, 25, 101, 39, 49, 27]
58	[35, 113, 22, 92, 66, 116, 116]	[67, 60, 97, 9, 109, 48, 96, 72, 119, 24]
59	[60, 30, 116, 30, 79, 26, 57]	[11, 59, 102, 95, 14, 89, 108, 74, 29, 96]
60	[80, 103, 11, 110, 44, 0, 40]	[116, 78, 69, 78, 14, 119, 89, 88, 78, 83]
61	[20, 47, 75, 49, 124, 0, 54]	[41, 84, 59, 123, 116, 55, 103, 82, 38]
62	[122, 44, 102, 99, 76, 53, 53]	[81, 99, 80, 48, 83, 42, 51, 122, 123]
63	[90, 124, 47, 57, 100, 77, 77]	[112, 81, 12, 119, 23, 20, 20, 67, 64, 79]
64	[105, 2, 81, 79, 49, 70, 70]	[97, 80, 63, 66, 113, 71, 29, 59, 21, 23]
65	[78, 98, 65, 27, 1, 7, 7]	[34, 122, 109, 66, 97, 39, 61, 1, 31, 10]
66	[102, 12, 117, 103, 114, 106, 106]	[92, 0, 49, 52, 123, 1, 108, 53, 83, 60]
67	[87, 90, 117, 56, 97, 0, 101]	[56, 74, 26, 82, 15, 124, 0, 117, 8, 71]
68	[23, 0, 36, 47, 23, 122, 73]	[118, 27, 21, 68, 33, 79, 23, 37, 54, 118]
69	[31, 9, 42, 71, 41, 0, 114]	[31, 2, 23, 19, 86, 41, 27, 42, 21, 29]
70	[102, 117, 100, 39, 0, 0, 54]	[11, 82, 14, 58, 48, 41, 12, 60, 39, 79]
71	[100, 107, 98, 51, 71, 0, 83]	[76, 8, 75, 123, 37, 14, 67, 110, 113, 23]
72	[113, 3, 5, 76, 82, 66, 48]	[113, 103, 123, 59, 79, 13, 42, 104, 98, 81]
73	[96, 65, 113, 6, 1, 0, 4]	[50, 85, 63, 82, 76, 36, 84, 67, 8, 3]
74	[33, 98, 100, 89, 116, 0, 72]	[99, 123, 0, 45, 115, 44, 91, 15, 12, 45]
75	[86, 15, 89, 1, 114, 4, 4]	[5, 77, 100, 44, 65, 13, 118, 83, 54, 40]
76	[22, 1, 13, 38, 39, 0, 75]	[93, 24, 79, 6, 117, 93, 19, 113, 37, 28]
77	[13, 116, 105, 69, 28, 90, 15]	[96, 56, 43, 63, 83, 102, 64, 116, 68, 100]
78	[117, 48, 2, 31, 114, 38, 38]	[40, 84, 4, 66, 6, 16, 27, 92, 65, 41]
79	[8, 67, 93, 9, 70, 27, 27]	[99, 0, 103, 15, 114, 1, 29, 16, 30, 58]
80	[10, 115, 78, 21, 1, 47, 47]	[43, 113, 25, 79, 119, 63, 59, 1, 40, 65]
81	[26, 2, 33, 11, 103, 123, 123]	[119, 32, 56, 79, 74, 124, 23, 37, 106, 108]
82	[97, 110, 101, 35, 6, 14, 14]	[73, 33, 67, 90, 108, 105, 105, 75, 57, 11]
83	[53, 1, 118, 45, 98, 54, 54]	[32, 62, 121, 122, 95, 7, 28, 38, 31]

(*Continued*)

Table A.1. (*Continued*)

i	Q_i	A_i
84	[105, 101, 12, 103, 110, 0, 17]	[80, 31, 37, 114, 92, 38, 9, 34, 62]
85	[18, 104, 117, 29, 82, 0, 45]	[66, 62, 14, 86, 105, 69, 100, 6, 105, 23]
86	[52, 70, 94, 60, 70, 111, 89]	[38, 59, 70, 46, 27, 41, 64, 114, 3, 119]
87	[74, 24, 42, 115, 94, 0, 85]	[40, 86, 52, 14, 59, 78, 69, 117, 21, 24]
88	[113, 101, 49, 43, 88, 21, 21]	[59, 84, 74, 16, 62, 24, 7, 63, 103, 21]
89	[25, 124, 13, 117, 109, 89, 89]	[46, 119, 8, 41, 15, 79, 92, 94, 37, 74]
90	[42, 19, 109, 33, 7, 0, 98]	[96, 37, 50, 98, 114, 28, 80, 96, 94, 16]
91	[14, 19, 6, 116, 111, 0, 95]	[18, 24, 100, 2, 14, 19, 35, 79, 34, 114]
92	[112, 4, 10, 33, 120, 27, 27]	[21, 37, 76, 55, 42, 60, 11, 97, 13, 50]
93	[20, 116, 62, 58, 16, 97, 48]	[16, 58, 85, 111, 76, 105, 57, 96, 90, 80]
94	[32, 41, 113, 30, 42, 25, 25]	[73, 109, 32, 76, 50, 11, 0, 103, 30, 52]
95	[25, 117, 14, 12, 16, 110, 110]	[61, 59, 24, 124, 19, 23, 115, 115, 16, 48]
96	[36, 15, 12, 62, 106, 0, 11]	[48, 55, 122, 18, 79, 83, 63, 18, 100, 39]
97	[123, 48, 13, 76, 22, 0, 61]	[81, 117, 79, 70, 13, 38, 47, 93, 37, 27]
98	[7, 17, 8, 47, 77, 83, 83]	[104, 100, 77, 26, 99, 57, 103, 44, 46, 115]
99	[86, 20, 60, 90, 28, 22, 11]	[106, 89, 116, 38, 44, 109, 29, 85, 36, 44]
100	[82, 22, 48, 32, 26, 0, 107]	[64, 43, 59, 46, 108, 109, 19, 27, 30, 110]
101	[66, 65, 123, 66, 6, 97, 97]	[99, 119, 34, 100, 32, 43, 12, 11, 56, 40]
102	[44, 80, 113, 7, 14, 0, 101]	[31, 4, 108, 2, 74, 117, 57, 1, 66, 71]
103	[34, 107, 102, 41, 20, 0, 28]	[57, 82, 37, 100, 29, 25, 89, 21, 44, 71]
104	[117, 46, 10, 45, 20, 21, 21]	[15, 39, 93, 64, 51, 51, 5, 74, 25, 100]
105	[29, 74, 17, 123, 64, 0, 57]	[25, 52, 105, 106, 39, 36, 107, 27, 21, 89]
106	[41, 80, 74, 44, 81, 24, 24]	[121, 25, 41, 13, 18, 66, 0, 9, 44, 15]
107	[24, 93, 69, 67, 86, 71, 71]	[59, 37, 109, 110, 89, 108, 91, 91, 86, 102]
108	[60, 85, 67, 55, 27, 0, 66]	[102, 38, 113, 88, 11, 30, 56, 88, 6, 63]
109	[82, 72, 36, 21, 60, 0, 24]	[18, 63, 28, 36, 90, 14, 112, 123, 123, 47]
110	[47, 87, 48, 101, 14, 30, 30]	[5, 6, 14, 20, 116, 35, 9, 83, 100, 91]
111	[30, 102, 34, 1, 64, 67, 46]	[105, 73, 114, 55, 95, 109, 120, 99, 32, 2]
112	[70, 8, 76, 68, 28, 0, 37]	[42, 95, 66, 114, 76, 55, 7, 117, 59, 106]
113	[101, 54, 102, 7, 69, 44, 44]	[45, 46, 69, 105, 92, 64, 49, 30, 6, 98]
114	[16, 26, 36, 119, 107, 28, 79]	[21, 19, 99, 55, 30, 24, 108, 15, 58, 30]
115	[43, 28, 8, 80, 105, 0, 22]	[35, 34, 61, 6, 23, 24, 51, 106, 83, 124]
116	[11, 10, 70, 11, 100, 90, 90]	[92, 97, 82, 46, 80, 34, 75, 79, 63, 31]
117	[23, 122, 87, 114, 57, 0, 35]	[24, 15, 26, 27, 63, 60, 28, 21, 106, 51]
118	[80, 32, 122, 83, 33, 109, 109]	[112, 24, 80, 68, 88, 79, 0, 49, 83, 85]
119	[46, 110, 56, 91, 41, 31, 31]	[110, 115, 100, 70, 120, 24, 118, 88, 83, 111]
120	[102, 100, 90, 99, 61, 0, 91]	[31, 105, 14, 35, 90, 31, 23, 84, 102, 77]

Table A.2. Minimal polynomials $F(z) = z^3 - 3Q_iz + 2A_i$ for the 121 cubic fields of unusual discriminant $D = 1 + t^3 + 3t^9 + 2t^{12}$ and signature $(1, 1; 1, 2)$.

i	Q_i	A_i
0	[1, 0, 0, 3]	[3, 0, 0, 1, 0, 0, 4, 0, 0, 2]
1	[113, 32, 7, 84, 121, 47]	[61, 84, 44, 46, 83, 46, 65, 52, 116, 95]
2	[122, 80, 101, 40, 73, 7]	[37, 40, 30, 6, 44, 6, 10, 85, 99, 93]
3	[74, 41, 47, 31, 112, 101]	[59, 31, 83, 100, 30, 100, 78, 15, 92, 117]
4	[48, 74, 36, 112, 11, 84]	[74, 18, 49, 78, 56, 115, 81, 72, 56, 73]
5	[102, 122, 60, 73, 66, 31]	[122, 88, 103, 10, 39, 91, 33, 120, 39, 121]
6	[8, 113, 58, 121, 79, 40]	[113, 50, 9, 65, 63, 98, 42, 111, 63, 112]
7	[3, 3, 3, 3, 1, 2]	[4, 0, 1, 4, 1, 3, 3, 1, 2, 2]
8	[2, 0, 0, 2, 0, 1]	[2, 1, 2, 3, 2, 1, 3, 3, 4, 2]
9	[4, 2, 3, 0, 1]	[2, 1, 3, 0, 1, 4]
10	[12, 41, 95, 19, 112, 43]	[22, 52, 123, 112, 71, 87, 30, 26, 7, 112]
11	[75, 32, 93, 51, 121, 34]	[28, 85, 70, 121, 110, 17, 83, 105, 101, 121]
12	[67, 80, 117, 89, 73, 82]	[107, 15, 114, 73, 124, 54, 44, 20, 47, 73]
13	[117, 74, 20, 66, 97, 62]	[16, 26, 105, 105, 17, 80, 91, 117, 81, 101]
14	[95, 113, 26, 11, 90, 38]	[53, 105, 20, 20, 54, 41, 115, 95, 42, 47]
15	[93, 122, 105, 79, 119, 55]	[86, 20, 26, 26, 87, 32, 98, 93, 33, 7]
16	[102, 84, 79, 71, 88, 110]	[46, 4, 67, 41, 118, 96, 108, 14, 66, 108]
17	[8, 31, 11, 124, 50, 71]	[100, 4, 75, 80, 94, 118, 29, 69, 79, 29]
18	[48, 40, 66, 110, 18, 124]	[6, 4, 12, 32, 96, 94, 23, 77, 11, 23]
19	[4, 4, 1, 4]	[3, 3, 1, 0, 0, 0, 1]
20	[2, 1, 0, 2, 0, 3]	[2, 0, 1, 3, 3, 1, 3, 1, 1, 2]
21	[2, 0, 4, 0, 1, 4]	[2, 4, 4, 1, 0, 2, 2, 3, 4, 1]
22	[1, 4, 0, 0, 2, 3]	[2, 2, 2, 2, 3, 2, 4, 0, 0, 4]
23	[2, 0, 2, 1]	[0, 4, 2, 4, 0, 0, 1]
24	[2, 2, 0, 3, 1, 1]	[0, 0, 1, 2, 2, 3, 4, 1, 4, 3]
25	[106, 0, 0, 23]	[47, 0, 0, 8, 0, 0, 4]
26	[21, 0, 0, 29]	[7, 0, 0, 102, 0, 0, 4]
27	[27, 0, 0, 108]	[101, 0, 0, 48, 0, 0, 4]
28	[124, 34, 85, 40, 72, 31]	[94, 23, 97, 40, 90, 46, 35, 75, 67, 10]
29	[110, 43, 52, 84, 120, 40]	[96, 108, 119, 84, 97, 100, 64, 12, 75, 65]
30	[71, 82, 15, 31, 111, 84]	[118, 29, 90, 31, 119, 6, 57, 67, 12, 78]
31	[45, 117, 91, 88, 60, 78]	[80, 103, 106, 16, 109, 55, 22, 119, 43, 38]
32	[104, 93, 98, 50, 58, 10]	[32, 9, 27, 86, 25, 38, 107, 90, 82, 62]
33	[5, 95, 115, 18, 36, 65]	[41, 49, 21, 53, 24, 62, 28, 97, 34, 55]
34	[2, 2, 0, 2, 4, 4]	[2, 0, 2, 2, 3, 4, 3, 3, 0, 1]
35	[3, 3, 4, 0, 3]	[4, 3, 4, 2, 3, 0, 2]
36	[4, 0, 0, 1, 1, 2]	[2, 2, 3, 2, 0, 0, 4, 3, 4, 3]
37	[62, 66, 17, 48, 36, 37]	[25, 19, 112, 26, 97, 117, 69, 106, 109, 112]
38	[38, 11, 54, 8, 58, 59]	[109, 51, 121, 105, 90, 95, 14, 21, 24, 121]
39	[55, 79, 87, 102, 60, 61]	[24, 89, 73, 20, 119, 93, 77, 27, 25, 73]
40	[105, 95, 94, 77, 120, 79]	[35, 53, 108, 124, 49, 85, 81, 4, 48, 7]

(*Continued*)

Table A.2. (*Continued*)

i	Q_i	A_i
41	[70, 95, 25, 79, 22, 53]	[60, 35, 36, 52, 103, 7, 94, 73, 18, 32]
42	[89, 46, 4, 50, 76, 40]	[121, 34, 44, 2, 70, 95, 93, 75, 93, 61]
43	[34, 71, 87, 46, 72, 124]	[106, 114, 106, 22, 82, 63, 12, 124, 93, 37]
44	[117, 78, 22, 90, 28, 68]	[67, 12, 1, 92, 65, 37, 34, 49, 109, 7]
45	[64, 78, 23, 43, 48, 112]	[86, 92, 33, 36, 96, 82, 61, 31, 90, 90]
46	[124, 105, 57, 77, 86, 18]	[109, 109, 55, 113, 73, 70, 103, 81, 60, 37]
47	[79, 61, 6, 77, 24]	[61, 73, 40, 97, 38, 8, 58]
48	[30, 90, 19, 59, 23, 51]	[64, 88, 40, 3, 78, 103, 76, 94, 52, 52]
49	[53, 86, 39, 9, 46, 16]	[93, 56, 91, 79, 9, 76, 95, 57, 107, 11]
50	[18, 20, 122, 37, 11, 74]	[10, 81, 100, 97, 65, 91, 64, 52, 64, 124]
51	[116, 110, 18, 48, 96, 82]	[72, 70, 57, 38, 22, 91, 24, 4, 36, 79]
52	[117, 86, 26, 6, 65, 52]	[57, 77, 91, 105, 110, 28, 82, 68, 71, 107]
53	[87, 87, 25, 111, 23, 71]	[66, 104, 35, 90, 107, 77, 89, 25, 22, 114]
54	[81, 82, 27, 91, 109]	[39, 55, 78, 56, 34, 104, 36]
55	[85, 7, 48, 4, 33, 108]	[24, 17, 4, 105, 34, 106, 21, 57, 97, 59]
56	[71, 4, 44, 119, 46, 38]	[24, 75, 9, 68, 58, 27, 96, 61, 17, 17]
57	[67, 115, 119, 79, 124, 33]	[94, 22, 67, 79, 67, 45, 38, 69, 95, 16]
58	[107, 3, 65, 14, 107, 35]	[40, 120, 106, 121, 102, 59, 44, 23, 86, 56]
59	[5, 80, 66, 57, 10, 12]	[40, 46, 68, 55, 105, 27, 114, 22, 0, 29]
60	[96, 70, 93, 56, 109]	[70, 31, 3, 61, 11, 18, 36]
61	[65, 22, 4, 65, 74, 38]	[12, 25, 28, 27, 86, 92, 44, 25, 122, 86]
62	[12, 0, 6, 23, 89]	[18, 0, 83, 6, 72, 48, 13]
63	[59, 99, 61, 92, 19, 18]	[115, 24, 15, 93, 28, 106, 43, 75, 52, 117]
64	[118, 32, 9, 60, 51]	[123, 110, 98, 99, 34, 44, 68]
65	[70, 54, 1, 108, 46, 23]	[58, 83, 121, 12, 87, 120, 14, 6, 45, 104]
66	[115, 99, 57, 4, 15, 54]	[101, 74, 95, 95, 23, 64, 24, 10, 25, 22]
67	[98, 92, 64, 4, 52, 87]	[47, 113, 93, 93, 29, 35, 25, 78, 109, 28]
68	[96, 80, 103, 36, 89]	[70, 124, 91, 92, 82, 30, 13]
69	[114, 87, 1, 23, 6, 29]	[60, 44, 73, 75, 17, 72, 77, 100, 5, 45]
70	[94, 114, 117, 63, 24]	[114, 84, 3, 37, 79, 50, 58]
71	[22, 3, 10, 77, 22, 57]	[31, 72, 21, 73, 48, 61, 30, 29, 16, 63]
72	[104, 41, 11, 64, 78, 75]	[31, 6, 13, 62, 20, 106, 123, 28, 0, 108]
73	[10, 28, 4, 10, 113, 55]	[75, 109, 107, 106, 16, 116, 30, 109, 74, 16]
74	[75, 0, 100, 29, 19]	[50, 0, 44, 100, 111, 8, 76]
75	[61, 92, 37, 116, 51, 50]	[98, 25, 52, 117, 107, 21, 34, 67, 85, 95]
76	[66, 37, 100, 69, 25]	[37, 112, 31, 90, 55, 102, 60]
77	[83, 119, 51, 61, 29, 89]	[35, 18, 31, 3, 65, 49, 68, 118, 85, 85]
78	[71, 20, 64, 69, 16, 50]	[24, 24, 62, 122, 112, 114, 49, 42, 36, 59]
79	[20, 93, 118, 69, 72, 66]	[57, 86, 23, 71, 9, 15, 42, 4, 8, 101]
80	[114, 93, 109, 66, 28, 86]	[36, 57, 58, 85, 49, 101, 118, 112, 50, 80]
81	[19, 6, 4, 88, 68, 31]	[73, 82, 30, 2, 114, 93, 117, 67, 117, 37]
82	[95, 65, 28, 119, 107, 13]	[12, 75, 1, 116, 10, 59, 82, 9, 24, 101]
83	[35, 65, 29, 34, 8, 121]	[16, 116, 81, 58, 94, 43, 37, 84, 119, 119]

Table A.2. (*Continued*)

i	Q_i	A_i
84	[82, 110, 17, 6, 111, 71]	[21, 123, 21, 28, 43, 39, 75, 71, 117, 59]
85	[15, 101, 8, 4, 81, 23]	[25, 54, 4, 20, 82, 21, 27, 64, 90, 61]
86	[110, 4, 30, 97, 6, 55]	[25, 67, 103, 13, 60, 106, 94, 37, 54, 54]
87	[12, 98, 97, 66, 71, 81]	[118, 28, 12, 66, 12, 5, 55, 14, 93, 53]
88	[99, 124, 50, 8, 94, 43]	[111, 114, 64, 55, 28, 115, 25, 4, 58, 66]
89	[86, 16, 56, 103, 6, 53]	[117, 63, 115, 66, 103, 68, 93, 64, 22, 79]
90	[50, 26, 74, 59, 79, 113]	[78, 42, 46, 90, 10, 115, 35, 85, 35, 71]
91	[17, 17, 109, 120, 29, 110]	[11, 45, 57, 119, 22, 69, 19, 109, 28, 123]
92	[42, 43, 106, 115, 24]	[56, 62, 65, 63, 82, 45, 58]
93	[95, 16, 105, 100, 10, 85]	[64, 69, 115, 20, 124, 107, 43, 13, 110, 22]
94	[93, 53, 20, 46, 78, 15]	[35, 14, 98, 26, 71, 22, 34, 76, 124, 28]
95	[54, 54, 24, 72, 108, 124]	[79, 5, 64, 97, 28, 14, 51, 24, 107, 70]
96	[33, 34, 21, 98, 25]	[63, 38, 10, 39, 43, 5, 60]
97	[124, 4, 83, 90, 100, 62]	[109, 12, 49, 76, 36, 21, 118, 59, 87, 87]
98	[75, 91, 90, 11, 110, 42]	[96, 107, 75, 11, 75, 104, 62, 77, 117, 86]
99	[52, 47, 102, 4, 42, 29]	[109, 87, 4, 26, 43, 27, 106, 35, 119, 37]
100	[88, 105, 113, 61, 66, 122]	[65, 33, 6, 119, 78, 98, 57, 15, 57, 110]
101	[92, 71, 88, 102, 118, 34]	[120, 123, 35, 62, 107, 98, 109, 4, 60, 11]
102	[16, 53, 63, 49, 100, 86]	[95, 39, 98, 11, 49, 13, 117, 35, 28, 66]
103	[78, 107, 4, 78, 122, 62]	[67, 24, 22, 21, 53, 99, 83, 24, 113, 53]
104	[67, 0, 46, 108, 51]	[88, 0, 30, 46, 120, 102, 68]
105	[37, 116, 59, 99, 89, 88]	[91, 109, 85, 95, 22, 27, 82, 12, 15, 93]
106	[91, 116, 35, 4, 85, 17]	[7, 122, 117, 117, 108, 57, 109, 65, 24, 107]
107	[94, 41, 49, 58, 19]	[114, 71, 115, 116, 43, 83, 76]
108	[123, 17, 1, 29, 100, 108]	[36, 30, 112, 67, 54, 111, 69, 46, 104, 5]
109	[118, 123, 95, 39, 25]	[123, 40, 3, 59, 66, 88, 60]
110	[28, 3, 78, 69, 28, 64]	[84, 111, 27, 112, 8, 37, 83, 108, 53, 39]
111	[45, 32, 79, 35, 65, 67]	[84, 100, 76, 38, 26, 21, 70, 107, 0, 23]
112	[43, 124, 54, 100, 120, 110]	[27, 70, 27, 107, 34, 56, 67, 110, 95, 61]
113	[93, 10, 107, 97, 22, 76]	[75, 67, 1, 99, 78, 61, 43, 103, 25, 47]
114	[57, 10, 108, 82, 102, 73]	[53, 99, 42, 60, 118, 34, 59, 40, 97, 97]
115	[44, 97, 89, 37, 108, 19]	[57, 50, 84, 3, 10, 9, 13, 96, 15, 15]
116	[110, 26, 35, 14, 53, 88]	[25, 25, 38, 74, 121, 123, 9, 33, 58, 61]
117	[11, 59, 46, 14, 109]	[59, 121, 84, 119, 62, 48, 36]
118	[26, 117, 96, 14, 111, 11]	[64, 16, 29, 110, 103, 52, 33, 4, 102, 47]
119	[123, 117, 24, 11, 107, 16]	[58, 64, 60, 15, 9, 47, 96, 121, 88, 41]
120	[51, 100, 4, 18, 13, 84]	[112, 43, 83, 2, 123, 117, 95, 12, 95, 59]

Table A.3. Minimal polynomials $F(z) = z^3 - 3Q_i z + 2A_i$ for the 243 cubic fields of unusual discriminant $D = 1 + t^3 + 3t^9 + 2t^{12}$ and signature $(3, 1)$.

i	Q_i	A_i
0	[104, 75, 45, 91, 39, 102]	[18, 53, 94, 29, 86, 0, 17, 57, 3]
1	[85, 30, 91, 94, 34, 47]	[10, 93, 38, 18, 35, 60, 87, 85, 77]
2	[67, 1, 99, 98, 63, 55]	[106, 119, 77, 103, 26, 10, 53, 80, 112]
3	[3, 82, 38, 112, 122, 97]	[109, 36, 56, 48, 75, 40, 42, 8, 48]
4	[54, 60, 20, 96, 43, 38]	[4, 49, 47, 67, 96, 114, 107, 114, 36]
5	[13, 113, 8, 91, 1, 16]	[13, 53, 19, 51, 92, 33, 25, 0, 2]
6	[2, 111, 114, 62, 7, 33]	[67, 51, 5, 27, 36, 25, 115, 51, 63]
7	[78, 117, 107, 42, 113, 104]	[10, 65, 27, 72, 2, 106, 0, 47, 98]
8	[99, 112, 43, 42, 41, 96]	[59, 52, 70, 93, 6, 117, 80, 117, 19]
9	[65, 95, 22, 33, 122, 45]	[78, 10, 106, 111, 2, 21, 0, 7, 91]
10	[92, 121, 34, 33, 32, 94]	[61, 85, 114, 117, 100, 95, 41, 95, 51]
11	[2, 120, 123, 38, 101, 81]	[12, 89, 104, 106, 58, 109, 98, 89, 39]
12	[15, 83, 115, 118, 82, 7]	[78, 117, 55, 50, 57, 36, 17, 15, 69]
13	[12, 1, 92, 91, 39, 62]	[21, 97, 69, 49, 105, 78, 86, 41, 121]
14	[45, 67, 5, 115, 56, 48]	[50, 86, 118, 108, 16, 0, 54, 64, 3]
15	[76, 122, 102, 115, 1, 53]	[76, 86, 51, 89, 116, 81, 109, 0, 2]
16	[3, 43, 55, 121, 74, 90]	[24, 58, 63, 8, 67, 31, 33, 102, 8]
17	[87, 36, 26, 94, 34, 55]	[4, 9, 7, 12, 94, 123, 22, 123, 58]
18	[3, 34, 62, 73, 113, 119]	[25, 60, 39, 102, 12, 84, 81, 48, 102]
19	[17, 58, 105, 118, 82, 62]	[4, 103, 101, 75, 118, 70, 28, 70, 60]
20	[68, 74, 48, 98, 1, 86]	[68, 16, 89, 19, 99, 42, 24, 0, 2]
21	[116, 73, 82, 81, 80, 118]	[37, 15, 123, 95, 46, 93, 32, 93, 89]
22	[2, 72, 70, 55, 47, 42]	[75, 19, 45, 21, 60, 24, 91, 19, 56]
23	[10, 93, 28, 81, 74, 5]	[65, 78, 21, 120, 2, 27, 0, 101, 115]
24	[75, 1, 116, 115, 56, 38]	[27, 90, 14, 9, 20, 65, 16, 32, 73]
25	[5, 12, 104, 98, 63, 8]	[88, 16, 96, 23, 53, 0, 87, 35, 3]
26	[52, 44, 98, 96, 43, 101]	[65, 95, 62, 88, 64, 58, 54, 52, 14]
27	[28, 96, 58, 61, 62, 70]	[64, 18, 9, 1, 59, 5, 68, 65, 87]
28	[7, 20, 119, 29, 120, 73]	[17, 1, 115, 12, 106, 53, 105, 85, 114]
29	[10, 8, 70, 50, 26, 116]	[85, 106, 12, 100, 73, 76, 20, 9, 9]
30	[40, 44, 17, 96, 51, 2]	[73, 34, 21, 33, 112, 22, 124, 81, 53]
31	[56, 92, 4, 39, 76, 119]	[104, 19, 12, 14, 21, 7, 71, 100, 35]
32	[23, 90, 81, 27, 0, 70]	[62, 47, 88, 0, 107, 112, 110, 58, 73]
33	[47, 11, 70, 30, 42, 57]	[68, 85, 8, 24, 4, 109, 120, 96, 30]
34	[64, 63, 65, 98, 46, 90]	[72, 83, 108, 60, 54, 79, 25, 98, 8]
35	[10, 110, 96, 11, 18, 88]	[41, 95, 18, 62, 77, 12, 7, 91, 105]
36	[7, 79, 114, 83, 33, 64]	[13, 15, 102, 25, 4, 24, 72, 94, 83]
37	[35, 39, 10, 91, 6, 119]	[111, 44, 23, 36, 87, 66, 109, 91, 102]
38	[78, 124, 94, 79, 50, 18]	[32, 93, 50, 38, 69, 75, 101, 115, 20]
39	[107, 94, 60, 37, 38, 114]	[35, 50, 103, 1, 61, 104, 13, 10, 17]
40	[101, 26, 97, 108, 72, 112]	[54, 1, 98, 75, 21, 86, 20, 15, 123]
41	[78, 102, 114, 88, 105, 99]	[15, 21, 75, 46, 112, 68, 26, 103, 103]

Table A.3. (*Continued*)

i	Q_i	A_i
42	[63, 116, 4, 56, 68, 97]	[45, 51, 75, 77, 27, 101, 110, 46, 57]
43	[29, 119, 42, 106, 0, 114]	[38, 7, 18, 0, 22, 121, 124, 60, 112]
44	[31, 30, 54, 94, 89, 2]	[112, 82, 27, 81, 121, 28, 71, 42, 86]
45	[39, 99, 4, 63, 13, 90]	[5, 89, 67, 69, 106, 47, 124, 6, 64]
46	[108, 97, 33, 21, 0, 123]	[55, 101, 50, 0, 28, 73, 71, 36, 121]
47	[84, 83, 87, 118, 19, 2]	[121, 43, 106, 42, 73, 107, 110, 33, 16]
48	[65, 71, 118, 66, 88, 50]	[80, 117, 88, 55, 14, 67, 47, 98, 26]
49	[101, 66, 123, 44, 81, 35]	[76, 52, 48, 109, 4, 25, 111, 118, 44]
50	[57, 56, 78, 115, 100, 97]	[120, 30, 29, 58, 17, 11, 24, 115, 48]
51	[22, 118, 36, 59, 55, 123]	[57, 88, 49, 1, 37, 45, 76, 78, 54]
52	[47, 105, 90, 23, 111, 121]	[87, 1, 91, 67, 27, 16, 26, 52, 70]
53	[65, 48, 123, 18, 20, 92]	[52, 27, 67, 6, 121, 13, 105, 49, 49]
54	[43, 29, 11, 13, 62, 14]	[43, 99, 3, 118, 6, 42, 61, 76, 96]
55	[7, 3, 89, 58, 110, 90]	[73, 90, 74, 85, 71, 111, 43, 82, 3]
56	[5, 51, 122, 57, 68, 108]	[27, 20, 100, 48, 41, 53, 102, 115, 96]
57	[78, 67, 9, 116, 27, 103]	[64, 71, 71, 80, 121, 66, 118, 97, 33]
58	[34, 41, 34, 116, 57, 31]	[64, 36, 111, 3, 72, 50, 3, 88, 1]
59	[40, 45, 70, 12, 88, 112]	[82, 54, 87, 78, 115, 112, 121, 52, 76]
60	[99, 89, 0, 55, 10, 9]	[0, 18, 34, 58, 44, 119, 100, 119, 106]
61	[14, 17, 16, 118, 108, 99]	[31, 39, 90, 101, 113, 101, 49, 9, 13]
62	[110, 99, 7, 116, 55, 50]	[21, 61, 59, 2, 71, 94, 53, 12, 93]
63	[92, 19, 0, 62, 78, 103]	[0, 50, 82, 60, 30, 97, 46, 97, 21]
64	[77, 54, 53, 96, 23, 92]	[84, 56, 119, 47, 122, 47, 9, 103, 76]
65	[124, 92, 101, 99, 62, 88]	[27, 37, 61, 2, 110, 118, 86, 75, 117]
66	[104, 89, 74, 64, 13, 23]	[106, 26, 46, 8, 32, 86, 48, 98, 94]
67	[34, 108, 79, 76, 38, 77]	[34, 92, 3, 96, 100, 33, 37, 68, 94]
68	[101, 3, 19, 60, 124, 119]	[112, 119, 113, 15, 110, 120, 34, 43, 3]
69	[65, 12, 103, 99, 106, 49]	[35, 110, 110, 41, 73, 11, 96, 90, 81]
70	[82, 32, 82, 99, 64, 84]	[35, 58, 120, 3, 111, 88, 3, 18, 1]
71	[31, 5, 114, 75, 18, 121]	[43, 87, 17, 65, 98, 121, 73, 85, 68]
72	[84, 104, 123, 67, 50, 73]	[34, 17, 54, 10, 91, 73, 112, 15, 13]
73	[10, 75, 49, 92, 21, 9]	[57, 124, 124, 32, 112, 79, 94, 119, 42]
74	[43, 80, 43, 92, 35, 40]	[57, 60, 72, 3, 120, 18, 3, 50, 1]
75	[69, 87, 86, 94, 29, 116]	[40, 63, 97, 7, 74, 7, 103, 49, 68]
76	[71, 116, 47, 92, 38, 18]	[106, 59, 37, 2, 124, 96, 16, 67, 95]
77	[116, 51, 0, 38, 65, 49]	[0, 88, 43, 36, 83, 90, 6, 90, 27]
78	[47, 3, 51, 36, 71, 97]	[121, 97, 122, 52, 124, 72, 82, 34, 3]
79	[45, 19, 113, 35, 76, 29]	[21, 105, 6, 102, 80, 16, 8, 91, 118]
80	[82, 23, 66, 68, 55, 69]	[82, 116, 3, 94, 46, 81, 59, 13, 118]
81	[116, 30, 77, 79, 44, 94]	[118, 114, 121, 95, 107, 4, 24, 55, 13]
82	[67, 54, 36, 109, 11, 55]	[98, 25, 18, 42, 107, 39, 21, 49, 106]
83	[118, 18, 98, 35, 15, 52]	[2, 123, 117, 89, 17, 43, 27, 19, 67]

(*Continued*)

Table A.3. (*Continued*)

i	Q_i	A_i
84	[87, 60, 83, 21, 121, 96]	[89, 116, 110, 19, 8, 69, 36, 88, 67]
85	[118, 36, 26, 124, 74, 25]	[2, 28, 113, 23, 15, 35, 109, 91, 2]
86	[51, 73, 59, 67, 116, 24]	[33, 36, 11, 10, 47, 50, 32, 62, 69]
87	[31, 57, 73, 93, 93, 96]	[26, 51, 84, 59, 66, 122, 28, 113, 35]
88	[41, 104, 1, 113, 15]	[116, 82, 89, 77, 58, 73, 26, 37]
89	[27, 18, 105, 121, 43, 39]	[37, 16, 66, 72, 48, 92, 51, 102, 19]
90	[79, 69, 46, 75, 97, 71]	[31, 11, 107, 68, 27, 11, 4, 27, 35]
91	[1, 17, 120, 99, 75, 117]	[113, 79, 76, 36, 18, 35, 85, 81, 122]
92	[5, 94, 7, 15, 96, 93]	[103, 26, 78, 51, 97, 52, 48, 69, 29]
93	[14, 84, 102, 60, 40, 95]	[96, 64, 99, 61, 41, 63, 52, 84, 109]
94	[12, 46, 64, 30, 42, 71]	[118, 70, 108, 70, 56, 116, 86, 20, 47]
95	[59, 122, 100, 96, 107]	[84, 112, 71, 8, 118, 66, 39, 87, 48]
96	[117, 32, 53, 102, 79, 118]	[58, 70, 57, 59, 106, 115, 113, 50, 3]
97	[61, 43, 79, 29, 27, 9]	[7, 73, 117, 105, 75, 32, 66, 17, 35]
98	[80, 36, 64, 9, 56, 74]	[110, 78, 119, 107, 74, 10, 69, 106, 71]
99	[21, 18, 68, 31, 67, 96]	[61, 83, 56, 3, 116, 44, 9, 73, 73]
100	[75, 7, 98, 84, 67, 49]	[50, 16, 122, 52, 101, 104, 30, 112, 18]
101	[117, 13, 74, 76, 83, 38]	[99, 16, 97, 32, 9, 60, 69, 67, 66]
102	[103, 77, 8, 32, 29, 6]	[81, 22, 29, 111, 78, 23, 31, 9, 12]
103	[115, 23, 11, 24, 113, 93]	[39, 109, 117, 51, 75, 40, 118, 3, 40]
104	[1, 99, 22, 108, 5, 93]	[18, 13, 111, 92, 124, 67, 20, 38, 54]
105	[115, 55, 36, 111, 107, 25]	[39, 22, 65, 68, 81, 43, 42, 107, 120]
106	[14, 43, 84, 36, 62, 117]	[54, 96, 5, 107, 26, 62, 87, 113, 114]
107	[100, 36, 9, 91, 31, 57]	[16, 23, 65, 28, 71, 16, 19, 6, 25]
108	[96, 50, 91, 57, 52, 85]	[2, 70, 95, 19, 54, 34, 106, 51, 12]
109	[99, 83, 69, 66, 30, 118]	[96, 123, 73, 93, 22, 4, 25, 62, 76]
110	[12, 87, 58, 24, 79, 62]	[91, 109, 50, 33, 22, 56, 27, 9, 21]
111	[96, 58, 105, 71, 113, 109]	[2, 107, 122, 29, 52, 57, 24, 115, 2]
112	[89, 112, 61, 12, 99, 25]	[81, 58, 79, 78, 7, 88, 80, 38, 14]
113	[17, 36, 44, 27, 73, 94]	[19, 99, 124, 51, 102, 14, 58, 18, 12]
114	[84, 64, 112, 117, 117, 94]	[105, 89, 40, 61, 11, 74, 107, 122, 57]
115	[32, 45, 1, 122, 52]	[99, 43, 19, 69, 60, 112, 105, 59]
116	[106, 50, 20, 73, 34, 56]	[59, 53, 11, 111, 8, 116, 89, 48, 51]
117	[66, 14, 6, 67, 90, 110]	[84, 79, 22, 13, 106, 79, 4, 106, 57]
118	[1, 54, 72, 92, 67, 95]	[122, 66, 68, 58, 50, 57, 15, 42, 74]
119	[104, 118, 101, 52, 94, 117]	[49, 105, 65, 89, 90, 85, 8, 14, 108]
120	[61, 74, 46, 94, 22]	[40, 121, 110, 102, 96, 11, 56, 17, 8]
121	[77, 40, 48, 36, 31, 93]	[94, 35, 92, 37, 32, 39, 85, 40, 24]
122	[75, 6, 35, 83, 33, 110]	[96, 114, 23, 114, 63, 99, 16, 26, 7]
123	[37, 34, 66, 108, 106, 103]	[101, 112, 95, 20, 67, 80, 11, 54, 57]
124	[41, 58, 35, 103, 63, 113]	[124, 65, 97, 22, 113, 78, 14, 21, 110]
125	[95, 80, 86, 48, 66, 96]	[60, 114, 64, 61, 21, 98, 122, 88, 3]
126	[67, 101, 91, 40, 12, 9]	[88, 53, 74, 85, 47, 45, 83, 121, 50]

Table A.3. (*Continued*)

i	Q_i	A_i
127	[95, 76, 113, 68, 44, 55]	[92, 53, 90, 80, 103, 36, 14, 12, 11]
128	[27, 50, 13, 84, 12, 94]	[37, 44, 63, 3, 99, 30, 103, 112, 112]
129	[49, 69, 102, 80, 108, 100]	[42, 28, 108, 120, 65, 29, 84, 103, 75]
130	[98, 29, 79, 25, 122, 117]	[56, 24, 95, 89, 67, 31, 96, 3, 31]
131	[1, 92, 28, 23, 104, 117]	[50, 76, 120, 116, 71, 12, 26, 55, 87]
132	[46, 58, 103, 115, 84, 64]	[53, 29, 10, 107, 110, 53, 51, 100, 109]
133	[98, 62, 58, 120, 22, 109]	[56, 28, 10, 13, 42, 34, 33, 22, 72]
134	[77, 34, 40, 58, 38, 95]	[87, 94, 104, 22, 105, 38, 17, 122, 123]
135	[92, 44, 14, 11, 83, 96]	[94, 70, 112, 117, 28, 4, 109, 38, 68]
136	[75, 17, 60, 25, 66, 38]	[115, 24, 88, 81, 28, 63, 106, 103, 27]
137	[94, 88, 115, 64, 85, 15]	[2, 114, 93, 51, 87, 82, 21, 89, 75]
138	[19, 121, 37, 75, 92, 109]	[42, 60, 66, 65, 101, 18, 41, 55, 77]
139	[54, 58, 30, 106, 112, 118]	[51, 92, 71, 89, 48, 77, 60, 50, 75]
140	[94, 60, 20, 110, 122, 24]	[2, 22, 74, 108, 85, 64, 25, 98, 2]
141	[21, 88, 26, 112, 82, 63]	[61, 86, 79, 120, 102, 99, 19, 8, 89]
142	[40, 35, 121, 95, 95, 118]	[20, 19, 31, 37, 79, 113, 22, 74, 64]
143	[80, 5, 1, 74, 85]	[92, 34, 51, 14, 36, 121, 20, 61]
144	[45, 96, 47, 85, 118, 95]	[9, 20, 10, 19, 119, 15, 102, 77, 23]
145	[11, 77, 100, 12, 119, 124]	[40, 66, 28, 76, 21, 66, 4, 21, 64]
146	[1, 87, 111, 116, 12, 93]	[74, 11, 13, 60, 88, 64, 52, 33, 113]
147	[69, 31, 8, 58, 84, 117]	[118, 57, 116, 59, 80, 56, 15, 31, 25]
148	[67, 100, 57, 44, 81, 124]	[94, 123, 29, 123, 39, 92, 53, 105, 101]
149	[37, 113, 6, 118, 28]	[31, 73, 124, 48, 94, 79, 63, 54, 102]
150	[59, 82, 11, 23, 21, 49]	[47, 121, 93, 26, 12, 41, 79, 87, 64]
151	[32, 60, 57, 49, 39, 122]	[71, 10, 90, 28, 122, 65, 77, 27, 124]
152	[93, 41, 16, 8, 11, 94]	[36, 123, 35, 37, 27, 91, 74, 18, 3]
153	[12, 47, 115, 31, 75, 103]	[18, 86, 113, 15, 7, 5, 44, 73, 88]
154	[93, 68, 122, 13, 30, 62]	[116, 86, 119, 41, 49, 58, 77, 75, 79]
155	[106, 88, 76, 40, 75, 118]	[59, 30, 39, 3, 92, 83, 49, 121, 121]
156	[1, 116, 107, 29, 45, 95]	[88, 68, 72, 99, 110, 75, 105, 62, 17]
157	[9, 14, 48, 41, 23, 46]	[33, 107, 23, 72, 10, 108, 40, 49, 67]
158	[91, 108, 66, 109, 74, 95]	[63, 25, 93, 19, 12, 84, 94, 3, 84]
159	[69, 82, 31, 60, 55, 93]	[17, 118, 45, 28, 20, 55, 54, 74, 70]
160	[6, 60, 49, 98, 40, 35]	[86, 108, 78, 22, 124, 86, 89, 46, 24]
161	[91, 38, 60, 72, 28, 24]	[63, 107, 78, 76, 33, 82, 81, 28, 111]
162	[115, 64, 5, 19, 100, 120]	[25, 71, 82, 34, 21, 76, 118, 110, 89]
163	[57, 100, 97, 17, 106, 31]	[43, 112, 97, 70, 122, 5, 95, 31, 70]
164	[59, 65, 100, 100, 24, 73]	[59, 3, 112, 51, 26, 50, 79, 99, 2]
165	[111, 29, 7, 41, 61, 100]	[100, 102, 7, 91, 23, 76, 50, 100, 89]
166	[121, 112, 76, 1, 60, 78]	[94, 14, 49, 56, 82, 12, 83, 69, 66]
167	[26, 2, 115, 64, 56, 64]	[68, 18, 64, 38, 97, 37, 42, 97, 44]
168	[73, 47, 86, 82, 102, 73]	[74, 112, 80, 32, 50, 8, 58, 5, 55]

(*Continued*)

Table A.3. (*Continued*)

i	Q_i	A_i
169	[43, 13, 32, 90, 103, 99]	[27, 34, 22, 108, 100, 113, 73, 79, 41]
170	[66, 38, 101, 103, 60, 51]	[37, 18, 25, 30, 59, 5, 89, 42, 96]
171	[77, 82, 60, 6, 33, 116]	[51, 77, 92, 110, 89, 54, 81, 78, 48]
172	[93, 96, 59, 1, 26, 97]	[56, 86, 13, 90, 12, 15, 47, 107, 5]
173	[22, 53, 24, 111, 55, 81]	[116, 2, 111, 82, 3, 63, 11, 85, 116]
174	[123, 70, 83, 118, 25, 88]	[58, 64, 111, 28, 96, 18, 65, 3, 9]
175	[3, 107, 54, 6, 93, 118]	[73, 58, 82, 85, 20, 5, 36, 39, 62]
176	[20, 28, 57, 92, 13, 5]	[64, 21, 124, 113, 52, 83, 50, 17, 12]
177	[27, 64, 45, 90, 106, 118]	[97, 7, 25, 116, 48, 123, 90, 83, 43]
178	[123, 27, 8, 68, 107, 54]	[117, 94, 7, 57, 37, 57, 77, 58, 19]
179	[120, 58, 1, 28, 69, 47]	[82, 40, 56, 81, 122, 55, 9, 56, 21]
180	[47, 39, 120, 23, 59, 49]	[110, 97, 109, 17, 108, 63, 106, 23, 89]
181	[50, 12, 73, 59, 68, 28]	[78, 104, 64, 120, 57, 42, 119, 117, 55]
182	[101, 18, 27, 65, 46, 30]	[76, 84, 76, 22, 20, 52, 25, 91, 17]
183	[28, 93, 63, 63, 30, 39]	[48, 78, 119, 49, 87, 48, 67, 64, 49]
184	[20, 108, 106, 67, 6, 110]	[109, 115, 19, 65, 69, 122, 32, 15, 2]
185	[11, 38, 34, 41, 9, 14]	[96, 8, 44, 51, 101, 36, 104, 97, 61]
186	[96, 83, 12, 114, 27, 65]	[113, 29, 17, 64, 19, 123, 102, 113, 85]
187	[102, 49, 62, 3, 46, 124]	[34, 117, 19, 69, 95, 62, 116, 76, 60]
188	[66, 14, 62, 46, 27, 74]	[71, 72, 45, 49, 113, 27, 4, 99, 34]
189	[3, 22, 87, 100, 117, 96]	[112, 60, 43, 15, 26, 104, 58, 56, 38]
190	[26, 107, 64, 116, 76, 104]	[35, 27, 71, 122, 85, 44, 88, 54, 75]
191	[70, 114, 44, 96, 109, 18]	[60, 35, 120, 107, 94, 50, 10, 3, 103]
192	[70, 106, 102, 13, 22, 87]	[95, 118, 101, 64, 59, 64, 69, 60, 51]
193	[72, 60, 1, 107, 14, 7]	[43, 31, 63, 42, 74, 62, 103, 63, 27]
194	[106, 35, 5, 119, 21, 96]	[90, 101, 109, 99, 8, 70, 119, 44, 34]
195	[69, 43, 36, 100, 81, 99]	[89, 69, 116, 124, 19, 87, 42, 65, 8]
196	[117, 94, 61, 1, 105, 90]	[63, 16, 76, 119, 75, 52, 7, 22, 104]
197	[28, 86, 25, 120, 62, 42]	[99, 2, 120, 43, 3, 39, 79, 15, 99]
198	[107, 117, 39, 39, 83, 56]	[8, 65, 97, 9, 17, 8, 12, 35, 9]
199	[26, 23, 21, 12, 100, 124]	[24, 98, 51, 10, 14, 74, 80, 52, 2]
200	[79, 55, 82, 32, 103, 77]	[94, 102, 30, 89, 47, 58, 45, 90, 37]
201	[48, 9, 38, 3, 6, 71]	[82, 95, 51, 14, 93, 38, 99, 68, 36]
202	[11, 77, 38, 6, 106, 113]	[110, 111, 5, 9, 122, 106, 4, 92, 82]
203	[94, 44, 75, 123, 106, 10]	[122, 108, 54, 35, 51, 70, 48, 122, 15]
204	[47, 50, 106, 10, 6, 83]	[68, 40, 68, 28, 26, 85, 109, 115, 54]
205	[7, 56, 72, 29, 61, 9]	[124, 90, 24, 54, 23, 39, 21, 29, 19]
206	[88, 75, 112, 61, 13, 107]	[65, 45, 35, 72, 64, 33, 97, 95, 62]
207	[120, 108, 101, 32, 37, 46]	[46, 48, 101, 115, 29, 68, 88, 46, 19]
208	[73, 121, 68, 1, 36, 65]	[118, 77, 9, 63, 43, 75, 44, 14, 11]
209	[105, 2, 98, 35, 63, 35]	[13, 50, 35, 55, 90, 59, 33, 90, 30]
210	[11, 55, 47, 49, 36, 89]	[59, 50, 109, 83, 61, 104, 19, 33, 94]
211	[112, 7, 16, 43, 48, 112]	[113, 121, 41, 80, 88, 102, 60, 104, 62]

Table A.3. (*Continued*)

i	Q_i	A_i
212	[34, 76, 80, 119, 49, 92]	[106, 82, 28, 23, 46, 122, 112, 66, 32]
213	[64, 46, 90, 54, 21, 84]	[34, 121, 90, 114, 74, 104, 93, 84, 114]
214	[61, 10, 46, 46, 25, 112]	[61, 3, 121, 89, 105, 88, 66, 92, 2]
215	[98, 35, 104, 51, 46, 72]	[109, 110, 43, 82, 27, 68, 96, 124, 19]
216	[8, 103, 55, 3, 100, 110]	[43, 93, 89, 77, 117, 55, 92, 13, 58]
217	[79, 69, 55, 100, 21, 122]	[124, 120, 104, 103, 74, 21, 4, 116, 43]
218	[118, 30, 67, 70, 21, 78]	[74, 23, 87, 57, 89, 114, 8, 74, 52]
219	[7, 88, 21, 78, 100, 44]	[13, 31, 13, 107, 105, 15, 24, 98, 87]
220	[101, 63, 111, 108, 37, 103]	[71, 119, 25, 87, 29, 56, 27, 108, 51]
221	[18, 67, 121, 37, 76, 22]	[10, 5, 57, 111, 35, 81, 90, 93, 38]
222	[66, 62, 43, 80, 49, 69]	[118, 48, 83, 19, 7, 60, 5, 119, 59]
223	[22, 95, 56, 56, 44, 63]	[102, 10, 90, 103, 54, 102, 75, 57, 103]
224	[105, 29, 27, 75, 46, 71]	[25, 91, 89, 78, 77, 113, 41, 85, 2]
225	[121, 101, 53, 34, 8, 121]	[122, 73, 32, 41, 18, 48, 36, 45, 38]
226	[82, 68, 41, 97, 9, 116]	[21, 43, 107, 29, 6, 74, 121, 11, 80]
227	[79, 62, 7, 9, 58, 19]	[61, 88, 24, 44, 37, 45, 51, 81, 118]
228	[35, 6, 119, 87, 27, 40]	[82, 73, 119, 123, 113, 45, 117, 40, 123]
229	[37, 78, 6, 6, 109, 121]	[37, 3, 73, 19, 20, 18, 11, 116, 2]
230	[91, 57, 45, 89, 6, 111]	[24, 124, 34, 43, 106, 13, 94, 71, 51]
231	[112, 73, 13, 1, 58, 10]	[96, 69, 103, 39, 34, 67, 30, 77, 79]
232	[20, 2, 91, 57, 39, 57]	[76, 88, 57, 62, 119, 61, 81, 119, 83]
233	[72, 23, 47, 80, 59, 6]	[6, 8, 47, 98, 108, 13, 18, 6, 51]
234	[21, 57, 104, 97, 27, 94]	[119, 47, 24, 92, 102, 114, 97, 30, 82]
235	[114, 21, 48, 76, 28, 17]	[93, 96, 47, 35, 61, 35, 14, 36, 89]
236	[111, 36, 1, 22, 77, 101]	[34, 84, 39, 33, 113, 38, 49, 39, 106]
237	[107, 16, 109, 72, 38, 33]	[92, 2, 72, 34, 3, 56, 66, 52, 92]
238	[14, 34, 58, 46, 42, 92]	[19, 14, 99, 71, 51, 17, 33, 10, 102]
239	[95, 118, 37, 1, 20, 119]	[39, 53, 68, 97, 67, 85, 101, 28, 45]
240	[3, 28, 17, 46, 95, 94]	[121, 36, 34, 52, 105, 45, 60, 63, 55]
241	[105, 22, 35, 99, 68, 45]	[57, 106, 110, 74, 15, 30, 18, 87, 67]
242	[114, 123, 30, 94, 24, 50]	[36, 57, 72, 22, 118, 88, 78, 3, 49]

References

[1] E. Artin, Quadratische Körper im Gebiete der höheren Kongruenzen I, II, *Math. Zeitschrift* **19** (1924) 153–206.

[2] M. L. Bauer, M. J. Jacobson, Jr., Y. Lee and R. Scheidler, Construction of quadratic function fields of high three-rank, *Math. Comp.* **77** (2008) 503–530.

[3] K. Belabas, A fast algorithm to compute cubic fields, *Math. Comp.* **66** (1997) 1213–1237.

[4] W. E. H. Berwick, On cubic fields with a given discriminant, *Proc. London Math. Soc.* **23**(2) (1925) 359–378.

[5] M. Bhargava, A. Shankar and J. Tsimerman, On the Davenport–Heilbronn theorem and second order terms, *Invent. Math.* **193** (2013) 439–499.

[6] H. Cohen, *Advanced Topics in Computational Number Theory*, Graduate Texts in Mathematics, Vol. 193 (Springer-Verlag, New York, 2000).

[7] H. Cohen, F. Diaz y Diaz and M. Olivier, On the density of discriminants of cyclic extensions of prime degree, *J. Reine Angew. Math.* **550** (2002) 169–209.

[8] H. Cohen and A. Morra, Counting cubic extensions with given quadratic resolvent, *J. Algebra* **325** (2011) 461–478.

[9] B. Datskovsky and D. Wright, Density of discriminants of cubic extensions, *J. Reine Angew. Math.* **386** (1988) 116–138.

[10] H. Davenport and H. Heilbronn, On the density of discriminants of cubic fields I, *Bull. London Math. Soc.* **1** (1969) 345–348.

[11] H. Davenport and H. Heilbronn, On the density of discriminants of cubic fields II, *Proc. Roy. Soc. London Ser. A* **322** (1971) 405–420.

[12] C. Fieker, I. Gaál and M. Pohst, On computing integral points of a Mordell curve over rational function fields in characteristic > 3, *J. Number Theory* **133** (2013) 738–750.

[13] E. Friedman and L. C. Washington, On the distribution of divisor class groups of curves over a finite field, in *Théorie des Nombres* (de Gruyter, Berlin, 1989), pp. 227–239.

[14] G. W.-W. Fung, Computational problems in complex cubic fields, Doctoral Dissertation, University of Manitoba (1990).

[15] J. F. Hammell, Index calculus in the infrastructure of real quadratic function fields, Master's Thesis, University of Calgary (2008).

[16] H. Hasse, Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage (German), *Math. Zeitschr.* **31** (1930) 565–582.

[17] M. J. Jacobson, Jr., R. Scheidler and A. Stein, Fast arithmetic on hyperelleptic curves via continued fraction expansions, in *Advances in Coding Theory and Cryptology*, Series on Coding Theory and Cryptology, Vol. 3 (World Scientific Publishing, Hackensack, New Jersey, 2007), pp. 201–244.

[18] E. Landquist, P. Rozenhart, R. Scheidler, J. Webster and Q. Wu, An explicit treatment of cubic function fields with applications, *Canad. J. Math.* **62**(4) (2010) 787–807.

[19] Y. Lee, The unit rank classification of a cubic function field by its discriminant, *Manuscr. Math.* **116** (2005) 173–181.

[20] Y. Lee, The Scholz theorem in function fields, *J. Number Theory* **122** (2007) 408–414.

[21] P. Llorente and E. Nart, Effective determination of the decomposition of the rational primes in a cubic field, *Proc. Amer. Math. Soc.* **87** (1983) 579–585.

[22] M. E. Pohst, On computing non-Galois cubic global function fields of prescribed discriminant in characteristic > 3, *Publ. Math. Debrecen* **79**(3–4) (2011) 611–621.

[23] J. Quer, Sobre el 3-rang dels cossos quadratics i la corba elliptica $y^2 = x^3 + M$ (Catalan) Doctoral dissertation, Bellaterra, Spain (1987).

[24] M. Rosen, The Hilbert class field in function fields, *Expo. Math.* **5** (1987) 365–378.

[25] M. Rosen, *Number Theory in Function Fields* (Springer, New York, 2002).

[26] P. Rozenhart, Fast tabulation of cubic function fields, Doctoral dissertation, University of Calgary, Canada (2009).

[27] P. Rozenhart, M. J. Jacobson, Jr. and R. Scheidler, Tabulation of cubic function fields via polynomial binary cubic forms, *Math. Comp.* **81** (2012) 2335–2359.

[28] P. Rozenhart, M. J. Jacobson, Jr. and R. Scheidler, Computing quadratic function fields wiith high 3-rank via cubic field tabulation, to appear in *Rocky Mountain J. Math.*

[29] P. Rozenhart and R. Scheidler, Tabulation of cubic function fields with imaginary and unusual Hessian, in *Proc. 8th Algorithmic Number Theory Symp. ANTS-VIII*, Lecturer Notes in Computer Science, Vol. 5011 (Springer, Berlin, 2008), pp. 357–370.

[30] F. K. Schmidt, Analytische Zahlentheorie in Körpern der Charakteristik p, *Math. Zeitschr.* **33** (1931) 1–32.

[31] A. Scholz, Über die Beziehung der Klassenzahlen quadratischer Körper zueinander, *J. Reine Angew. Math.* **166** (1932) 201–203.

[32] D. Shanks, The infrastructure of real quadratic fields and its application, in *Proc. 1972 Number Theory Conf.*, Boulder, Colorado (1972), pp. 217–224.

[33] D. Shanks, Recent applications of the infrastructure of real quadratic fields $\mathbb{Q}(\sqrt{N})$, *Notices Amer. Math. Soc.* **23** (1976) 59, Abstract 731-12-12.

[34] D. Shanks, Determining all cubic fields having a given fundamental discriminant, unpublished manuscript (1987).

[35] D. Shanks, Determining all cubic fields having a given fundamental discriminant, a talk presented at the AMS Summer Research Conference on Computational Number Theory, Brunswick, Maine (1988).

[36] D. Shanks, On Gauss and composition II, *NATO ASI Ser. C.* **265** (1989) 179–204.

[37] D. Shanks and P. Weinberger, A quadratic field of prime discriminant requiring three generators for its class group, and related theory, *Acta Arith.* **XXI** (1972) 71–87.

[38] V. Shoup, NTL: A library for doing number theory, Software (2001); `http://www.shoup.net/ntl`.

[39] A. Stein and E. Teske, The parallelized Pollard kangaroo method in real quadratic function fields, *Math. Comp.* **71** (2002) 793–814.

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

[41] H. Stichtenoth, *Algebraic Function Fields and Codes*, 2nd edn., Graduate Texts in Mathematics, Vol. 254 (Springer-Verlag, Berlin, 2009).

[42] A. V. Sutherland, Structure computation and discrete logarithms in finite abelian p-groups, *Math. Comp.* **80** (2011) 477–500.

[43] T. Taniguchi and F. Thorne, Secondary terms in counting functions for cubic fields, *Duke Math. J.* **162**(13) (2013) 2451–2508.

[44] F. Thorne, Four perspectives on secondary terms in the Davenport–Heilbronn theorems, *Integers* **12B** (2012/13), Paper No. A5, 23 pp.

[45] C. Weir, Constructing and tabulating dihedral function fields, doctoral dissertation, University of Calgary (2013).

[46] C. Weir, R. Scheidler and E. W. Howe, Constructing and tabulating dihedral function fields, in *Proc. 10th Algorithmic Number Theory Symp.* (*ANTS-X 2012*), The Open Book Series, Vol. 1 (Mathematical Science Publishers, Berkeley, California, 2013), pp. 557–585.