Computation of the Fundamental Units and the Regulator of a Cyclic Cubic Function Field

Y. Lee, R. Scheidler and C. Yarrish

CONTENTS

2000 AMS Subject Classification: Primary 11R58; Secondary 11R16, 11R27, 14H05, 11-04

Keywords: Purely cubic function field, reduced ideal, minimum, fundamental unit, regulator

This paper presents algorithms for computing the two fundamental units and the regulator of a cyclic cubic extension of a rational function field over a field of order $q \equiv 1 \pmod 3$. The procedure is based on a method originally due to Voronoi that was recently adapted to purely cubic function fields of unit rank one. Our numerical examples show that the two fundamental units tend to have large degree, and frequently, the extension has a very small ideal class number.

1. INTRODUCTION

A central problem in computational number theory is the question of finding the regulator or even a system of fundamental units of an algebraic number field. This is generally a difficult task, in part because the regulator is frequently exponential in the size of the field, resulting in up to doubly exponentially large fundamental units. Nevertheless, efforts to find regulators and fundamental units of certain types of number field extensions have been quite fruitful, particularly in the case of real quadratic number fields. Therefore, it seemed natural to explore the possibility of adapting some of these techniques to algebraic function fields of finite characteristic. This was achieved with considerable success in the case of real hyperelliptic function fields $K = \mathbb{F}_q(t)(\sqrt{D(t)})$ with $\deg(D(t))$ even [Stein and Williams 99] and, more recently, purely cubic function fields $K = \mathbb{F}_q(t)(\sqrt[3]{D(t)})$ with $q \equiv -1 \pmod 3$ and $\deg(D(t)) \equiv 0 \pmod 3$ [Scheidler and Stein 00]; both are unit rank 1 extensions.

Purely cubic function fields were classified in [Scheidler and Stein 00] and come in three flavors, to wit, unit rank 0, 1, or 2, depending on whether the place at infinity of $\mathbb{F}_q(t)$ splits one-, two-, or three-fold in K. This is in stark contrast to purely cubic number fields $\mathbb{Q}(\sqrt[3]{D})$ with $D \in \mathbb{Z}$, which are complex cubic fields and thus always have unit rank 1. Fast arithmetic in the Jacobian of a purely cubic function field extension of unit rank 0 was described in [Bauer 03]. As mentioned above, the case of unit rank 1 was dealt with in [Scheidler and Stein 00]. In this paper, we present a method for finding a pair of fundamental units and the regulator of a purely cubic function field $K = \mathbb{F}_q(t)(\sqrt[3]{D(t)})$ of unit rank 2 and characteristic at least 5. In this scenario, $\deg(D)$ is divisible by 3 and, more importantly, $q \equiv 1 \pmod 3$, so $\mathbb{F}_q$ (and hence K) contains a primitive cube root of unity. Kummer theory establishes that under these conditions, cyclic cubic fields are exactly those extensions that have a purely cubic representation, and we will see that such a representation is easily computable. Hence, our paper not only completely settles the question of fundamental unit computation in purely cubic function fields (except in characteristic 2 and 3), but the method given here will work in *all* cyclic cubic function fields with q odd and $q \equiv 1 \pmod 3$.

Purely cubic extensions of unit rank 0 share many properties with imaginary hyperelliptic function fields. Since they contain no nontrivial units, their regulator is equal to 1, the ideal class group is isomorphic to the Jacobian, and the class number is exponentially large. The numerical computations of [Scheidler and Stein 00] indicate that purely cubic function fields of unit rank 1 also behave very much like their quadratic counterparts, generally exhibiting very small ideal class numbers and exponentially large regulators and period lengths. There is no quadratic analog to the unit rank 2 case, and very little (if any) work has been done even in the setting of cubic number fields on the number of steps required to compute the regulator, and on the size of the fundamental units. Our examples in this paper show that the regulator of a purely cubic function field of unit rank 2 tends to be big, and the two fundamental units have very large coefficients (as expected), but in the interest of limiting the length of this paper, we decided to leave a more formal investigation of this subject for future research.

Berwick [Berwick 32] showed that any cyclic cubic number field contains a unit ϵ such that ϵ and its conjugate ϵ' form a pair of fundamental units. Here, ϵ is the unique minimal unit exceeding 1 whose conjugates have absolute value less than 1. There are, in fact, exactly six pairs of fundamental units of the form $\{\eta, \eta'\}$, given by $\eta \in \{\epsilon, \epsilon', \epsilon'', \epsilon^{-1}, \epsilon'^{-1}, \epsilon''^{-1}\}$ [Delone and Fadeev 64, pages 134f]. These results are easily extendable to cyclic cubic function fields. On first glance, it thus appears that one might only need to compute one fundamental unit, obtaining a second one "for free." Unfortunately, given a unit η that is known to be one of a pair of fundamental units, there appears to be no easy way to determine whether η and one of its conjugates generate the full unit group of the field, or just a subgroup of finite index.

The algorithms in [Scheidler and Stein 00] and in this paper both go back to the ideas of Voronoi [Voronoi 96]; see also [Delone and Fadeev 64, pages 246-273]. The first table of systematically machine-computed fundamental units in cubic number fields using Voronoi's algorithm was given in [Williams et al. 73]. To our knowledge, Mang [Mang 87] was the first to generate systems of fundamental units of purely cubic function fields of both unit rank 1 or 2. His technique, based on the Pohst-Zassenhaus method used for number fields [Pohst and Zassenhaus 97, Chapter 5], is entirely different from ours. By Mang's own admission, his procedure is slow and infeasible for even modest size fields. Our own ideas and terminology are primarily based on [Scheidler and Stein 00] and [Buchmann 85]; the latter source developed the theory for fundamental unit computation in number fields of unit rank 1 and 2.

2. CUBIC FUNCTION FIELDS

A general introduction to function fields can be found in [Stichtenoth 93]. Details of the purely cubic case are discussed in [Mang 87] and [Scheidler and Stein 00].

A *cubic function field* K is an extension of degree 3 of a field $k(t)$ of rational functions; here, $k = \mathbb{F}_q$ is a finite field of order q whose characteristic is not 3. The extension $K/k(t)$ is *purely cubic* if it is a radical extension, i.e., $K = k(t)(\rho)$ where $\rho^3 = D(t) \in k[t]$ is a cube-free polynomial with coefficients in k. Write $D = GH^2$ where $G, H \in k[t]$ are square-free and coprime. Then the curve $y^3 - D = 0$ defining $K/k(t)$ is singular if and only if H is nonconstant, in which case the singular points are exactly the points $(a, 0)$ where $H(a) = 0$. For our purposes, it suits us to work with such a (possibly singular) model.

If $K/k(t)$ is a normal (i.e., cyclic) cubic extension that contains the primitive cube roots of unity, then a purely cubic representation of K always exists and is, in fact, easy to find.

Lemma 2.1. *Let $K/k(t)$ be a cubic extension and $q \equiv 1 \pmod 3$. Then $K/k(t)$ is purely cubic if and only if $K/k(t)$ is cyclic.*

Proof: Since $q \equiv 1 \pmod 3$, k contains a primitive cube root of unity u. If $K = k(t)(\rho)$ with $\rho^3 \in k[t]$ cube-free, then the conjugates $u\rho$ and $u^2\rho$ of ρ both lie in K, so $K/k(t)$ is Galois with Galois group $\mathbb{Z}/3\mathbb{Z}$. Conversely, let α be any nonzero element in $K \setminus k(t)$ with minimal polynomial $f(y) = y^3 + Ay^2 + By + C$ $(A, B, C \in k(t))$. By replacing α by $\alpha - A/3$ if necessary, we may assume that $Tr(\alpha) = -A = 0$ where $Tr(\alpha) = \alpha + \alpha' + \alpha''$ is the trace of α and $\alpha', \alpha'' \in K$ denote the conjugates of α. If $\alpha' = u\alpha$, then $B = Tr(\alpha\alpha') = 0$, so $\alpha^3 = -C \in k(t)$. Suppose now that $\alpha' \neq u\alpha$ and consider the Lagrange resolvent $\beta = \alpha + u\alpha' + u^2\alpha'' \in K$ of α. It is easy to verify that $\beta = (1-u)(\alpha - u\alpha'')$, so $\beta \neq 0$. Furthermore, $Tr(\beta) = Tr(\beta\beta') = 0$, so $\beta^3 \in k(t)$. Hence, there always exists a nonzero element $\beta \in K$ with $\beta^3 \in k(t)$. Write $\beta^3 = G/H$ with $G, H \in k[t]$ nonzero and $\gcd(G, H) = 1$, and set $\rho = H\beta \in K$. Then $\rho^3 = GH^2 \in k[t]$ is cube-free and $K = k(t)(\rho)$. □

Henceforth, let $K = k(t)(\rho)$ be a purely cubic function field with $\rho^3 = D = GH^2$ as before. The *genus*[1] of K/k is $g = \deg(GH) - 2$ or $g = \deg(GH) - 1$, depending on whether or not the degree of D is divisible by 3. The *maximal order* or *ring of algebraic functions* in K is the integral closure $\mathcal{O} = \overline{k[t]}$ of $k[t]$ in K. The set $\mathcal{O}$ is a $k[t]$-module of rank 3 generated by 1, ρ and ω where $\omega = \rho^2/H$, so $\omega^3 = G^2H$. Its unit group $\mathcal{O}^*$ is a finitely generated Abelian group of rank r, the *unit rank* of K. The torsion part of $\mathcal{O}^*$ is the set k^* of nonzero constants, and a set of generators of the infinite part of $\mathcal{O}^*$ is a *system of fundamental units.*

The completion with respect to the infinite place of $k(t)$ (defined by the negative degree valuation) is the field $k\langle t^{-1}\rangle$ of Puiseux series in t^{-1} over k. For a nonzero element $\alpha = \sum_{i=-m}^{\infty} a_i t^{-i} \in k\langle t^{-1}\rangle$, $(m \in \mathbb{Z}, a_i \in k$ for $i \geq -m, a_{-m} \neq 0)$, we write $\operatorname{sgn}(\alpha) = a_{-m}$, $\deg(\alpha) = m$, $|\alpha| = q^m = q^{\deg(\alpha)}$, and $\lfloor \alpha \rfloor = \sum_{i=-m}^{0} a_i t^{-i}$ (with $\operatorname{sgn}(0) = 0$, $|0| = 0$, and $\lfloor 0 \rfloor = 0$). Then $\lfloor \alpha \rfloor \in k[t]$ and $|\alpha - \lfloor \alpha \rfloor| < 1$. As usual, α is said to be *monic* if $\operatorname{sgn}(\alpha) = 1$.

According to Theorem 2.1 of [Scheidler and Stein 00], the unit rank of a purely cubic function field can be 0, 1, or 2. The first scenario happens if and only if the degree of D is not divisible by 3 or the leading coefficient $\operatorname{sgn}(D)$ of D is not a cube in k. If $\deg(D) \equiv 0 \pmod 3$ and $\operatorname{sgn}(D) \in (k^*)^3$, then $r = 1$ if $q \equiv -1 \pmod 3$ and $r = 2$ if $q \equiv 1 \pmod 3$. In the case of nonzero unit rank, we can explicitly extract a cube root ρ of D which lies in $k\langle t^{-1}\rangle$; the other two cube roots of D are $u\rho$ and $u^2\rho$ where u is a fixed primitive cube root of unity. If $q \equiv 1 \pmod 3$, or equivalently, $u \in k$, then K is normal over $k(t)$, and all three cube roots lie in $k\langle t^{-1}\rangle$, giving rise to three distinct embeddings of K into $k\langle t^{-1}\rangle$. Here, the place at infinity of $k(t)$ splits completely. If on the other hand, $q \equiv -1 \pmod 3$, then there is a unique such embedding, the infinite place of $k(t)$ splits only two-fold, and $K/k(t)$ is not a normal extension.

We now limit our discussion to cyclic cubic fields of unit rank 2 in purely cubic representation. Let σ be a generator of the Galois group of $K/k(t)$ so that $\sigma(\rho) = u\rho$ and $\sigma^2(\rho) = u^2\rho$. Write $\alpha = \alpha^{(0)}$, $\sigma(\alpha) = \alpha^{(1)} = \alpha'$ and $\sigma^2(\alpha) = \alpha^{(2)} = \alpha''$ for any $\alpha \in K$, and let $N(\alpha) = \alpha\alpha'\alpha'' \in k(t)$ denote the norm of α. Let ∞ be one of the three places at infinity in K and $|\cdot|_\infty$ its associated (multiplicative) valuation. Then $|\alpha'|_\infty = |\alpha|_{\infty''}$ and $|\alpha''|_\infty = |\alpha|_{\infty'}$ for all $\alpha \in K$. We number the valuations $|\cdot|_0$, $|\cdot|_1$, $|\cdot|_2$ so that $|\alpha|_\infty = |\alpha|_0$, $|\alpha'|_0 = |\alpha|_1$ and $|\alpha''|_0 = |\alpha|_2$, so $|\alpha^{(i)}|_0 = |\alpha^{(0)}|_i$ for $i \in \{0, 1, 2\}$. Then $|\alpha|_i$ is called the *i-value* of α. We note that $|\rho|_0 = |\rho|_1 = |\rho|_2 = |D|^{1/3}$, so henceforth, we omit the subscript and simply write $|\rho|$ and $|\omega|$.

Let $\{\epsilon_1, \epsilon_2\}$ be a system of fundamental units in K. The *regulator* of K is the absolute value of the determinant of any 2×2 submatrix of the 2×3 matrix

$$\begin{pmatrix} \deg(\epsilon_1) & \deg(\epsilon_1') & \deg(\epsilon_1'') \\ \deg(\epsilon_2) & \deg(\epsilon_2') & \deg(\epsilon_2'') \end{pmatrix};$$

it is independent of the choice of the submatrix and the system of fundamental units.

3. MINIMA, NEIGHBORS, AND i-CHAINS

A *fractional ideal* of $\mathcal{O}$ is a set of the form $\mathfrak{f} = d^{-1}\mathfrak{a}$ where $d \in k[t]$ is a nonzero polynomial and $\mathfrak{a}$ is an ideal (in the ordinary sense) of $\mathcal{O}$. The unique monic polynomial $d(\mathfrak{f})$ of minimal degree such that $d(\mathfrak{f})\mathfrak{f} \subseteq \mathcal{O}$ is the *denominator* of $\mathfrak{f}$. For $\alpha \in K$, $(\alpha) = \{\alpha\theta \mid \theta \in \mathcal{O}\}$ denotes the *principal fractional ideal generated by* α. Every nonzero fractional ideal $\mathfrak{f}$ in $\mathcal{O}$ is a $k[t]$-module of rank 3; if $\{\lambda, \mu, \nu\}$ is a $k[t]$-basis of $\mathfrak{f}$ where $\lambda = (l_0 + l_1\rho + l_2\omega)/d$, $\mu = (m_0 + m_1\rho + m_2\omega)/d$, $\nu = (n_0 + n_1\rho + n_2\omega)/d$ with $d = d(\mathfrak{f})$ and $l_0, l_1, l_2, m_0, m_1, m_2, n_0, n_1, n_2, d \in k[t]$ coprime, then the *norm* and the *discriminant* of $\mathfrak{f}$, respectively, are the two rational functions

$$N(\mathfrak{f}) = \frac{1}{d^3} \det \begin{pmatrix} l_0 & l_1 & l_2 \\ m_0 & m_1 & m_2 \\ n_0 & n_1 & n_2 \end{pmatrix} \quad \text{and}$$

$$\Delta(\mathfrak{f}) = \det \begin{pmatrix} \lambda & \lambda' & \lambda'' \\ \mu & \mu' & \mu'' \\ \nu & \nu' & \nu'' \end{pmatrix}^2$$

which are unique up to nonzero constant factors in K and independent of the choice of basis of $\mathfrak{f}$. The maximal

[1] The genus is an invariant of K/k; it is independent of the transcendental element t and hence, the representation of K/k.

order $\mathcal{O} = [1, \rho, \omega]$ has norm 1 and discriminant $\Delta = \Delta(\mathcal{O}) = -27G^2H^2$. Norm and discriminant of an ideal $\mathfrak{f}$ are related through the identity $\Delta(\mathfrak{f}) = aN(\mathfrak{f})^2\Delta$ for suitable $a \in k^*$. We note that since for all nonzero $\alpha \in \mathfrak{f}$, $(d)\mathfrak{f}$ divides $(d\alpha)$ (as integral ideals), we have $|N(\mathfrak{f})| \leq |N(\alpha)|$.

In our context, fractional ideals are always assumed to contain 1; in particular, they are nonzero, and 1 can always be chosen as a basis element. For a fractional ideal $\mathfrak{f}$ and $\theta \in \mathfrak{f}$, we define the set

$$\mathcal{N}_{\mathfrak{f}}(\theta) = \{\alpha \in \mathfrak{f} \mid |\alpha|_i \leq |\theta|_i \text{ for } i = 0, 1, 2\}.$$

θ is a *minimum* in $\mathfrak{f}$ if $\mathcal{N}_{\mathfrak{f}}(\theta) = k\theta$, i.e., $\mathcal{N}_{\mathfrak{f}}(\theta)$ consists only of constant multiples of θ. The ideal $\mathfrak{f}$ is *reduced* if 1 is a minimum in $\mathfrak{f}$. We briefly summarize some properties of minima and reduced ideals.

Lemma 3.1. *Let $\mathfrak{f}$ be a fractional ideal of $\mathcal{O}$ and $\theta \in \mathfrak{f}$.*

1. *θ is a minimum in $\mathfrak{f}$ if and only if the fractional ideal $(\theta^{-1})\mathfrak{f}$ is reduced.*
2. *If θ is a minimum in $\mathfrak{f}$ and ϵ a unit in $\mathcal{O}$, then $\epsilon\theta$ is a minimum in $\mathfrak{f}$. So the unit group $\mathcal{O}^*$ acts on the set of minima of any fractional ideal by multiplication.*
3. *If $\mathfrak{f}$ is reduced, then $|N(\mathfrak{f})| > |\Delta|^{-1/2}$ and $|d(\mathfrak{f})| < |\Delta|^{1/2}$.*

Proof: Part 1 is easy to see, and the proof of Part 2 is completely analogous to that of Proposition 4.2 of [Scheidler and Stein 00]. Part 3 follows from Theorem 4.5 and Corollary 4.6 of [Scheidler and Stein 00]; the proofs given in that source are independent of the unit rank of K. □

As usual, we call two elements in $\mathcal{O}$ *associate* if they differ by a factor in $\mathcal{O}^*$, and *nonassociate* otherwise.

Lemma 3.2.

1. *$\mathcal{O}$ is reduced.*
2. *Every unit in $\mathcal{O}$ is a minimum in $\mathcal{O}$.*
3. *If θ is a minimum in $\mathcal{O}$, then $|N(\theta)| < |\Delta|^{1/2}$.*
4. *The action of the unit group on the set of minima in $\mathcal{O}$ decomposes this set into a finite number of orbits. So the number of nonassociate minima in $\mathcal{O}$ is finite.*

Proof: Properties 1 and 2 are easy to establish; see also Theorem 4.1 and Corollary 4.3 of [Scheidler and Stein 00]. To see Part 3, we observe that by Part 1 of Lemma 3.1, the principal fractional ideal (θ^{-1}) is reduced and hence, has norm exceeding $|\Delta|^{-1/2}$ in absolute value by Part 3 of that lemma. It follows that the norm of a minimum in $\mathcal{O}$ can only take on finitely many values, and for each such value, the number of nonassociate minima with this norm is also finite. This proves Part 4. □

Fix an index $i \in \{0, 1, 2\}$ and let $\alpha, \beta \in K^*$ be distinct elements. Write $\alpha \leq_i \beta$ if the triple $(|\alpha|_i, |\alpha|_{i+1}, |\alpha|_{i+2})$ appears before the triple $(|\beta|_i, |\beta|_{i+1}, |\beta|_{i+2})$ with respect to lexicographical order, where we allow the possibility that the two triples are equal. Here, the indices $i+1$ and $i+2$ are taken modulo 3 to lie between 0 and 2 inclusive; this convention for the indices will be used throughout the paper. The following statement is obvious.

Remark 3.3. The set of monic minima in any fractional ideal $\mathfrak{f}$ is totally ordered under the ordering $\leq_i$; in particular, by antisymmetry, if α, β are minima in $\mathfrak{f}$ with $\alpha \leq_i \beta \leq_i \alpha$, then α and β differ by a nonzero constant factor.

For $i \in \{0, 1, 2\}$, $\mathfrak{f}$ a fractional ideal of $\mathcal{O}$, and $\theta \in \mathfrak{f}$, we let

$$\mathcal{H}_{\mathfrak{f},i}(\theta) = \{\alpha \in \mathfrak{f} \mid |\alpha|_i > |\theta|_i, |\alpha|_j \leq |\theta|_j$$
$$\text{for all } j \neq i, |\alpha|_j < |\theta|_j \text{ for at least one } j \neq i\}.$$

Theorem 3.4. *Let $i \in \{0, 1, 2\}$, $\mathfrak{f}$ a reduced fractional ideal, and θ a minimum in $\mathfrak{f}$. Then there exists an element $\phi \in \mathcal{H}_{\mathfrak{f},i}(\theta)$ such that $\phi \leq_i \alpha$ for all $\alpha \in \mathcal{H}_{\mathfrak{f},i}(\theta)$. The element ϕ is unique up to nonzero constant factors and is also a minimum in $\mathfrak{f}$.*

Proof: For brevity, set $\mathcal{H} = \mathcal{H}_{\mathfrak{f},i}(\theta)$. Let $\epsilon \in \mathcal{O}^*$ with $|\epsilon|_i > 1$, so $|\epsilon'\epsilon''|_i < 1$. Without loss of generality, assume that $|\epsilon|_j \leq 1$ for $j \neq i$ (one of $\epsilon, (\epsilon')^{-1}, (\epsilon'')^{-1}$ satisfies these inequalities). Then $|\epsilon|_j < 1$ for at least one $j \neq i$. It follows that $\epsilon\theta \in \mathcal{H}$, so $\mathcal{H}$ is nonempty.

To define ϕ, we repeatedly use the Well-Ordering Principle as follows. Since $|\alpha|_i > |\theta|_i$ for all $\alpha \in \mathcal{H}$, there exists an element in $\mathcal{H}$ of minimal i-value q^m, say. Now for all $\alpha \in \mathcal{H}$ with $|\alpha|_i = q^m$, we have $|\alpha'\alpha''|_i = |N(\alpha)||\alpha|_i^{-1} \geq |N(\mathfrak{f})|q^{-m}$, so there exists $\beta \in \mathcal{H}$ with $|\beta|_i = q^m$ and $|\beta'\beta''|_i$ is minimal, say equal to q^n. Finally, if $\gamma \in \mathcal{H}$ with $|\gamma|_i = q^m$ and $|\gamma'\gamma''|_i = q^n$, then $|\gamma|_{i+1} = q^n|\gamma|_{i+2}^{-1} \geq q^n|\theta|_{i+2}^{-1}$, so there exists $\phi \in \mathcal{H}$ with $|\phi|_i = q^m$, $|\phi'\phi''|_i = q^n$, and $|\phi|_{i+1}$ minimal. Now for all $\alpha \in \mathcal{H}$, $|\phi|_i \leq |\alpha|_i$, $|\phi|_{i+1} \leq |\alpha|_{i+1}$, and if equality holds in both these relations, then the property $|\phi'\phi''|_i \le |\alpha'\alpha''|_i$ yields $|\phi|_{i+2} \le |\alpha|_{i+2}$. So $\phi \le_i \alpha$.

To see that ϕ is a minimum in $\mathfrak{f}$, let $\alpha \in \mathcal{N}_{\mathfrak{f}}(\phi)$. Then

$$|\alpha|_i \le |\phi|_i, \quad |\alpha|_j \le |\phi|_j, \quad |\alpha|_h \le |\phi|_h,$$
$$|\theta|_i < |\phi|_i, \quad |\theta|_j \ge |\phi|_j, \quad |\theta|_h > |\phi|_h,$$

where $j, h \in \{1,2,3\} \setminus \{i\}$ are suitably labelled.

If $|\alpha|_i \le |\theta|_i$, then from the above inequalities $|\alpha|_j \le |\theta|_j$ and $|\alpha|_h < |\theta|_h$, so $\alpha \in \mathcal{N}_{\mathfrak{f}}(\theta) = k\theta$, in which case $|\alpha|_h < |\theta|_h$ implies $\alpha = 0 \in k\phi$. So suppose that $|\alpha|_i > |\theta|_i$. Then $\alpha \in \mathcal{H}$, so $\phi \le_i \alpha$ and hence, $|\alpha|_m = |\phi|_m$ for $m = 0,1,2$. Set $\beta = \alpha - \operatorname{sgn}(\alpha)\operatorname{sgn}(\phi)^{-1}\phi$, then $\beta \in \mathfrak{f}$ and $|\beta|_i < |\phi|_i$. Therefore, $\phi \not\le_i \beta$, and hence, $\beta \notin \mathcal{H}$. Since $|\beta|_j \le |\phi|_j \le |\theta|_j$ and $|\beta|_h \le |\phi|_h < |\theta|_h$, we must have $|\beta|_i \not> |\theta|_i$. But then $\beta \in \mathcal{N}_{\mathfrak{f}}(\theta) = k\theta$. Since $|\beta|_h < |\theta|_h$, we must have $\beta = 0$ as before. Hence, α and ϕ differ by a constant factor.

Finally, ϕ is unique up to nonzero constant factors by Remark 3.3. □

An element in $\mathcal{H}_{\mathfrak{f},i}(\theta)$ that is minimal with respect to $\le_i$ is an *i-neighbor* of θ in $\mathfrak{f}$. We henceforth ignore constant factors, speaking of "the" i-neighbor of θ in $\mathfrak{f}$ which we denote by $\varphi_{\mathfrak{f},i}(\theta)$. Hence, it needs to be understood that equalities such as those in Lemma 3.5 and in Theorem 4.2 only hold up to nonzero constant factors.

Lemma 3.5. *Let $i \in \{0,1,2\}$, $\mathfrak{f}$ a reduced fractional ideal, and θ a minimum in $\mathfrak{f}$.*

1. *$\theta\, \varphi_{(\theta^{-1})\mathfrak{f},i}(1) = \varphi_{\mathfrak{f},i}(\theta)$.*
2. *$\epsilon\, \varphi_{\mathfrak{f},i}(\theta) = \varphi_{\mathfrak{f},i}(\epsilon\theta)$ for every $\epsilon \in \mathcal{O}^*$.*

Proof: For brevity, set $\phi = \varphi_{\mathfrak{f},i}(\theta)$.

1. By Part 1 of Lemma 3.1, $(\theta^{-1})\mathfrak{f}$ is reduced, so $\phi_1 = \varphi_{(\theta^{-1})\mathfrak{f},i}(1)$ exists. We first observe that $\phi_1 \in \mathcal{H}_{(\theta^{-1})\mathfrak{f},i}(1)$, so $\theta\phi_1 \in \mathcal{H}_{\mathfrak{f},i}(\theta)$ and hence, $\phi \le_i \theta\phi_1$. Conversely, $\phi \in \mathcal{H}_{\mathfrak{f},i}(\theta)$ implies $\theta^{-1}\phi \in \mathcal{H}_{(\theta^{-1})\mathfrak{f},i}(1)$, so $\phi_1 \le_i \theta^{-1}\phi$ and hence, $\theta\phi_1 \le_i \phi$. Since ϕ_1 is a minimum in $(\theta^{-1})\mathfrak{f}$, $\theta\phi_1$ is a minimum in $\mathfrak{f}$, so the claim now follows from Remark 3.3.

2. Clearly, $\epsilon\phi \in \mathfrak{f}$ and $\epsilon\phi \in \mathcal{H}_{\mathfrak{f},i}(\epsilon\theta)$. Set $\phi_2 = \varphi_{\mathfrak{f},i}(\epsilon\theta)$, then $\phi_2 \le_i \epsilon\phi$. On the other hand, $\epsilon^{-1}\phi_2 \in \mathcal{H}_{\mathfrak{f},i}(\theta)$, so $\phi \le_i \epsilon^{-1}\phi_2$. Since $\epsilon\phi$ is a minimum in $\mathfrak{f}$ by Part 2 of Lemma 3.1, Remark 3.3 again yields the desired result. □

Let $i \in \{0,1,2\}$ and θ a minimum in $\mathcal{O}$. Define $\theta_0 = \theta$ and $\theta_n = \varphi_{\mathcal{O},i}(\theta_{n-1})$ for $n \in \mathbb{N}_0 (= \mathbb{N} \cup \{0\})$. We call the sequence $(\theta_n)_{n\in\mathbb{N}_0}$ the *i-chain* of θ.

Theorem 3.6. *Let $i \in \{0,1,2\}$, θ a minimum in $\mathcal{O}$, and $(\theta_n)_{n\in\mathbb{N}_0}$ the i-chain of θ. For $n \in \mathbb{N}_0$, set $\mathfrak{f}_n = (\theta_n^{-1})$*

1. *The sequence $(\mathfrak{f}_n)_{n\in\mathbb{N}_0}$ is periodic, i.e., there exist minimal integers $p \ge 0$ and $l \ge 1$ such that $\mathfrak{f}_{ml+p+n} = \mathfrak{f}_{p+n}$ for all $m \in \mathbb{N}_0$ and $n \in \{0,1,\ldots,l-1\}$.*
2. *There exists a unit $\epsilon \in \mathcal{O}^*$ such that $\theta_{ml+p+n} = \epsilon^m\theta_{p+n}$ for all $m \in \mathbb{N}_0$ and $n \in \{0,1,\ldots,l-1\}$.*
3. *$\theta_{n+1} = \alpha_n\theta_n$ with $\alpha_n = \varphi_{\mathfrak{f}_n,i}(1)$ for all $n \in \mathbb{N}_0$.*

Proof: The sequence $(\mathfrak{f}_n)_{n\in\mathbb{N}_0}$ is periodic by Part 4 of Lemma 3.2 and the i-chain of θ is of the form described in the second part of the theorem by Part 2 of Lemma 3.5. The ideal $\mathfrak{f}_n$ is reduced by Part 1 of Lemma 3.1, and the recursion for the chain follows from Part 1 of Lemma 3.5. □

The portions $(\theta_n)_{0\le n<p}$ and $(\theta_n)_{p\le n<p+l}$ are the *preperiod* and the *(primitive) period*, respectively, of the i-chain of θ. Here, p is the *preperiod length*, l the *period length*, and $\epsilon = \theta_{l+p}\theta_p^{-1}$ the *primitive unit* of the chain. For $j \in \{0,1,2\} \setminus \{i\}$, the i-chain of θ is *degenerated in j-direction* if $|\epsilon|_j = 1$, or equivalently, if $|\alpha_n|_j = 1$, i.e. $|\theta_{n+1}|_j = |\theta_n|_j$, for all $n \in \mathbb{N}$. It is easy to see that any chain can be degenerated in at most one direction.

Our algorithm for computing a pair of fundamental units of K is based on the following theorem. For the corresponding result in number fields and its proof, see Theorems 2.1 and 2.2 in [Buchmann 85, Part II]; the proofs of that source essentially carry over literally to the function field scenario.

Theorem 3.7. *Let $\{i,j,k\} = \{0,1,2\}$, θ a minimum in $\mathcal{O}$, $(\theta_n)_{n\in\mathbb{N}_0}$ the i-chain of θ, and $(\phi_n)_{n\in\mathbb{N}_0}$ the j-chain of θ. Suppose the i-chain of θ is not degenerated in k-direction.*

1. *There exists an element in the j-chain of θ which is different from θ and is nontrivially associate to an element in the primitive period of the i-chain of θ.*
2. *Let $m, n \in \mathbb{N}$ be minimal so that θ_n and ϕ_m are nontrivially associate. Let ϵ_1 be the primitive unit of the i-chain of θ and $\epsilon_2 = \phi_m\theta_n^{-1}$. Then $\{\epsilon_1, \epsilon_2\}$ is a pair of fundamental units of K.*

Thus, in order to find a pair of fundamental units, we need a procedure for generating i-chains, which in turn requires a method for computing the i-neighbor of 1 in any given reduced fractional ideal by Part 3 of Theorem 3.6. In Section 4, we explain how to accomplish this.

4. REDUCED BASES

Much of the ideas and terminology in this section are similar to Section 7 of [Scheidler and Stein 00]. Henceforth, we exclude the characteristic 2 case; that is, we require k to be a finite field of characteristic at least 5. For $\alpha = a + b\rho + c\omega \in K$ with $a, b, c \in k(t)$, we let

$$\begin{aligned} \xi_\alpha &= b\rho + c\omega &&= \frac{1}{3}(2\alpha - \alpha' - \alpha''),\\ \eta_\alpha &= b\rho - c\omega &&= \frac{1}{2u+1}(\alpha' - \alpha''),\\ \zeta_\alpha &= 2a - b\rho - c\omega &&= \alpha' + \alpha'' \;=\; 2\alpha - 3\xi_\alpha, \end{aligned} \tag{4–1}$$

where as before, $u \in k$ is a primitive cube root of unity, and ρ, ω are defined as in Section 2.. The following lemma will be useful later on:

Lemma 4.1. *Let $i \in \{0,1,2\}$ and let $\beta = a + b\rho + c\omega \in K$ ($a, b, c \in k(t)$) with $|\beta|_i > 1$, $|\beta|_{i+1} = 1$, and $|\zeta_\beta|_i < 1$. Set $\alpha = \beta - \operatorname{sgn}(\beta^{(i+1)})$. Then $|\alpha|_i = |\beta|_i > 1$, $|\alpha|_{i+1} < 1$, and $|\alpha|_{i+2} = 1$.*

Proof: Since $|\beta|_i > 1$, $|\alpha|_i = |\beta|_i$. Since $|\beta^{(i+1)}|_0 = |\beta|_{i+1} = 1 > |\zeta_\beta|_i = |\beta^{(i+1)} + \beta^{(i+2)}|_0$, we have $|\beta^{(i+1)}|_0 = |\beta^{(i+2)}|_0 = 1$ and $\operatorname{sgn}(\beta^{(i+1)}) = -\operatorname{sgn}(\beta^{(i+2)})$; also $\operatorname{sgn}(\beta^{(j)}) = \lfloor \beta^{(j)} \rfloor$ for $j \in \{i+1, i+2\}$. It follows that $|\alpha|_{i+1} = |\alpha^{(i+1)}|_0 = |\beta^{(i+1)} - \lfloor \beta^{(i+1)} \rfloor|_0 < 1$ and $|\alpha|_{i+2} = |\beta^{(i+2)} + \lfloor \beta^{(i+2)} \rfloor|_0 = |\beta|_{i+2} = 1$. □

Fix $i \in \{0,1,2\}$. We call a $k[t]$-basis $\{1, \mu, \nu\}$ of any fractional ideal $\mathfrak{f}$ *i-reduced* if

$$|\xi_\mu|_i > |\xi_\nu|_i, \quad |\eta_\mu|_i < 1 \le |\eta_\nu|_i, \quad |\zeta_\mu|_i < 1,\ |\zeta_\nu|_i < 1. \tag{4–2}$$

We note that $|\eta_\nu|_i \ge 1 > |\zeta_\nu|_i$ implies $|\eta_\nu|_i = |\nu|_{i+1} = |\nu|_{i+2} \ge 1$. Also, $|\eta_\mu|_i, |\zeta_\mu|_i < 1$ yield $|\mu|_{i+1}, |\mu|_{i+2} < 1$, so if $\mathfrak{f}$ is reduced, then we must have $|\mu|_i > 1$ and hence, $|\mu|_i = |\xi_\mu|_i$ and $\mu \in \mathcal{H}_{\mathfrak{f},i}(1)$. Reduced bases provide a means for finding neighbors of 1:

Theorem 4.2. *Let $i \in \{0,1,2\}$ and let $\{1, \mu, \nu\}$ be an i-reduced basis of a reduced fractional ideal $\mathfrak{f}$.*
If $|\nu|_{i+1} = 1$, then $\varphi_{\mathfrak{f},i}(1) = \nu - \operatorname{sgn}(\nu^{(i+1)})$.
If $|\nu|_{i+1} > 1$, then $\varphi_{\mathfrak{f},i}(1) = \mu$.

Proof: For brevity, set $\phi = \varphi_{\mathfrak{f},i}(1)$ and $\alpha = \nu - \operatorname{sgn}(\nu^{(i+1)})$. Label the valuations so that $|\phi|_i > 1$, $|\phi|_j \le 1$, $|\phi|_h < 1$. By (4–1), $|\eta_\phi|_i \le 1$, $|\zeta_\phi|_i \le 1$, and $|\xi_\phi|_i = |\phi|_i$. Write $\phi = l + m\mu + n\nu$ with $l, m, n \in k[t]$.

Case 1. $|\nu|_{i+1} = 1$. Then $|\nu|_{i+2} = |\eta_\nu|_i = 1$. Since $\mathfrak{f}$ is reduced, we must have $|\nu|_i > 1$; hence, by (4–1), $|\nu|_i = |\xi_\nu|_i$.

We prove $|m| < |n|$. To this end, suppose $|m| \ge |n|$. If $m = 0$, then $\phi = l$, so $|\phi|_h < 1$ implies $\phi = l = 0$, a contradiction. So $m \ne 0$, in which case by (4–2), $|m\xi_\mu|_i > |n\xi_\nu|_i$. Also by Lemma 4.1, $\alpha \in \mathcal{H}_{\mathfrak{f},i}(1)$, so $\phi \le_i \alpha$. In particular, $|\phi|_i \le |\alpha|_i = |\nu|_i$. It follows that

$$\begin{aligned} |\nu|_i = |\alpha|_i \ge |\phi|_i = |\xi_\phi|_i &= |m\xi_\mu + n\xi_\nu|_i \\ &= |m\xi_\mu|_i \ge |\xi_\mu|_i > |\xi_\nu|_i = |\nu|_i, \end{aligned}$$

again a contradiction. So we must have $|m| < |n|$.

Now (4–2) implies $|m\eta_\mu|_i < |n\eta_\nu|_i = |n|$, so $1 \ge |\eta_\phi|_i = |m\eta_\mu + n\eta_\nu|_i = |n|$. Thus, $n \in k^*$ and $m = 0$; without loss of generality, $n = 1$. Then $\phi = l + \nu = \tilde{l} + \alpha$ with $\tilde{l} = l + \operatorname{sgn}(\nu^{(i+1)}) \in k$. Therefore, $|\phi|_i = |\alpha|_i$, and since $\phi \le_i \alpha$, we must have $|\phi|_{i+1} \le |\alpha|_{i+1} < 1$ by Lemma 4.1. It follows that $|\tilde{l}| = |\phi - \alpha|_{i+1} < 1$, so $\tilde{l} = 0$ and $\phi = \alpha$.

Case 2. $|\nu|_{i+1} > 1$. Then $|\eta_\nu|_i > 1$. In this scenario, we prove $|m| > |n|$. This is clear if $n = 0$, as $|m| \le |n|$ would imply $m = n = 0$ and $|l| = |\phi|_h < 1$, so $\phi = l = 0$ which is impossible. If $n \ne 0$, then the inequalities $|n\eta_\nu|_i > 1$ and $1 \ge |\eta_\phi|_i = |m\eta_\mu + n\eta_\nu|_i$ imply $|m\eta_\mu|_i = |n\eta_\nu|_i$, in which case by (4–2), $|m| > |m\eta_\mu|_i = |n\eta_\nu|_i > |n|$. Hence, $|m| > |n|$ and by (4–2), $|m\xi_\mu|_i > |n\xi_\nu|_i$. Now $\mu \in \mathcal{H}_{\mathfrak{f},i}(1)$, so $\phi \le_i \mu$ and hence $|\phi|_i \le |\mu|_i$. It follows that

$$|\phi|_i = |\xi_\phi|_i = |m\xi_\mu + n\xi_\nu|_i = |m\xi_\mu|_i \ge |\xi_\mu|_i = |\mu|_i \ge |\phi|_i,$$

so $|m| = 1$, i.e., $m \in k^*$, and $n = 0$. Again, normalize so $m = 1$ and $\phi = l + \mu$. Finally, $|l| = |\phi - \mu|_h < 1$, so $l = 0$ and $\phi = \mu$. □

Corollary 4.3. *Let $i \in \{0,1,2\}$ and θ be a minimum in $\mathcal{O}$. Then the i-chain $(\theta_n)_{n \in \mathbb{N}_0}$ of θ is not degenerated in $(i+1)$-direction.*

Proof: Let $n \in \mathbb{N}_0$ and let $\{1, \mu_n, \nu_n\}$ be an i-reduced basis of $\mathfrak{f}_n = (\theta_n^{-1})$. By Theorem 4.2, Lemma 4.1, and the remark following (4–2), we have $|\varphi_{\mathfrak{f}_n,i}(1)|_{i+1} < 1$. The corollary now immediately follows from Part 3 of Theorem 3.6. □

We can now show that reduced bases are essentially unique:

Theorem 4.4. *Two fractional ideals are equal if and only if they have the same i-reduced bases (up to constant factors) for some $i \in \{0,1,2\}$. More exactly, let $i \in \{0,1,2\}$ and for $j = 1,2$, let $\{1,\mu_j,\nu_j\}$ be an i-reduced basis of a fractional ideal $\mathfrak{f}_j$. Then $\mathfrak{f}_1 = \mathfrak{f}_2$ if and only if there exist $v, w \in k^*$ such that $\mu_2 = v\mu_1$ and $\nu_2 = w\nu_1$.*

Proof: The "if" part is obvious, so assume that $\mathfrak{f}_1 = \mathfrak{f}_2$. Then by Theorem 3.4,

$$\operatorname{sgn}(\varphi_{\mathfrak{f}_1,i}(1))^{-1}\varphi_{\mathfrak{f}_1,i}(1) = \operatorname{sgn}(\varphi_{\mathfrak{f}_2,i}(1))^{-1}\varphi_{\mathfrak{f}_2,i}(1);$$

denote this quantity by ϕ and note that ϕ is monic. Without loss of generality, assume that μ_j, ν_j are also monic for $j = 1,2$. Now there exists a unimodular 3×3 matrix with entries in $k[t]$ that transforms the basis $\{1,\mu_1,\nu_1\}$ into the basis $\{1,\mu_2,\nu_2\}$.

Case 1. $|\nu_1|_{i+1} = 1$. Then by Theorem 4.2, $\phi = \nu_1 - \operatorname{sgn}(\nu_1^{(i+1)})$, so by Lemma 4.1, $|\phi|_{i+2} = 1$. Since $|\mu_2|_{i+2} < 1$, we cannot have $\phi = \mu_2$, so we must have $\phi = \nu_2 - \operatorname{sgn}(\nu_2^{(i+1)})$. Hence, $\nu_1 = \nu_2 + s$ with $s = \operatorname{sgn}(\nu_2^{(i+1)}) - \operatorname{sgn}(\nu_1^{(i+1)}) \in k$. Then $|s| = |\zeta_s|_i = |\zeta_{\nu_1} - \zeta_{\nu_2}|_i < 1$ by (4–2), so $s = 0$ and $\nu_1 = \nu_2$.

Now there exist $l, m, n \in k[t]$ with $\mu_2 = l + m\mu_1 + n\nu_1$, and since the basis transformation matrix is unimodular, we must have $m \in k^*$. Since by (4–2), $1 > |\eta_{\mu_2} - m\eta_{\mu_1}|_i = |n\eta_{\nu_1}|_i = |n|$, we have $n = 0$. Similarly, $1 > |\zeta_{\mu_2} - m\zeta_{\mu_1}|_i = |l|$ implies $l = 0$, so $m = 1$ and $\mu_1 = \mu_2$.

Case 2. $|\nu_1|_{i+1} > 1$. Then by Theorem 4.2, $\phi = \mu_1$. Since $|\mu_1|_{i+2} < 1$, ϕ cannot equal $\nu_2 - \operatorname{sgn}(\nu_2^{(i+1)})$, so $\phi = \mu_2$, giving $\mu_1 = \mu_2$. As before, $\nu_2 = l + m\mu_1 + n\nu_1$ for some $l, m \in k[t]$ and $n \in k^*$. Then $|m\xi_{\mu_1}|_i = |\xi_{\nu_2} - n\xi_{\nu_1}|_i < |\xi_{\mu_1}|_i$, so $m = 0$. Finally, $|l| = |\zeta_{\nu_2} - n\zeta_{\nu_1}|_i < 1$, so $l = 0$, $n = 1$, and $\nu_1 = \nu_2$. □

If $i \in \{0,1,2\}$ and $\{1,\mu,\nu\}$ is a basis of some fractional ideal $\mathfrak{f}$, then an easy computation shows that there exists $a \in k^*$ such that

$$\det\begin{pmatrix} \xi_\mu & \eta_\mu \\ \xi_\nu & \eta_\nu \end{pmatrix}^2 = (\xi_\mu\eta_\nu - \xi_\nu\eta_\mu)^2 = a\Delta(\mathfrak{f}). \qquad (4\text{–}3)$$

If the basis is i-reduced, then (4–3) implies $|\mu|_i|\nu|_j = |\Delta(\mathfrak{f})|^{1/2}$ for $j \in \{0,1,2\} \setminus \{i\}$. Using (4–2), (4–3), and Part 3 of Lemma 3.1, one can now prove analogously to Proposition 5.1 of [Scheidler 00] that reduced bases are small; more exactly:

Proposition 4.5. *Let $i \in \{0,1,2\}$ and let $\{1,\mu,\nu\}$ be an i-reduced basis of a reduced fractional ideal $\mathfrak{f}$ where $\mu = (m_0 + m_1\rho + m_2\omega)/d$, $\nu = (n_0 + n_1\rho + n_2\omega)/d$ with $m_0, m_1, m_2, n_0, n_1, n_2, d \in k[t]$ and $\gcd(m_0, m_1, m_2, n_0, n_1, n_2, d) = 1$. Then*

1. *$\lfloor m_0/d \rfloor = \lfloor m_1\rho/d \rfloor = \lfloor m_2\omega/d \rfloor = \lfloor \mu \rfloor/3$.*
2. *$|\nu|_i < |\mu|_i \le |\Delta(\mathfrak{f})|^{1/2}$, so $|m_0| = |m_1\rho| = |m_2\omega| \le |\Delta|^{1/2}$ and $|n_0|, |n_1\rho|, |n_2\omega| < |\Delta|^{1/2}$.*

Part 3 of Theorem 3.6, as well as Theorem 4.2, show how to generate i-chains ($i \in \{0,1,2\}$). Suppose we have an i-reduced basis $\{1,\mu_n,\nu_n\}$ ($n \in \mathbb{N}_0$) of the reduced fractional ideal $\mathfrak{f}_n = (\theta_n^{-1})$ where θ_n is the n-th element of the i-chain of $\theta_0 \in \mathcal{O}$. Since $\theta_{n+1} = \varphi_{\mathfrak{f}_n,i}(1)\theta_n$, we have $\mathfrak{f}_{n+1} = (\varphi_{\mathfrak{f}_n,i}(1)^{-1})\mathfrak{f}_n$. If $|\nu_n|_{i+1} = 1$, then by Theorem 4.2, $\varphi_{\mathfrak{f}_n,i}(1) = \alpha_n$ with $\alpha_n = \nu_n - \operatorname{sgn}(\nu_n^{(i+1)})$. Since $\mathfrak{f}_n = [1,\mu_n,\alpha_n]$, we have $\mathfrak{f}_{n+1} = (\alpha_n^{-1})\mathfrak{f}_n = [1,\alpha_n^{-1},\mu_n\alpha_n^{-1}]$. If $|\nu_n|_{i+1} > 1$, then again by Theorem 4.2, $\mathfrak{f}_{n+1} = (\mu_n^{-1})\mathfrak{f}_n = [1,\mu_n^{-1},\nu_n\mu_n^{-1}]$. Either of these basis representations of $\mathfrak{f}_{n+1}$ is usually nonreduced, so we now compute a reduced basis $\{1,\mu_{n+1},\nu_{n+1}\}$ of $\mathfrak{f}_{n+1}$ (using Algorithm 4.6 below). At the very beginning of our computation, we start out with $\mathfrak{f}_0 = \mathcal{O} = [1,\rho,\omega]$ and apply the algorithm to find our first reduced basis $\{1,\mu_0,\nu_0\}$ of $\mathcal{O}$.

The following algorithm produces an i-reduced basis of a reduced fractional ideal $\mathfrak{f}$, provided $\mathfrak{f}$ is given in terms of a basis $\{1,\tilde{\mu},\tilde{\nu}\}$ where

$$\begin{aligned} \{\tilde{\mu},\tilde{\nu}\} &= \{\rho,\omega\} \text{ or} \\ \{\tilde{\mu},\tilde{\nu}\} &= \{\alpha^{-1},\mu\alpha^{-1}\} \text{ with } \alpha = \nu - \operatorname{sgn}(\nu^{(i+1)}) \text{ or} \\ \{\tilde{\mu},\tilde{\nu}\} &= \{\mu^{-1},\nu\mu^{-1}\} \end{aligned} \qquad (4\text{–}4)$$

and $\mathfrak{g} = (\varphi_{\mathfrak{f},i}(1))\mathfrak{f} = [1,\mu,\nu]$ is a reduced fractional ideal. Here, the first case corresponds to $\mathfrak{f} = \mathcal{O}$ and the second and third cases to the situations where $|\tilde{\nu}|_{i+1} = 1$, $\mathfrak{f} = (\alpha^{-1})\mathfrak{g}$, and $|\tilde{\nu}|_{i+1} > 1$, $\mathfrak{f} = (\mu^{-1})\mathfrak{g}$, respectively. The method is an adaptation and slight simplification of Algorithm 7.1 in [Scheidler and Stein 00].

Algorithm 4.6. (Reduction Algorithm.)

Input: $(i,\tilde{\mu},\tilde{\nu})$ where $i \in \{0,1,2\}$ and $\tilde{\mu},\tilde{\nu}$ are given by (4–4).

Output: (μ,ν) where $\{1,\mu,\nu\}$ is an i-reduced basis of $\mathfrak{f} = [1,\tilde{\mu},\tilde{\nu}]$.

Algorithm:

1. Set $\mu = \tilde{\mu}$, $\nu = \tilde{\nu}$.
2. If $|\xi_\mu|_i < |\xi_\nu|_i$ or if $|\xi_\mu|_i = |\xi_\nu|_i$ and $|\eta_\mu|_i < |\eta_\nu|_i$, replace $\begin{pmatrix} \mu \\ \nu \end{pmatrix}$ by $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} \mu \\ \nu \end{pmatrix}$.

```
3. If $|\eta_\mu|_i \geq |\eta_\nu|_i$ then
    3.1. While $|\xi_\nu\eta_\nu|_i > |\Delta(\mathfrak{f})|^{1/2}$, replace $\begin{pmatrix} \mu \\ \nu \end{pmatrix}$ by
         $\begin{pmatrix} 0 & 1 \\ -1 & \lfloor \xi_{\mu^{(i)}}/\xi_{\nu^{(i)}} \rfloor \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}$.
    3.2. Replace $\begin{pmatrix} \mu \\ \nu \end{pmatrix}$ by
         $\begin{pmatrix} 0 & 1 \\ -1 & \lfloor \xi_{\mu^{(i)}}/\xi_{\nu^{(i)}} \rfloor \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}$.
    3.3. If $|\eta_\mu|_i = |\eta_\nu|_i$, replace $\begin{pmatrix} \mu \\ \nu \end{pmatrix}$ by
         $\begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}$
         where $a = \operatorname{sgn}(\eta_{\mu^{(i)}})\operatorname{sgn}(\eta^{-1}_{\nu^{(i)}})$.
4. While $|\eta_\mu|_i \geq 1$, replace $\begin{pmatrix} \mu \\ \nu \end{pmatrix}$ by
   $\begin{pmatrix} \lfloor \eta_{\nu^{(i)}}/\eta_{\mu^{(i)}} \rfloor & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}$.
5. Replace $\mu$ by $\mu - \lfloor \zeta_{\mu^{(i)}} \rfloor/2$ and $\nu$ by $\nu - \lfloor \zeta_{\nu^{(i)}} \rfloor/2$.
6. Return $(\mu, \nu)$.
```

Before we prove the correctness of Algorithm 4.6, we require an auxiliary lemma.

Lemma 4.7. *Let $i \in \{0, 1, 2\}$ and $\mathfrak{f} = [1, \tilde{\mu}, \tilde{\nu}]$ where $\tilde{\mu}$ and $\tilde{\nu}$ satisfy (4–4). Then* $\min\{|\xi_{\tilde{\mu}}|_i, |\xi_{\tilde{\nu}}|_i\} < |\Delta(\mathfrak{f})|^{1/2}$.

Proof: Clear for $\{\tilde{\mu}, \tilde{\nu}\} = \{\rho, \omega\}$. Suppose that $\mathfrak{g} = (\varphi_{\mathfrak{f},i}(1)\mathfrak{f} = [1, \mu, \nu]$ is a reduced ideal and assume first that $|\nu|_{i+1} = 1$. Then $\mathfrak{g} = (\alpha)\mathfrak{f}$ with $\alpha = \nu - \operatorname{sgn}(\nu^{(i+1)})$, and without loss of generality, $\tilde{\mu} = \alpha^{-1}$, $\tilde{\nu} = \mu\alpha^{-1}$. By Lemma 4.1 and Proposition 4.5, $1 < |\alpha|_i = |\nu|_i < |\Delta(\mathfrak{g})|^{1/2} = |N(\alpha)||\Delta(\mathfrak{f})|^{1/2}$, $|\alpha|_{i+1} < 1$, $|\alpha|_{i+2} = 1$, so

$$|\xi_{\tilde{\mu}}|_i = \left|\frac{2}{\alpha} - \frac{1}{\alpha'} - \frac{1}{\alpha''}\right|_i = \frac{1}{|\alpha'|_i} = \frac{|\alpha|_i}{|N(\alpha)|} < |\Delta(\mathfrak{f})|^{1/2}.$$

Now assume that $|\nu|_{i+1} > 1$, so $\mathfrak{g} = (\mu)\mathfrak{f}$, and without loss of generality, $\tilde{\mu} = \mu^{-1}$, $\tilde{\nu} = \nu\mu^{-1}$. Then by (4–2) and Proposition 4.5, $1 < |\mu|_i \leq |\Delta(\mathfrak{g})|^{1/2} = |N(\mu)||\Delta(\mathfrak{f})|^{1/2}$ and $|\mu|_{i+1}, |\mu|_{i+2} < 1$, so

$$|\xi_{\tilde{\mu}}|_i = \left|\frac{2}{\mu} - \frac{1}{\mu'} - \frac{1}{\mu''}\right|_i \leq \max\left\{\frac{1}{|\mu'|_i}, \frac{1}{|\mu''|_i}\right\}$$
$$= \frac{|\mu|_i \max\{|\mu'|_i, |\mu''|_i\}}{|N(\mu)|} < \frac{|\mu|_i}{|N(\mu)|} \leq |\Delta(\mathfrak{f})|^{1/2}.$$

□

Proposition 4.8. *Algorithm 4.6 terminates and produces a reduced basis.*

Proof: We first note that for any $\alpha \in K$, $|\xi_\alpha|_i = |\xi_\alpha^{(i)}|_0 = |\xi_{\alpha^{(i)}}|_0$; similarly for η_α and ζ_α.

Upon entering Step 3, we have $|\xi_\mu|_i \geq |\xi_\nu|_i$ and $|\eta_\mu|_i \geq |\eta_\nu|_i$. Now by (4–3), $|\xi_\nu\eta_\nu|_i > |\Delta(\mathfrak{f})|^{1/2}$ if and only if $|\xi_\mu/\xi_\nu - \eta_\mu/\eta_\nu|_i < 1$ or equivalently, $\lfloor \xi_{\mu^{(i)}}/\xi_{\nu^{(i)}} \rfloor = \lfloor \eta_{\mu^{(i)}}/\eta_{\nu^{(i)}} \rfloor$. If μ, ν are the inputs to Step 3.1 and $\alpha = \nu, \beta = -\mu + \lfloor \xi_{\mu^{(i)}}/\xi_{\nu^{(i)}} \rfloor \nu$, then

$$|\xi_\beta|_i = \left|-\xi_\mu + \left\lfloor \frac{\xi_{\mu^{(i)}}}{\xi_{\nu^{(i)}}} \right\rfloor \xi_\nu\right|_i = \left|-\xi_{\mu^{(i)}} + \left\lfloor \frac{\xi_{\mu^{(i)}}}{\xi_{\nu^{(i)}}} \right\rfloor \xi_{\nu^{(i)}}\right|_0$$
$$< |\xi_{\nu^{(i)}}|_0 = |\xi_\nu|_i = |\xi_\alpha|_i;$$

similarly, $|\eta_\beta|_i < |\eta_\alpha|_i$. So both $|\xi_\nu|_i$ and $|\eta_\nu|_i$ decrease in each iteration of the loop in Step 3.1. Hence, this loop terminates and leaves the inequalities $|\xi_\mu|_i \geq |\xi_\nu|_i$ and $|\eta_\mu|_i \geq |\eta_\nu|_i$ intact (both inequalities are strict if the loop is executed at least once) .

Now Step 3.2 decreases $|\xi_\nu|_i$ further, thereby achieving $|\xi_\mu|_i > |\xi_\nu|_i$. If α and β are as before, then

$$|\eta_\beta|_i =$$
$$\left|\left(-\eta_{\mu^{(i)}} + \left\lfloor \frac{\eta_{\mu^{(i)}}}{\eta_{\nu^{(i)}}} \right\rfloor \eta_{\nu^{(i)}}\right) + \left(\left\lfloor \frac{\xi_{\mu^{(i)}}}{\xi_{\nu^{(i)}}} \right\rfloor - \left\lfloor \frac{\eta_{\mu^{(i)}}}{\eta_{\nu^{(i)}}} \right\rfloor\right) \eta_{\nu^{(i)}}\right|_0$$
$$\geq |\eta_\nu|_i = |\eta_\alpha|_i$$

because $|\lfloor \xi_{\mu^{(i)}}/\xi_{\nu^{(i)}} \rfloor - \lfloor \eta_{\mu^{(i)}}/\eta_{\nu^{(i)}} \rfloor|_i \geq 1$ and the expression inside the first pair of parentheses has i-value less than $|\eta_\nu|_i$. We note that in Step 3.3, $a = \lfloor \eta_{\mu^{(i)}}/\eta_{\nu^{(i)}} \rfloor$, so if we set $\alpha = \mu - a\nu$ and $\beta = \nu$, then as before, $|\eta_\alpha|_i < |\eta_\beta|_i$, and since $|\xi_\mu|_i > |\xi_\nu|_i$, we have $|\xi_\alpha|_i = |\xi_\mu|_i > |\xi_\beta|_i$. It follows that upon entering Step 4, we have

$$|\xi_\mu|_i > |\xi_\nu|_i, \quad |\eta_\mu|_i < |\eta_\nu|_i. \tag{4–5}$$

Using (4–3), we infer that after Step 3.2, $|\eta_\beta|_i = |\Delta(\mathfrak{f})|^{1/2}|\xi_\nu|_i^{-1}$, and Step 3.3 does not change η_β. We recall that throughout Step 3, $|\xi_\nu|_i$ decreases, and since Step 2 ensures that $|\xi_\nu|_i < |\Delta(\mathfrak{f})|^{1/2}$ by Lemma 4.7, we have $|\eta_\nu|_i > 1$ upon entering Step 4. Using analogous reasoning as above, it is easily proved that throughout Step 4, $|\xi_\mu|_i$ increases, $|\eta_\mu|_i$ decreases, and inequalities (4–5) are maintained, with $|\eta_\mu|_i < 1 \leq |\eta_\nu|_i$ at the end of Step 4.

Finally, if $\alpha = \mu - \lfloor \zeta_{\mu^{(i)}} \rfloor/2$, then since $\zeta_{\lfloor \zeta_{\mu^{(i)}} \rfloor} = 2\lfloor \zeta_{\mu^{(i)}} \rfloor$, we have $\zeta_\alpha = \zeta_\mu - \lfloor \zeta_{\mu^{(i)}} \rfloor$ and $|\zeta_\alpha|_i = |\zeta_{\mu^{(i)}} - \lfloor \zeta_{\mu^{(i)}} \rfloor|_0 < 1$; similarly for $\zeta_{\nu^{(i)}}$. Hence, after Step 5, the output basis $\{1, \mu, \nu\}$ is reduced. □

5. FUNDAMENTAL UNIT COMPUTATION

As mentioned before, Theorem 3.7 provides the basis for finding a pair of fundamental units $\{\epsilon_1, \epsilon_2\}$ of K. According to this theorem, we obtain the first such unit $\epsilon_1 = \theta_{p+l}\theta_p^{-1}$ by computing the preperiod and primitive period $\mathcal{C} = (\theta_0, \theta_1, \dots, \theta_p, \dots, \theta_{p+l-1})$ of the 0-chain of $\theta_0 = 1$; here, p is the preperiod length and l the period length of the chain. Theorem 4.4 provides a simple method for establishing whether or not two elements in $\mathcal{C}$ are associate; we simply need to compare the 0-reduced bases $\{1, \mu_n, \nu_n\}$ of the reduced principal fractional ideals (θ_n^{-1}) with $\theta_n \in \mathcal{C}$. For this purpose, we maintain a list $\mathcal{I}$ consisting of these reduced bases, normalized so that their first nonzero coefficients and denominators are monic. Once ϵ_1 is found, we remove the preperiod $(\theta_n)_{0 \le n < p}$ of the 0-chain from $\mathcal{C}$ and the first p reduced basis element pairs from $\mathcal{I}$, but we preserve the primitive period $(\theta_n)_{p \le n < p+l}$ as well as the reduced basis element pairs $(\mu_n, \nu_n)_{p \le n < p+l}$.

By Corollary 4.3, the 0-chain of 1 is not degenerated in 1-direction. To find the second fundamental unit ϵ_2, we generate elements $\phi_0 = \theta_p, \phi_1, \phi_2, \dots$ of the 2-chain of θ_p one by one, until an entry is found that differs from one of $\{\theta_p, \theta_{p+1}, \dots, \theta_{p+l-1}\}$ by a unit factor ϵ_2. Then ϵ_2 is the desired second fundamental unit. To check whether an element ϕ_j is associate to any of the θ_i $(p \le i < p + l)$, we compute a 0-reduced basis of the ideal $\mathfrak{g}_j = (\phi_j^{-1})$ (in addition to the 2-reduced basis $\{\sigma_j, \tau_j\}$ computed to generate the 2-chain), again normalized as above, and compare it to all the 0-reduced bases in the list $\mathcal{I}$. Alternatively, one could check whether for any $i \in \{p, p+1, \dots, p+l-1\}$, ϕ_j divides θ_i in $\mathcal{O}$ and vice versa; this is the case if and only if the norms $N(\phi_j)$ and $N(\theta_i)$ differ by a constant factor and $N(\phi_j)$ divides a, b, c where $\phi_j'\phi_j''\theta_i = a + b\rho + c\omega$. However, our numerical experiments revealed that this test is significantly slower than simply computing and comparing 0-reduced bases.

Algorithm 5.1. (First Fundamental Unit Computation.)

Input: q, G, H.

Output: $(\epsilon_1, \mathcal{C}, \mathcal{I}, p, l)$ where

- ϵ_1 is the first of a pair of fundamental units of K;
- $\mathcal{C}$ is the primitive period of the 0-chain of 1;
- $\mathcal{I}$ contains the 0-reduced bases of the reduced fractional ideals generated by the inverses of the elements in $\mathcal{C}$;
- p is the preperiod length of $\mathcal{C}$;
- l is the period length of $\mathcal{C}$.

Algorithm:

```
1. Set $\mathcal{C} = \mathcal{I} = \emptyset$ and $\theta = 1$.
2. Call Algorithm 4.6 on input $(0, \rho, \omega)$ to compute $(\mu, \nu)$ where $\{1, \mu, \nu\}$ is a 0-reduced basis of $\mathcal{O}$ (normalize so that the denominator is 1 and the first nonzero coefficients of $\mu$ and $\nu$ are monic).
3. Repeat
   3.1. Append $\theta$ to $\mathcal{C}$ and $(\mu, \nu)$ to $\mathcal{I}$;
   3.2. If $|\nu|_1 = 1$, then set N = TRUE and $\alpha = \nu - \mathrm{sgn}(\nu')$, else set N = FALSE;
   3.3. If $(N)$, then replace $\theta$ by $\theta\alpha$, else replace $\theta$ by $\theta\mu$;
   3.4. If $(N)$, then replace $\{\mu, \nu\}$ by $\{\alpha^{-1}, \mu\alpha^{-1}\}$, else replace $\{\mu, \nu\}$ by $\{\mu^{-1}, \nu\mu^{-1}\}$;
   3.5. Call Algorithm 4.6 to replace $(\mu, \nu)$ by the elements $(\mu, \nu)$ of a 0-reduced basis $\{1, \mu, \nu\}$ of the reduced principal fractional ideal $(\theta^{-1})$ (normalize so that the denominator and the first nonzero coefficients of $\mu$ and $\nu$ are monic);
   until $(\mu, \nu) \in \mathcal{I}$.
4. Set $p$ to be one less than the first position in which $(\mu, \nu)$ appeared in $\mathcal{I}$.
5. Remove the first $p$ elements from $\mathcal{C}$ (so now $\mathcal{C} = (\theta_p, \theta_{p+1}, \dots, \theta_{p+l-1})$).
6. Remove the first $p$ basis pairs from $\mathcal{I}$ (so now $\mathcal{I} = ((\mu_p, \nu_p), (\mu_{p+1}, \nu_{p+1}), \dots, (\mu_{p+l-1}, \nu_{p+l-1})))$.
7. Set $\epsilon_1 = \theta\theta_p^{-1}$ and $l = \#C$.
8. Return $(\epsilon_1, \mathcal{C}, \mathcal{I}, p, l)$.
```

Algorithm 5.2. (Second Fundamental Unit Computation.)

Input: q, G, H, and the lists $\mathcal{C}, \mathcal{I}$ generated in Algorithm 5.1.

Output: (ϵ_2, m) where

- ϵ_2 is the second of a pair of fundamental units of K;
- m is the number of elements computed in the 2-chain of the first element of $\mathcal{C}$ to obtain ϵ_2.

Algorithm:

```
1. Set $\phi$ to be the first element in $\mathcal{C}$, $(\sigma, \tau)$ the first pair in $\mathcal{I}$, and $m = 0$.
2. Repeat
   2.1. Call Algorithm 4.6 to replace $(\sigma, \tau)$ by the elements $(\sigma, \tau)$ of a 2-reduced basis $\{1, \sigma, \tau\}$ of the reduced principal fractional ideal $(\phi^{-1})$;
```

```
    2.2. If $|\tau|_0 = 1$, then set T = TRUE and $\beta = \tau - \mathrm{sgn}(\tau)$, else set T = FALSE;
    2.3. If $(T)$, then replace $\phi$ by $\phi\beta$, else replace $\phi$ by $\phi\sigma$;
    2.4. If $(T)$, then replace $\{\sigma, \tau\}$ by $\{\beta^{-1}, \sigma\beta^{-1}\}$, else replace $\{\sigma, \tau\}$ by $\{\sigma^{-1}, \tau\sigma^{-1}\}$;
    2.5. Call Algorithm 4.6 on input $(0, \sigma, \tau)$ to compute $(\mu, \nu)$ where $\{1, \mu, \nu\}$ is a 0-reduced basis of the reduced principal fractional ideal $(\phi^{-1})$ (normalize so that the denominator and the first nonzero coefficients of $\mu$ and $\nu$ are monic);
    2.6. Increase $m$ by 1;
    until $(\mu, \nu) \in \mathcal{I}$;
3. Set $j$ to be the position in which $(\mu, \nu)$ appeared in $\mathcal{I}$.
4. Set $\epsilon_2 = \phi\theta^{-1}$ where $\theta$ is the $j$-th element in $\mathcal{C}$.
5. Return $(\epsilon_2, m)$.
```

6. REGULATOR COMPUTATION

From the Hasse-Weil Theorem (see Theorem V.1.15, page 166, and Theorem V.2.1, page 169, of [Stichtenoth 93]), we know that

$$(\sqrt{q} - 1)^{2g} \leq hR \leq (\sqrt{q} + 1)^{2g}, \tag{6–1}$$

where as before, $g = \deg(GH) - 2$ is the genus of K, h is the ideal class number of $K/k(t)$, R is the regulator of $K/k(t)$, and the product hR is the order of the Jacobian of K. If h is small, then R is therefore of magnitude $q^{\deg(GH)-2}$, and our numerical examples (see Section 7) reveal that R can, in fact, come close to the upper bound in (6–1). Since the size of the field K is given by the degrees of G and H as well as the number of bits in q, the regulator can be exponentially large in the size of the field, and the fundamental units doubly exponential. In order to compute regulators of even moderately sized fields, it is thus necessary to avoid computing fundamental units explicitly. To find R, we therefore only generate the list $\mathcal{I}$ of 0-reduced bases, but not the list $\mathcal{C}$ of minima. We also store the degrees of the 0-neighbors of 1 and the degrees of their conjugates in an array $\mathcal{N}$. Once two identical pairs of basis elements (μ_p, ν_p) and (μ_{p+l}, ν_{p+l}) in $\mathcal{I}$ are encountered, we compute

$$\deg(\epsilon_1) = \sum_{n=p}^{p+l-1} \deg(\varphi_{\mathfrak{f}_n,0}(1)),$$

$$\deg(\epsilon_1') = \sum_{n=p}^{p+l-1} \deg(\varphi_{\mathfrak{f}_n,0}(1)').$$

Similarly, we have

$$\begin{aligned}
\deg(\epsilon_2) &= \sum_{n=0}^{m-1} \deg(\varphi_{\mathfrak{g}_n,2}(1)) - \sum_{n=p}^{p+j-1} \deg(\varphi_{\mathfrak{f}_n,0}(1)), \\
\deg(\epsilon_2') &= \sum_{n=0}^{m-1} \deg(\varphi_{\mathfrak{g}_n,2}(1)') - \sum_{n=p}^{p+j-1} \deg(\varphi_{\mathfrak{f}_n,0}(1)'),
\end{aligned}$$

where j, m are as in Algorithm 5.2. The algorithm for computing the regulator R of K is given below. Here, $e_{11} = \deg(\epsilon_1)$, $e_{12} = \deg(\epsilon_1')$, $e_{21} = \deg(\epsilon_2)$, $e_{22} = \deg(\epsilon_2')$, and $R = |e_{11}e_{22} - e_{12}e_{21}|$.

Algorithm 6.1. (Regulator Computation.)

```
Input: $q, G, H$.
Output: $(R, p, l, m)$ where
  • $R$ is the regulator of $K$;
  • $p$ and $l$ are as in Algorithm 5.1;
  • $m$ is as in Algorithm 5.2.
Algorithm:
1. Set $\mu = \rho$, $\nu = \omega$, $\mathcal{I} = \mathcal{N} = \emptyset$.
2. Call Algorithm 4.6 on input $(0, \rho, \omega)$ to compute $\{\mu, \nu\}$ where $\{1, \mu, \nu\}$ is a 0-reduced basis of $\mathcal{O}$ (normalize so that the denominator is 1 and the first nonzero coefficients of $\mu$ and $\nu$ are monic).
3. Repeat
    3.1. Append $(\mu, \nu)$ to $\mathcal{I}$;
    3.2. If $|\nu|_1 = 1$, then set N = TRUE and $\alpha = \nu - \mathrm{sgn}(\nu')$, else set N = FALSE;
    3.3. If $(N)$, then append $(\deg(\alpha), \deg(\alpha'))$ to $\mathcal{N}$, else append $(\deg(\mu), \deg(\mu'))$ to $\mathcal{N}$;
    3.4. If $(N)$, then replace $\{\mu, \nu\}$ by $\{\alpha^{-1}, \mu\alpha^{-1}\}$, else replace $\{\mu, \nu\}$ by $\{\mu^{-1}, \nu\mu^{-1}\}$;
    3.5. Call Algorithm 4.6 to replace $(\mu, \nu)$ by the elements $(\mu, \nu)$ of a 0-reduced basis $\{1, \mu, \nu\}$ of the ideal $[1, \mu, \nu]$ (normalize so that the denominator and the first nonzero coefficients of $\mu$ and $\nu$ are monic);
    until $(\mu, \nu) \in \mathcal{I}$.
4. Set $p$ to be one less than the first position in which $(\mu, \nu)$ appeared in $\mathcal{I}$.
5. Remove the first $p$ pairs from $\mathcal{I}$ and from $\mathcal{N}$.
```

```
6. Set $l = \#\mathcal{I}$.
7. Set $e_{11} = e_{12} = 0$.
8. For $n = p$ to $p + l - 1$ do
    8.1. Add the first element of the $n$-th pair of $\mathcal{N}$ to $e_{11}$;
    8.2. Add the second element of the $n$-th pair of $\mathcal{N}$ to $e_{12}$;
   end for.
9. Set $m = 0$, $e_{21} = e_{22} = 0$, $\sigma = \mu_p$, $\tau = \nu_p$.
10. Repeat
    10.1. Call Algorithm 4.6 to replace $(\sigma, \tau)$ by the elements $(\sigma, \tau)$ of a 2-reduced basis $\{1, \sigma, \tau\}$ of the ideal $[1, \sigma, \tau]$;
    10.2. If $|\tau|_0 = 1$, then set T = TRUE and $\beta = \tau - \mathrm{sgn}(\tau)$, else set T = FALSE;
    10.3. If $(T)$, then add $\deg(\beta)$ to $e_{21}$ and $\deg(\beta')$ to $e_{22}$, else add $\deg(\sigma)$ to $e_{21}$ and $\deg(\sigma')$ to $e_{22}$;
    10.4. If $(T)$, then replace $\{\sigma, \tau\}$ by $\{\beta^{-1}, \sigma\beta^{-1}\}$, else replace $\{\sigma, \tau\}$ by $\{\sigma^{-1}, \tau\sigma^{-1}\}$;
    10.5. Call Algorithm 4.6 on input $(0, \sigma, \tau)$ to compute $(\mu, \nu)$ where $\{1, \mu, \nu\}$ is a 0-reduced basis of the reduced principal fractional ideal $[1, \sigma, \tau]$ (normalize so that the denominator and the first nonzero coefficients of $\mu$ and $\nu$ are monic);
    10.6. Increase $m$ by 1;
   until $(\mu, \nu) \in \mathcal{I}$.
11. Set $j$ to be one less than the position in which $(\mu, \nu)$ appeared in $\mathcal{I}$.
12. For $n = p$ to $p + j - 1$ do
    12.1. Subtract the first element of the $n$-th pair of $\mathcal{N}$ from $e_{21}$;
    12.2. Subtract the second element of the $n$-th pair of $\mathcal{N}$ from $e_{22}$;
   end for.
13. Set $R = |e_{11}e_{22} - e_{12}e_{21}|$.
14. Return $(R, p, l, m)$.
```

7. IMPLEMENTATION AND EXAMPLES

We begin with the trivial case where $\deg(G) = \deg(H) = 1$, so $g = 0$ and K is a rational function field. We recall that $u \in k$ is a primitive cube root of unity.

Proposition 7.1. *Let q be any (even or odd) prime power with $q \equiv 1 \pmod 3$, $G = at + b$, $H = at + c$ with $a, b, c \in k$, $a \neq 0$, and $b \neq c$. Then the function field $K = k(t)(\sqrt[3]{GH^2})$ has regulator $R = 1$ and a pair of fundamental units $\{\epsilon_1, \epsilon_2\}$ where*

$$\epsilon_1 = at + b\frac{u+2}{3} + c\frac{u^2+2}{3} + \rho + \omega,$$
$$\epsilon_2 = at + b\frac{u^2+2}{3} - c\frac{u+2}{3} + \rho + \omega.$$

Proof: $R = h = 1$ follows from (6–1). An easy, though somewhat messy, calculation shows that ϵ_1 and ϵ_2 have nonzero constant norm. It is also easy to see that both have equal degree, namely 1, so they must be independent. □

We now proceed with nontrivial examples. Since elements in $k\langle t^{-1}\rangle$ (and hence in K) are infinite series, they need to be approximated by finite series, just as real numbers are approximated by rationals for the purpose of computing. To this end, we proceed as in [Scheidler 00] and define for a nonzero element $\alpha = \sum_{i=-m}^{\infty} a_i t^{-i} \in k\langle t^{-1}\rangle$ of degree m the *relative approximation of precision $n \in \mathbb{N}_0$ to α* to be $\hat{\alpha} = \sum_{i=-m}^{n-m} a_i t^{-i}$. Then $|1 - \hat{\alpha}/\alpha| < q^{-n}$.

Fix a primitive cube root of unity $u \in k$ and an embedding of K into $k\langle t^{-1}\rangle$ so that the restriction of $|\cdot|$ on $k\langle t^{-1}\rangle$ onto K is $|\cdot|_0$. For sufficiently large n, we first extract the leading $n+1$ terms of the Puiseux series of some cube root ρ of $D = GH^2$. This yields a relative approximation $\hat{\rho}_0$ of precision n to ρ, so $|1 - \hat{\rho}_0/\rho|_0 < q^{-n}$. Setting $\hat{\rho}_1 = u\hat{\rho}_0$ and $\hat{\rho}_2 = u\hat{\rho}_1 = u^2\hat{\rho}_0$, we have $|1 - \hat{\rho}_i/\rho|_i < q^{-n}$ for $i = 0, 1, 2$. As in Lemma 7.1 of [Scheidler 00], set

$$\hat{\omega}_0 = \left\lfloor \frac{t^{n-\deg(D)/3}\hat{\rho}_0}{H} \right\rfloor, \qquad \hat{\omega}_1 = u^2\hat{\omega}_0, \qquad \hat{\omega}_2 = u\hat{\omega}_0;$$

then $|1 - \hat{\omega}_i/\omega|_i < q^{-n}$ for $i = 0, 1, 2$. If $\theta = a + b\rho + c\omega$ is any of the quantities used in Algorithm 4.6, i.e., $\theta \in \{\mu, \nu, \xi_\mu, \xi_\nu, \eta_\mu, \eta_\nu, \zeta_\mu, \zeta_\nu\}$, then we replace $\theta^{(i)} = a + b\rho^{(i)} + c\omega^{(i)}$ everywhere by $\hat{\theta}_i = a + b\hat{\rho}_i + c\hat{\omega}_i$ $(i = 0, 1, 2)$. Hence, the precision n must be sufficiently large that the algorithm still generates correct results. Most importantly, replacing $\xi_{\mu^{(i)}}$ and $\xi_{\nu^{(i)}}$ by their respective approximations in the expression $\lfloor \xi_{\mu^{(i)}}/\xi_{\nu^{(i)}} \rfloor$ should produce the same partial quotient; similarly for $\eta_{\mu^{(i)}}$ and $\eta_{\nu^{(i)}}$. The precision analysis of [Scheidler 00] for the unit rank 1 case can easily be adapted to the unit rank 2 scenario, showing that $n = \deg(GH)$ is generally sufficient.

$q=7$	$G=x^2+2x+6$	$H=x^2+5x+3$
$p=0$	$l=4$	$m=1$
$\epsilon_1=(6x^7+5x^6+2x^4+5x^3+6x^2+5x)$ $+(6x^5+2x^4+2x^3+5x^2+5x+1)\rho$ $+(6x^5+x^4+x^3+3x^2+x+2)\omega$		$\epsilon_2=(6x^3+4x^2+4)$ $+(5x+2)\rho$ $+3\omega$
Time for each unit: <1 s		

TABLE 1. A fundamental unit example.

Our implementation was written in Magma and run on a 1.2 Gigahertz AMD Athlon PC with 512 megabytes of memory. All our examples were done over prime fields $k=\mathbb{F}_q$ where q is a prime with $q \equiv 1 \pmod 3$. We randomly generated monic square-free coprime polynomials $G, H \in \mathbb{F}_q[t]$ so that $\deg(GH^2) \equiv 0 \pmod 3$ and $\deg(G) \geq \deg(H)$; the latter condition was imposed in lieu of the fact that the curves $y^3=GH^2$ and $y^3=G^2H$ generate the same function field and maximal order. For several not too large fields K, we computed a pair of fundamental units; however, for most fields, this was not feasible due to the size of the units—one runs out of virtual memory for fields of even moderate size—so we computed the regulator only. Our largest regulator $R=15\,314\,917$ occurred for $q=37$, $G=x^5+7x^4+31x^3$, $H=x^2+19x+24$, and took 9 hours, 47 minutes to compute.

We also compared some of our computational results with those given by Magma's built-in `Regulator()` function. In those cases where the built-in function produces a result, it gives the answer faster than our algorithm. However, `Regulator()` requires far more storage than Voronoi's algorithm and sometimes runs out of memory for even quite small fields; for example, it was unable to compute the not very large regulator $R=32239$ for $q=43$, $G=x^3+37x^2+17x+15$, and $H=x^3+18x^2+8x+33$, which our method produced in only 38 seconds. To be fair, however, Magma's `Regulator()` function works for arbitrary function fields, whereas Voronoi's technique is only applicable to cubic extensions.

As in the unit and regulator algorithms, p denotes the preperiod length and l the period length of the 0-chain of 1. Also, m is the number of steps performed for finding the second unit, i.e., the number of elements computed in the 2-chain of θ where θ is the first element in the primitive period of the 0-chain of 1. The set $\{\epsilon_1, \epsilon_2\}$ is a pair of fundamental units, and R is the regulator of the field $K=\mathbb{F}_q(t)(\sqrt[3]{GH^2})$. Table 1 explicitly lists the two fundamental units for an example with minimal nontrivial parameters ($q=7$, $\deg(G)=\deg(H)=2$). In Table 2, which uses larger parameters, we only give the degree of ϵ_1 and ϵ_2''; note that if $\epsilon_i=e_{0i}+e_{1i}\rho+e_{2i}\omega$ ($e_{0i}, e_{1i}, e_{2i} \in k[t]$ for $i=1,2$), then $|\epsilon_1|_0=|e_{01}|=|e_{11}\rho|=|e_{21}\omega|$ and $|\epsilon_2|_2=|e_{02}|=|e_{12}\rho|=|e_{22}\omega|$. For these examples, we still did compute the units explicitly; they were simply too large to write down while at the same time keeping the length of this paper within reasonable limits. Tables 1 and 2 also show the computation time (in minutes and seconds) for each unit.

For a more extensive set of parameters, we computed the regulator only (Table 3). Here, we give the total time required (in seconds, minutes, and hours) to find R. In four of our examples, $2R$ exceeds the upper Hasse-Weil bound (6–1), implying that the purely cubic function fields in question have ideal class number 1 and their Jacobians have order R. This occurred when $\deg(G)=4$ and $\deg(H)=1$ for $q=73$, 103, and 199, as well as when $q=811$. The corresponding values of R in Table 3 are marked with an asterisk (*).

We noticed that the preperiod p is often small compared to the period l, and is frequently equal to zero, particularly when $\deg(G)=\deg(H)$. Furthermore, all our examples show that m is very small compared to l most of the time; the only case where m is as large as l happens for some, but not all, of the examples where $\deg(G)=\deg(H)$. Finally, we observed that if G and H have equal degree, then the regulator R tends to be comparatively small. In fact, R is usually close to the product lm. From the bounds in Proposition 4.5, it is easy to infer that $l(m+j) \leq R \leq cl(m+j)$ where j is such that ϕ_m is associate to θ_j. Here, c depends only on $\deg(\Delta)$ and is no larger than $\deg(\Delta)^2/2$. Hence, if j is small, we do indeed expect $R \approx lm$, as our computations suggest. In any case, the sizes of R, p, l, m, and j clearly present an interesting subject for further study.

ACKNOWLEDGMENTS

Research of the second author was supported by NSA grant MSPF-00IG-253.

Field Parameters q, G, H	*p, l, m*	*Unit Degrees*	*Time per Unit*
$q = 7$	$p = 246$	$\deg(\epsilon_1) = 4791$	3 m 3 s
$G = x^8 + 2x^7 + 5x^6 + 5x^5 + 5x^4 + x^3 + 2x^2 + 4x + 3$	$l = 3595$	$\deg(\epsilon_2'') = 882$	1 s
$H = x^2 + 4x$	$m = 26$		
$q = 13$	$p = 5023$	$\deg(\epsilon_1) = 1547$	7 m 47 s
$G = x^7 + 4x^6 + 8x^5 + 9x^4 + 9x^3 + x + 7$	$l = 1312$	$\deg(\epsilon_2'') = 562$	38 s
$H = x + 1$	$m = 438$		
$q = 19$	$p = 231$	$\deg(\epsilon_1) = 1850$	40 s
$G = x^4 + 4x^3 + 18x$	$l = 1666$	$\deg(\epsilon_2'') = 646$	6 s
$H = x^4 + 12x^3 + 8x^2 + 14x + 15$	$m = 454$		
$q = 31$	$p = 0$	$\deg(\epsilon_1) = 998$	8 s
$G = x^4 + 28x^3 + 9x^2 + 30x + 13$	$l = 928$	$\deg(\epsilon_2'') = 454$	< 1 s
$H = x + 2$	$m = 2$		
$q = 37$	$p = 83$	$\deg(\epsilon_1) = 1849$	33 s
$G = x^3 + 26x + 26$	$l = 1744$	$\deg(\epsilon_2'') = 1265$	< 1 s
$H = x^3 + 19x^2 + 16x + 21$	$m = 44$		
$q = 43$	$p = 81$	$\deg(\epsilon_1) = 2975$	1 m 13 s
$G = x^4 + 42x^3 + 21x^2 + 19x + 35$	$l = 2841$	$\deg(\epsilon_2'') = 1309$	< 1 s
$H = x + 4$	$m = 8$		
$q = 73$	$p = 0$	$\deg(\epsilon_1) = 1144$	14 s
$G = x^2 + 65x + 34$	$l = 1131$	$\deg(\epsilon_2'') = 1061$	< 1 s
$H = x^2 + 45x + 43$	$m = 1$		

TABLE 2. Fundamental unit degree computations.

q	G	H	p	l	m	R	*Time*
7	$x^2 + 2x + 6$	$x^2 + 5x + 3$	0	4	1	13	< 1 s
	$x^4 + 5x^3 + 6x^2 + 5$	$x + 5$	0	7	7	163	1 s
	$x^3 + 2x^2 + 5x + 5$	$x^3 + 5x + 3$	0	2	2	37	< 1 s
	$x^5 + 4x^4 + 5x^3 + 4x^2 + 2x + 3$	$x^2 + 5x + 2$	21	47	42	3276	< 1 s
	$x^7 + 3x^6 + 2x^5 + 6x^4 + 3x^3 + x + 2$	$x + 5$	0	552	13	9589	2 s
	$x^4 + 5x^2 + 3x$	$x^4 + 4x^3 + 4x^2 + 4x + 3$	0	11	11	441	< 1 s
	$x^6 + 5x^5 + x^4 + x^3 + 6x^2 + 5$	$x^3 + 5x^2 + 4x + 1$	592	525	24	23344	7 s
	$x^8 + 2x^7 + 5x^6 + 5x^5 + 5x^4 + x^3 + 2x^2 + 4x + 3$	$x^2 + 4x$	246	3595	26	135121	46 s

TABLE 3. Regulator computations.

q	G	H	p	l	m	R	*Time*
13	$x^2+8x+10$	$x^2+10x+2$	0	11	3	61	<1 s
	$x^4+10x^3+11x^2+4x$	$x+9$	0	62	4	336	1 s
	x^3+7x^2+2x	x^3+8x^2 $+10x+11$	178	163	10	2569	4 s
	$x^5+9x^4+5x^3$ $+6x^2+2$	$x^2+10x+11$	3097	6933	12	186276	5 m 43 s
	$x^7+4x^6+8x^5+9x^4$ $+9x^3+x+7$	$x+1$	5023	1312	438	731092	2 m 57 s
	$x^4+8x^3+6x^2$ $+7x+12$	$x^4+x^3+11x^2$ $+2x+9$	192	3511	40	142861	1 m 20 s
	$x^6+8x^5+x^4+8x^3$ $+x^2+4x+1$	x^3+x^2 $+10x+12$	47819	32827	388	7401027	4 h 22 m
19	x^2+2x+5	x^2+7	0	156	2	307	<1 s
	x^4+9x^3+x+18	$x+13$	0	405	6	2817	1 s
	x^3+11x^2+x+15	x^3+3x^2+x+10	0	314	9	3769	<1 s
	$x^5+16x^4+18x^3$ $+6x^2+13x+5$	$x^2+17x+5$	188	10890	20	151801	5 m 17 s
	$x^7+8x^6+17x^5+17x^3$ $+16x^2+3x+1$	$x+13$	683	26324	127	3543631	26 m 58 s
	x^4+4x^3+18x	$x^4+12x^3+8x^2$ $+14x+15$	231	1666	544	1089148	18 s
31	$x^2+10x+10$	$x^2+10x+30$	0	1	1	4	<1 s
	$x^4+28x^3+9x^2$ $+30x+13$	$x+2$	0	928	2	3748	4 s
	x^3+28x^2+8x+3	$x^3+7x^2+18x+14$	0	66	66	5363	<1 s
	$x^5+12x^4+11x^3$ $+14x^2+11x+26$	$x^2+3x+20$	6068	13998	45	742228	18 m 48 s
37	$x^2+11x+32$	$x^2+27x+36$	0	3	3	25	<1 s
	$x^4+13x^3+36x^2$ $+36x+26$	$x+14$	111	133	132	19612	1 s
	$x^3+26x+26$	$x^3+19x^2+16x+21$	83	1744	44	90111	13 s
	$x^5+7x^4+31x^3$ $+12x^2+34x+35$	$x^2+19x+24$	4525	124605	113	15314917	9 h 47 m
43	$x^2+38x+30$	$x^2+30x+16$	194	297	5	1612	2 s
	$x^4+42x^3+21x^2$ $+19x+35$	$x+4$	81	2841	8	28861	29 s
	$x^3+37x^2+17x+15$	$x^3+18x^2+8x+33$	0	3393	9	32239	38 s
	$x^5+8x^4+26x^3$ $+31x^2+x+15$	$x^2+35x+17$	185	23690	21	849853	23 m 30 s

Table 3 (continued). Regulator computations.

q	G	H	p	l	m	R	*Time*
73	$x^2+65x+34$	$x^2+45x+43$	0	1131	1	1801	8 s
	$x^4+46x^3+51x^2$ $+51x+56$	$x+15$	384	17456	18	* 402928	14 m 21 s
	$x^3+24x^2+72x+32$	$x^3+58x^2+29x+13$	11847	18206	67	940251	41 m 34 s
103	$x^2+11x+101$	$x^2+101x+22$	10	31	31	1024	1 s
	x^4+63x^3 $+48x^2+96$	$x+62$	4349	20827	42	* 1046143	25 m 12 s
199	$x^2+156x+184$	$x^2+52x+158$	0	777	1	1459	19 s
	$x^4+47x^3+178x^2$ $+ 191\mathrm{x} + 68$	$x+33$	742	27561	243	* 6945127	40 m 41 s
811	$x^2+484x+424$	$x^2+546x+156$	145	765	765	* 591361	5 s
911	$x^2+516x+879$	$x^2+664x+267$	0	23060	3	107275	21 m 58 s

Table 3 (continued). Regulator computations.

REFERENCES

[Berwick 32] W. E. H. Berwick. "Algebraic Number-Fields with Two Independent Units." *Proc. London Math. Soc.* 34 (1932), 360–378.

[Bauer 03] M. Bauer. "The Arithmetic of Certain Cubic Function Fields." To appear in *Math. Comp.*

[Buchmann 85] J. A. Buchmann. "A Generalization of Voronoi's Algorithm I, II." *J. Number Theory* 20 (1985), 177–209.

[Delone and Fadeev 64] B. N. Delone and D. K. Fadeev. *The Theory of Irrationalities of the Third Degree. Transl. Math. Monographs* 10. Providence, RI: Amer. Math. Soc., 1964.

[Mang 87] M. Mang. "Berechnung von Fundamentaleinheiten in algebraischen, insbesondere rein-kubischen Kongruenzfunktionenkörpern." Diplomarbeit, Universität des Saarlandes, 1987.

[Pohst and Zassenhaus 97] M. Pohst and H. Zassenhaus. *Algorithmic Algebraic Number Theory*, 1st paperback edition. Cambridge, UK: Cambridge University Press, 1997.

[Scheidler 00] R. Scheidler. "Reduction in Purely Cubic Function Fields of Unit Rank One." In *Proc. Fourth Algorithmic Number Theory Symp. ANTS-IV*, pp. 515–532, Lect. Notes Comp. Sci. 1838. Berlin: Springer-Verlag, 2000.

[Scheidler and Stein 00] R. Scheidler and A. Stein. "Voronoi's Algorithm in Purely Cubic Congruence Function Fields of Unit Rank 1." *Math. Comp.* 69 (2000), 1245–1266.

[Stein and Williams 99] A. Stein and H. C. Williams. "Some Methods for Evaluating the Regulator of a Real Quadratic Function Field." *Experim. Math.* 8 (1999), 119–133.

[Stichtenoth 93] H. Stichtenoth. *Algebraic Function Fields and Codes.* Berlin: Springer-Verlag, 1993.

[Voronoi 96] G. F. Voronoi. "On a Generalization of the Algorithm of Continued Fractions (in Russian)." Doctoral dissertation, Warsaw, 1896.

[Williams et al. 73] H. C. Williams and C. R. Zarnke. "Computer Calculation of Units in Cubic Fields." In *Proc. Second Manitoba Conf. Num. Math. Congressus Numerantium* VII, pp. 433–468. Winnipeg, Manitoba: Utilitas Mathematica Publishing, Inc., 1973.

Yoonjin Lee, Department of Mathematics, Clark Science Center, Smith College, Northampton, MA 01063 (yjlee@smith.edu)

Renate Scheidler, Department of Mathematics and Statistics, University of Calgary, 2500 University Drive N.W.,
Calgary, AB, T2N 1N4, Canada (rscheidl@math.ucalgary.ca)

Christopher Yarrish, Harrisburg Area Community College, One HACC Drive, Harrisburg, PA 17110-2999 (cyarrish@hacc.edu)

Received July 31, 2002; accepted in revised form March 20, 2003.