# Reduction in Purely Cubic Function Fields of Unit Rank One

R. Scheidler
Department of Mathematical Sciences
University of Delaware, Newark DE 19716, USA
scheidle@math.udel.edu

April 27, 2000
CORR #2000-26

**Abstract**

This paper analyzes reduction of fractional ideals in a purely cubic function field of unit rank one. The algorithm is used for generating all the reduced principal fractional ideals in the field, thereby finding the fundamental unit or the regulator, as well as computing a reduced fractional ideal equivalent to a given nonreduced one. It is known how many reduction steps are required to achieve either of these tasks, but not how much time and storage each reduction step takes. Here, we investigate the complexity of a reduction step, the precision required in the approximation of the infinite power series that occur throughout the algorithm, and the size of the quantities involved.

## 1 Introduction and Motivation

Basis reduction of fractional ideals is one of the key ingredients in the computation of invariants of a purely cubic function field of unit rank one, such as the fundamental unit, the regulator, the ideal class number and, most importantly, the order of the Jacobian of the field. In fields of characteristic at least five, a basis reduction procedure was first presented in [2], and its discussion was continued in [1]. The algorithm was originally used for generating the entirety of reduced fractional principal ideals and thus finding the fundamental unit and the regulator of the field. Unfortunately, there are usually exponentially many such ideals, and enumerating them all is not the most efficient method for computing the regulator. This is where another aspect of ideal basis reduction comes into play: it quickly produces from a given nonreduced fractional ideal an equivalent reduced one.

The infrastructure of the set of reduced principal ideals is a powerful tool for invariant computations and a variety of other applications in both computational number theory and cryptography. Loosely speaking, the product of two reduced fractional principal ideals is generally not reduced; however, reduction produces a reduced ideal “close to” the product ideal, and the number of basis reduction steps required is polynomial in the size of the field. This phenomenon can be exploited for computing invariants of the field much faster than with the naive approach outlined above. For hyperelliptic, i.e. quadratic function fields (where reduction amounts to computing a simple continued fraction expansion), this was successfully accomplished in [3] with an improvement in complexity from $p$ to essentially $p^{2/5}$, where $p$ is the number of reduced fractional principal ideals. Work on the purely cubic setting is in progress at the time of writing, and we expect a similarly dramatic speed-up from our original method of [2].

While it is known how many reduction steps are required to compute the fundamental unit and the regulator of a purely cubic function field of unit rank one and characteristic at least five, it is as yet unclear how long an individual reduction step takes, how large the inputs and outputs get, and how much “precision” is required. Numerical experiments and heuristics suggest that the answers to these three questions are ‘not very long’, ‘not very large’, and ‘not too much’, respectively — at least in the reduced case — but we lack proof. This paper remedies this rather unsatisfactory situation. To that extent, we provide answers to the following questions:

- What is the complexity of an ideal basis reduction step?
- What is the size of the quantities involved?
- What is the minimal precision required in the approximation of the infinite series involved?

# 2 Purely Cubic Function Fields

A detailed treatment of this material can be found in [2] and [1]. A *purely cubic function field* is the function field of a plane curve given by the (not necessarily nonsingular) model $y^3 - D(x) = 0$ over a finite field $k = \mathbb{F}_q$ of order $q$ whose characteristic is not 3; here, $D(x) \in k[x]$ is a cubefree polynomial. Thus, a purely cubic function field can be viewed as a cubic extension $K = k(x)(\rho)$ of a rational function field $k(x)$ obtained by adjoining a cube root $\rho$ of a cubefree polynomial $D = D(x) \in k[x]$; this makes it the function field analogue of a purely cubic number field. We write $D = GH^2$ where $G, H \in k[x]$ are squarefree and coprime and $\deg(G) \geq \deg(H)$.

The integral closure $\mathcal{O}$ of $k[x]$ in $K$ is both a ring and a $k[x]$-module of rank 3 that is generated by the *integral basis* $\{1, \rho, \omega\}$ where $\omega = \rho^2/H$, so $\omega$ is a cube root of $\overline{D} = G^2H$. If $\alpha = a + b\rho + c\omega \in K$ $(a, b, c \in k(x))$, then the *conjugates* of $\alpha$ are $\alpha' = a + b\iota\rho + c\iota^2\omega$ and $\alpha'' = a + b\iota^2\rho + c\iota\omega$ where $\iota$ is a fixed primitive cube root of unity. The *norm* of $\alpha$ is $N(\alpha) = \alpha\alpha'\alpha'' = a^3 + b^3GH^2 + c^3G^2H - 3abcGH \in k(x)$.

We henceforth make the following assumptions:

- $q \equiv -1 \pmod 3$ (so $k$ contains no primitive cube roots of unity),
- $\deg(D) \equiv 0 \pmod 3$,
- The leading coefficient $\mathrm{sgn}(D)$ of $D$ is a cube in $k^* = k \setminus \{0\}$.

Then $K/k(x)$ has two points at infinity, namely one rational point and one quadratic point. The former gives rise to an embedding of $K$ into the field $k\langle x^{-1}\rangle$ of *Puiseux series* over $k$, and the Galois closure of $K$ is embeddable into $k(\iota)\langle x^{-1}\rangle$; nonzero elements in $k\langle x^{-1}\rangle$ (respectively, $k(\iota)\langle x^{-1}\rangle$) have the form $\alpha = \sum_{i=-m}^{\infty} a_i x^{-i} = \sum_{i=-\infty}^{m} a_{-i} x^i$ with $a_i \in k$ (respectively, $k(\iota)$) for $i \geq -m$ and $a_{-m} \neq 0$. The degree valuation on $k(x)$ extends canonically to $k\langle x^{-1}\rangle$ via $\deg(\alpha) = m$ and to $k(\iota)\langle x^{-1}\rangle$ via $\deg(\alpha + \beta\iota) = (\deg(\alpha + \beta\iota)(\alpha + \beta\iota^2)/2 = \deg(\alpha^2 - \alpha\beta + \beta^2)/2 \in \mathbb{Z}$ $(\alpha, \beta \in k\langle x^{-1}\rangle)$. For $\alpha = \sum_{i=-m}^{\infty} a_i x^{-i} \in k\langle x^{-1}\rangle$, we set $|\alpha| = q^{\deg(\alpha)}$, $\mathrm{sgn}(\alpha) = a_{-m}$, and $\lfloor \alpha \rfloor = \sum_{i=0}^{m} a_{-i} x^i$ (with $|0| = 0$ and $\lfloor 0 \rfloor = 0$). For $\alpha \in K$, we have $|\alpha'| = q^{\deg(\alpha')} = |\alpha'\alpha''|^{1/2}$. Note that $|G| \geq |H|$ implies $|\rho| \leq |\omega|$.

Under the above assumptions, $K$ has *unit rank* 1 over $k(x)$; that is, the the group $\mathcal{O}^*$ of units in $\mathcal{O}$ is isomorphic to $k^* \times \mathbb{Z}$ (see Theorem 2.1 of [2]). A generator $\epsilon$ of the torsionfree part of $\mathcal{O}^*$ is a *fundamental unit* of $K/k(x)$. If $\epsilon$ has positive degree (and is hence unique up to constant factors), then $R = \deg(\epsilon)/2 = -\deg(\epsilon')$ is the *regulator* of $K/k(x)$.

# 3 Fractional Ideals

A *fractional ideal* (of $\mathcal{O}$) is a subset $\mathfrak{f}$ of $K$ such that there exists a nonzero $d \in k[x]$ such that $d\mathfrak{f}$ is an integral ideal in $\mathcal{O}$, i.e. an additive subgroup of $\mathcal{O}$ that is also closed under multiplication by elements of $\mathcal{O}$. The unique monic polynomial $d = d(\mathfrak{f})$ of minimal degree that satisfies this condition is the *denominator* of $\mathfrak{f}$. $\mathfrak{f}$ is *principal* if it consists of $\mathcal{O}$-multiples of some $\theta \in K$; write $\mathfrak{f} = (\theta)$. The fractional ideals form an infinite Abelian group $\mathcal{I}$ under multiplication, of which the set of principal fractional ideals forms an infinite subgroup $\mathcal{P}$. The factor group $\mathcal{I}/\mathcal{P}$ is the *ideal class group* of $K/k(x)$; it is a finite Abelian group whose order is the *ideal class number* of $K/k(x)$. The product $h = Rh'$ where $R$ is the regulator of $K/k(x)$ is the order of the group of $k$-rational points on the *Jacobian* of $K$; it is independent of the element $x$ and thus the representation of $K$ as a function field. Two fractional ideals are *equivalent* if lie in the same coset in $\mathcal{I}/\mathcal{P}$, i.e. if they differ by a factor that is a principal fractional ideal.

We will henceforth assume "fractional ideal" to mean "nonzero fractional ideal containing 1". Then every fractional ideal $\mathfrak{f}$ is a $k[x]$-module of rank 3 with a basis $\{1, \mu, \nu\}$; write $\mathfrak{f} = [1, \mu, \nu]$. If $\mathfrak{f} = [1, \mu, \nu]$ where $\mu = (m_0 + m_1\rho + m_2\omega)/d$, $\nu = (n_0 + n_1\rho + n_2\omega)/d$ with $m_0$, $m_1$, $m_2$, $n_0$, $n_1$, $n_2$, $d \in k[x]$ jointly coprime and $d = d(\mathfrak{f})$, then the *norm of* $\mathfrak{f}$ is $N(\mathfrak{f}) = a(m_1n_2 - m_2n_1)/d^2 \in k(x)$ where $a \in k^*$ is chosen so that $N(\mathfrak{f})$ is monic. The *discriminant* of $\mathfrak{f}$ is

$$\Delta(\mathfrak{f}) = \det \begin{pmatrix} 1 & 1 & 1 \\ \mu & \mu' & \mu'' \\ \nu & \nu' & \nu'' \end{pmatrix}^2 \in k(x).$$

Both $N(\mathfrak{f})$ and $\Delta(\mathfrak{f})$ (up to a constant factor) are independent of the choice of $k[x]$-basis of $\mathfrak{f}$, and $N(\mathfrak{f})$ is multiplicative on the set of fractional ideals.

A *canonical basis* of a fractional ideal $\mathfrak{f}$ is a $k[x]$-basis $\{1, \alpha, \beta\}$ where $\alpha = s'(u + \rho)/s$, $\beta = s''(v + w\rho + \omega)/s$ with $s, s', s'', u, v, w \in k[x]$, $s's''$ divides $s$, $s''$ divides $H$, and $\gcd(s', H) = 1$. Here $s = d(\mathfrak{f})$ up to sign, and we may assume $|s'u|, |s''v| < |s|$, and $|w| < |s'|$. Such a basis always exists, and it is a simple matter to generate a canonical basis from any given basis, or compute a canonical basis of the product ideal of two fractional ideals given in terms of respective canonical bases (see [1]).

An element $\theta$ in a fractional ideal $\mathfrak{f}$ is a *minimum* in $\mathfrak{f}$ if for any $\phi \in \mathfrak{f}$, $|\phi| \le |\theta|$ and $|\phi'| \le |\theta'|$ imply $\phi \in k\theta$; that is, $\phi$ differs from $\theta$ only by a constant factor. $\mathfrak{f}$ is *reduced* if 1 is a minimum in $\mathfrak{f}$. It is easy to see that an element $\theta$ is a minimum in $\mathcal{O}$ if and only if the fractional principal ideal $\mathfrak{f} = (\theta^{-1})$ is reduced.

We summarize some properties of fractional ideals; the proofs of these results can be found in [2] and [1].

**Proposition 3.1** *Let $\mathfrak{f}$ be a fractional ideal.*

1. $\Delta(\mathfrak{f}) = a^2 N(\mathfrak{f})^2 \Delta$ *for some* $a \in k^*$.
2. $|d(\mathfrak{f})|^{-2} \le |N(\mathfrak{f})| \le |d(\mathfrak{f})|^{-1}$.
3. *If $\mathfrak{f}$ is reduced, then* $|\Delta(\mathfrak{f})| > 1$*, so* $|N(\mathfrak{f})| > |\Delta|^{-1/2}$.
4. *If $\mathfrak{f}$ is reduced, then* $|d(\mathfrak{f})| < |\Delta|^{1/2}$*, so* $|N(\mathfrak{f})| < |\Delta||d(\mathfrak{f})|^{-3}$.
5. *If* $|\Delta(\mathfrak{f})| > |d(\mathfrak{f})|^2$*, i.e.* $|d(\mathfrak{f})| < |N(\mathfrak{f})||\Delta|^{1/2}$*, then $\mathfrak{f}$ is reduced.*
6. *If $\mathfrak{f}$ is nonreduced, then* $|N(\mathfrak{f})| \le |\Delta|^{-1/4}$*, so* $|\Delta(\mathfrak{f})| \le |\Delta|^{1/2}$.

Let $\mathfrak{f}$ be a fractional ideal and let $\theta$ be a minimum in $\mathfrak{f}$. An element $\phi \in \mathfrak{f}$ is the *neighbor of $\theta$* in $\mathfrak{f}$ if $\phi$ is also a minimum in $\mathfrak{f}$, $|\theta| < |\phi|$, and for no $\psi \in \mathfrak{f}$, $|\theta| < |\psi| < |\phi|$ and

$|\psi'| < |\theta'|$. $\phi$ always exists and is unique up to nonzero constant factors (see Theorem 5.1 of [2]).

The *Voronoi chain* $(\theta_n)_{n\in\mathbb{N}}$ of successive minima in $\mathcal{O}$ where $\theta_1 = 1$ and $\theta_{n+1}$ is the neighbor of $\theta_n$ in $\mathcal{O}$ yields the entirety of minima in $\mathcal{O}$ of nonnegative degree (Voronoi first investigated this chain in cubic number fields in [4]). This chain is given by the recurrence $\theta_{n+1} = \mu_n\theta_n$ where $\mu_n$ is the neighbor of 1 in the reduced fractional principal ideal $\mathfrak{f}_n = (\theta_n^{-1})$ $(n \in \mathbb{N})$. The first nontrivial unit $\epsilon = \theta_{p+1}$ $(p \in \mathbb{N})$ encountered in this chain is the fundamental unit of $K$ of nonnegative degree. Since the recurrence for the Voronoi chain implies $\theta_{mp+n} = \epsilon^m\theta_n$ for $m \in \mathbb{N}_0$ and $n \in \mathbb{N}$, $\{\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_p\}$ is the complete set of reduced principal fractional ideals in $K$. The positive integer $p$ is the *period* of $\epsilon$. By Theorem 6.5 of [2], $p = O(q^{(\deg(\Delta)/2)-2})$, so there may be (and usually are) exponentially many reduced fractional ideals in $K/k(x)$.

# 4 Reduced Bases

For the remainder of the paper, we exclude the case of even characteristic, so $k$ has characteristic at least 5. For $\theta = l + m\rho + n\omega \in K$ with $l, m, n \in k(x)$, we define

$$\begin{aligned}
\xi_\theta &= \theta - l &&= m\rho + n\omega, \\
\eta_\theta &= (1+2\iota)^{-1}(\theta' - \theta'') &&= m\rho - n\omega, \\
\zeta_\theta &= \theta' + \theta'' &&= 2l - m\rho - n\omega,
\end{aligned} \tag{4.1}$$

where $\iota (\notin k)$ is a primitive cube root of unity. Then

$$\theta = \frac{1}{2}(3\xi_\theta + \zeta_\theta), \qquad \theta'\theta'' = \frac{1}{4}(3\eta_\theta^2 + \zeta_\theta^2), \tag{4.2}$$

so

$$|\theta'| = \max\{|\eta_\theta|, |\zeta_\theta|\}, \qquad |\xi_\theta| \le \max\{|\theta|, |\theta'|\}. \tag{4.3}$$

If $\{1, \theta, \phi\}$ is a basis of a fractional ideal $\mathfrak{f}$, then

$$(\xi_\mu\eta_\nu - \xi_\nu\eta_\mu)^2 = -\frac{4}{27}\Delta(\mathfrak{f}). \tag{4.4}$$

A $k[x]$-basis $\{1, \mu, \nu\}$ of a (reduced or nonreduced) fractional ideal $\mathfrak{f}$ is *reduced* if

$$\begin{gathered}
|\xi_\mu| > |\xi_\nu|, \quad |\zeta_\mu| < 1, \quad |\zeta_\nu| \le 1, \quad |\eta_\mu| < 1 \le |\eta_\nu|, \\
\text{if } \ |\eta_\nu| = 1, \ \text{then } \ |\nu| \ne 1.
\end{gathered} \tag{4.5}$$

The following procedure (which is essentially Algorithm 7.1 in [2]) generates a reduced basis of a fractional ideal.

**Algorithm 4.1** *(Ideal Basis reduction)*

*Input:* $\tilde{\mu}$, $\tilde{\nu}$ *where* $\{1, \tilde{\mu}, \tilde{\nu}\}$ *is a basis of some fractional ideal* $\mathfrak{f}$.

*Output:* $\mu$, $\nu$ *where* $\{1, \mu, \nu\}$ *is a reduced basis of* $\mathfrak{f}$.

*Algorithm:*

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

   3.1. *While* $|\xi_\nu \eta_\nu| > |\Delta(\mathfrak{f})|^{1/2}$, *replace*
$$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \quad by \quad \begin{pmatrix} 0 & 1 \\ -1 & \lfloor \xi_\mu/\xi_\nu \rfloor \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}.$$

   3.2. *Replace*
$$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \quad by \quad \begin{pmatrix} 0 & 1 \\ -1 & \lfloor \xi_\mu/\xi_\nu \rfloor \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}.$$

   3.3. *If* $|\eta_\mu| = |\eta_\nu|$, *replace*
$$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \quad by \quad \begin{pmatrix} 1 & -sgn(\eta_\mu \eta_\nu^{-1}) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}.$$
4. *While* $|\eta_\nu| < 1$, *replace*
$$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \quad by \quad \begin{pmatrix} 0 & 1 \\ -1 & \lfloor \xi_\mu/\xi_\nu \rfloor \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}.$$

   *While* $|\eta_\mu| \geq 1$, *replace*
$$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \quad by \quad \begin{pmatrix} \lfloor \eta_\nu/\eta_\mu \rfloor & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}.$$
5. *Replace* $\mu$ *by* $\mu - \lfloor \zeta_\mu \rfloor / 2$ *and* $\nu$ *by* $\nu - \lfloor \zeta_\nu \rfloor / 2$.
6. *If* $|\xi_\nu| = |\eta_\nu| = 1$, *replace* $\nu$ *by* $\nu - \lfloor \nu \rfloor$.

A reduced basis provides an easy means by which to determine whether or not an ideal is reduced (see [1]):

**Proposition 4.2** *Let $\{1, \mu, \nu\}$ be a reduced basis of a fractional ideal $\mathfrak{f}$.*

1. *If $\mathfrak{f}$ is reduced, then $\mu$ is the neighbor of 1 in $\mathfrak{f}$.*
2. *$\mathfrak{f}$ is reduced if and only if $|\mu| > 1$ and $\max\{|\nu|, |\eta_\nu|\} > 1$.*
3. *$\mathfrak{f}$ is nonreduced if and only if $|\mu| \leq 1$ or $|\nu| < |\eta_\nu| = 1$.*

Part 2 of Proposition 4.2 in conjunction with (4.3) and step 5 of Algorithm 4.1 implies that step 6 can only be entered if the input ideal $\mathfrak{f}$ is nonreduced. Part 1 of this proposition together with the recursion for the Voronoi chain shows that repeated application of Algorithm 4.1 to the ideal $\mathfrak{f}_n = (\theta_n^{-1})$ with subsequent division of $\mathfrak{f}_n$ by the neighbor $\mu_n$ of 1 in $\mathfrak{f}_n$ generates all the minima of nonnegative degree in $\mathcal{O}$ and hence the fundamental unit of $K$. A similar recursion allows for computing from a given nonreduced fractional ideal an equivalent reduced one.

Let $\mathfrak{f}$ be any nonreduced fractional ideal and define a sequence $(\mathfrak{f}_n)_{n\in\mathbb{N}}$ of pairwise equivalent fractional ideals as follows.

$$\mathfrak{f}_1 = \mathfrak{f}, \quad \mathfrak{f}_{n+1} = (\phi_n^{-1})\mathfrak{f}_n \quad \text{where} \quad \phi_n = \begin{cases} \mu_n & \text{if } |\mu_n| \leq 1, \\ \nu_n & \text{if } |\mu_n| > 1, \end{cases} \qquad (n \in \mathbb{N}) \tag{4.6}$$

and $\{1, \mu_n, \nu_n\}$ is a reduced basis of $\mathfrak{f}_n$. The case $\phi_n = \nu_n$ in (4.6) can happen at most once; that is, if $\mathfrak{f}_n$ is nonreduced with $|\mu_n| > 1$, then $\mathfrak{f}_{n+1}$ is reduced and a reduced basis of $\mathfrak{f}_{n+1}$ can be obtained directly without applying Algorithm 4.1:

**Proposition 4.3** *Let $\mathfrak{f}$ be a nonreduced ideal with a reduced basis $\{1, \mu, \nu\}$ and let $\mathfrak{g} = (\nu^{-1})\mathfrak{f} = [1, \mu\nu^{-1}, \nu^{-1}]$. If $|\mu| > 1$, then $\mathfrak{g}$ is reduced with a reduced basis $\{1, \mu\nu^{-1}, \nu^{-1}\}$.*

*Proof:* If $|\mu| > 1$, then by part 3 of Proposition 4.2 and (4.3) $|\nu| < 1 = |\eta_\nu| = |\nu'|$. Let $\alpha = \mu\nu^{-1}$ and $\beta = \nu^{-1}$. Then $|\alpha'| = |\mu'| < 1$, so $|\eta_\alpha| < 1$, $|\zeta_\alpha| < 1$, and since $|\alpha| > 1$, $|\xi_\alpha| = |\alpha|$ by (4.2). Furthermore, $|\beta'| = 1$, so $|\zeta_\beta| \leq 1$, and $|\xi_\beta| = |\beta| = |\nu|^{-1} > 1$. Since $\eta_\beta = -\eta_\nu(\nu'\nu'')^{-1}$, $|\eta_\beta| = 1$.

Since $|\alpha| > 1$ and $\max\{|\beta|, |\eta_\beta|\} > 1$, $\mathfrak{g}$ is reduced by part 2 of Proposition 4.2. Since $|\xi_\alpha| = |\alpha| > |\nu|^{-1} = |\xi_\beta|$, $|\eta_\alpha| < 1 = |\eta_\beta|$, $|\zeta_\alpha| < 1$, and $|\zeta_\beta| \leq 1$, $\{1, \alpha, \beta\}$ is a reduced basis of $\mathfrak{g}$. $\square$

A polynomial number of steps of recursion (4.6) produces a reduced ideal (see [1]):

**Proposition 4.4** *Let $\mathfrak{f} = \mathfrak{f}_1$ be a nonreduced fractional ideal.*

1. *The recursion (4.6) produces a reduced fractional ideal $\mathfrak{f}_m$ equivalent to $\mathfrak{f}$ for some $m \in \mathbb{N}$.*

2. *If $m$ in part 1 is minimal, i.e. $\mathfrak{f}_m$ is reduced and $\mathfrak{f}_n$ is nonreduced for $n < m$, then*

$$m \leq \max\left\{1, \frac{1}{2}\left(5 - \deg(N(\mathfrak{f})) - \frac{1}{4}\deg(\Delta)\right)\right\}.$$

3. *If $\mathfrak{f}$ is the product of two reduced ideals and $m$ is as in part 2, then*

$$m \leq \frac{3}{8}\left(\deg(\Delta) + 4\right).$$

As an aside, we mention the *infrastructure* of the set $\{\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_p\}$ of reduced principal fractional ideals. If $\mathfrak{f}_i = (\theta_i)^{-1}$ for $i = 1, 2, \ldots, p$, then the *distance* of $\mathfrak{f}_i$ is $\delta_i = \deg(\theta_i)$. From part 3 of Proposition 4.4, a reduced principal ideal $\mathfrak{f}$ can be obtained by applying no more than $3(\deg(\Delta) + 4)/8$ iterations of (4.6) to the initial (generally nonreduced) product ideal $\mathfrak{f}_i\mathfrak{f}_j$. Moreover, $\delta(\mathfrak{f}) = \delta_i + \delta_j + \delta$ with $\delta = O(\deg(\Delta)) = O(\log p)$, so the distance of $\mathfrak{f}$ is within a logarithmically small 'error' of where one would expect it to be. As pointed out in section 1, this phenomenon allows for much faster computation of the fundamental unit and other invariants of $K/k(x)$.

The implementation of Algorithm 4.1 raises a number of questions: How large do the degrees of $\theta$, $\xi_\theta$, and $\eta_\theta$ ($\theta \in \{\mu, \nu\}$) and those of their basis coefficients get throughout the algorithm? How often the while loops in steps 3.1 and 4 executed? And how does one determine absolute values of $\xi_\theta$ and $\eta_\theta$, and compute the quantities $\lfloor \xi_\mu/\xi_\nu \rfloor$ in steps 3.2 and 4 as well as $\lfloor \eta_\mu/\eta_\nu \rfloor$ in step 4? These questions will be addressed in the next three sections.

# 5 Input/Output Sizes in Ideal Basis Reduction

We begin with the following empirical observation; for quadratic integers (as opposed to Puiseux series), this is referred to as the *Gauß-Kuz'min law.* Let $\alpha = \alpha_0 \in k\langle x^{-1}\rangle$ and define $a_i = \lfloor \alpha_i \rfloor \in k[x]$ and $\alpha_{i+1} = (\alpha_i - a_i)^{-1}$ for $i \in \mathbb{N}_0$. Then the $a_i$ ($i \in \mathbb{N}_0$) are the partial quotients in the simple continued fraction expansion of $\alpha$, and for $i \in \mathbb{N}$, $a_i$ will almost always have very small degree. The quotients $\lfloor \xi_\mu/\xi_\nu \rfloor$ in steps 3.1, 3.2, and the first while loop of step 4 are easily seen to be partial quotients in the simple continued fraction expansion of $\xi_{\mu_0}/\xi_{\nu_0}$ where $\mu_0$ and $\nu_0$ are the inputs of step 3.1 or, if that loop is never entered, of step 3.2; similarly for $\lfloor \eta_\nu/\eta_\mu \rfloor$ in the second while loop of step 4. These quotients will therefore almost always have very small degree, with the possible exception of the very first such partial quotient.

Let $\{1, \mu, \nu\}$ be a reduced basis of some fractional ideal $\mathfrak{f}$ that was computed using Algorithm 4.1. Since $|\eta_\mu| < 1 \leq |\eta_\nu|$, and $\eta_\nu$ and $\eta_\mu$ differ by a factor that is a partial quotient as described above, $|\eta_\nu|$ will usually have quite small degree, and $|\eta_\mu|$ will not be much smaller that 1. By (4.5) and (4.4), $|\xi_\nu| < |\xi_\mu| \leq |\Delta(\mathfrak{f})|^{1/2}$, so usually, $|\xi_\mu|$ will be close to $|\Delta(\mathfrak{f})|^{1/2}$, and since $\xi_\mu$ and $\xi_\nu$ once again differ by a factor that is a partial quotient in a simple continued fraction expansion, $|\xi_\nu|$ will not be much smaller than $|\xi_\mu|$.

We have the following rigorous bounds on reduced bases:

**Proposition 5.1** *Let* $\{1, \mu, \nu\}$ *be a reduced basis of a fractional ideal, where* $\mu = (m_0 + m_1\rho + m_2\omega)/d$, $\nu = (n_0 + n_1\rho + n_2\omega)/d$ *with* $m_0, m_1, m_2, n_0, n_1, n_2 \in k[x]$ *and* $d = d(\mathfrak{f})$.

1. $\lfloor m_0/d \rfloor = \lfloor m_1\rho/d \rfloor = \lfloor m_2\omega/d \rfloor = 3\lfloor \mu \rfloor$.
2. $|\mu| \leq \max\{q^{-1}, |\Delta(\mathfrak{f})|^{1/2}\}$, $|m_0|, |m_1\rho|, |m_2\omega| \leq \max\{q^{-1}|d|, |\Delta|^{1/2}\}$, $|\nu| \leq \max\{1, q^{-1}|\Delta(\mathfrak{f})|^{1/2}\}$, $|n_1\rho + n_2\omega| < |\Delta|^{1/2}$, $|n_0| \leq \max\{|d|, q^{-1}|\Delta|^{1/2}\}$.
3. *If* $|\mu| > 1$, *then* $|\nu| < |\mu| \leq |\Delta(\mathfrak{f})|^{1/2}$, $|m_0| = |m_1\rho| = |m_2\omega| \leq |\Delta|^{1/2}$, $|n_0|, |n_1\rho|, |n_2\omega| < |\Delta|^{1/2}$.

*Proof:* Part 1 follows immediately from $|\eta_\mu| < 1$ and $|\zeta_\mu| < 1$. For part 2, we note that from (4.2), (4.5), and (4.4) $|\mu| \leq \max\{|\zeta_\mu|, |\xi_\mu|\}$ with $|\zeta_\mu| < 1$ and $|\xi_\mu| = |\Delta(\mathfrak{f})|^{1/2}|\eta_\nu|^{-1} \leq |\Delta(\mathfrak{f})|^{1/2}$. The bounds on $|m_1\rho|$ and $|m_2\omega|$ follow from $|m_1\rho - m_2\omega| = |d\eta_\mu| < |d|$ and $|m_1\rho + m_2\omega| = |d\xi_\mu| \leq |dN(\mathfrak{f})||\Delta|^{1/2} \leq |\Delta|^{1/2}$ by (4.4) and the first two parts of Proposition 3.1. Furthermore, $|m_0| \leq \max\{|d\xi_\nu|, |d\zeta_\nu|\}$. Now by (4.2) $|\nu| \leq \max\{|\zeta_\mu|, |\xi_\nu|\}$ with $|\zeta_\nu| \leq 1$ and $|\xi_\nu| < |\xi_\mu| \leq |\Delta(\mathfrak{f})|^{1/2}$ by (4.4), $|d\xi_\nu| < |d\xi_\mu| \leq |\Delta|^{1/2}$, and $|n_0| \leq \max\{|d\zeta_\nu|, |d\xi_\nu|\} \leq \max\{|d|, q^{-1}|\Delta|^{1/2}\}$. The bounds in part 3 follow from part 1, (4.2), and the fact that $|d| < |\Delta|^{1/2}$ by part 4 of Proposition 3.1. □

Note that unfortunately, we have no rigorous upper bound on $|\eta_\nu|$ and hence on $|n_1\rho|$ and $|n_2\omega|$ in the (nonreduced) case where $|\mu| \leq 1$. However, as we saw above, these values will generally not be too large. We proceed to analyze the sizes of the inputs of step 2 of Algorithm 4.1.

**Lemma 5.2**

1. *Let* $\mathfrak{f}_1$ *be a fractional ideal and let* $\mathfrak{f}_{n+1} = (\mu_n^{-1})\mathfrak{f}_n$ *where* $\{1, \mu_n, \nu_n\}$ *is a reduced basis of* $\mathfrak{f}_n$ $(n \in \mathbb{N})$. *Let* $\mathfrak{f} = \mathfrak{f}_{n+1} = [1, \mu^{-1}, \nu\mu^{-1}]$ *for some* $n \in \mathbb{N}$ *with* $\mu = \mu_n$ *and* $\nu = \nu_n$. *Then*

$$\max\left\{|\eta_{\mu^{-1}}|, \frac{|\eta_{\nu\mu^{-1}}|}{|\nu'|}\right\} = \frac{1}{|\mu'|},$$

$$|\xi_{\mu^{-1}}| \leq \frac{1}{\min\{|\mu|, |\mu'|\}}, \quad |\xi_{\nu\mu^{-1}}| \leq \max\left\{\frac{|\nu|}{|\mu|}, \frac{|\nu'|}{|\mu'|}\right\} \leq \frac{|\nu'|}{\min\{|\mu|, |\mu'|\}}.$$

$$|\Delta(\mathfrak{f})|^{1/2} \leq \max\{|\xi_{\mu^{-1}}\eta_{\nu\mu^{-1}}|, |\xi_{\nu\mu^{-1}}\eta_{\mu^{-1}}|\} \leq |\Delta(\mathfrak{f})|^{1/2}\frac{\max\{|\mu|, |\mu'|\}}{|\xi_\mu|}.$$

*If* $\mathfrak{f}_n$ *is reduced, then*

$$\max\{|\eta_{\mu^{-1}}|, |\xi_{\mu^{-1}}|\} = \frac{1}{|\mu'|} \leq |\Delta(\mathfrak{f})|^{1/4},$$

$$\max\{|\eta_{\nu\mu^{-1}}|, |\xi_{\nu\mu^{-1}}|\} = \frac{|\nu'|}{|\mu'|} < |\Delta(\mathfrak{f})|^{1/2},$$

$$\max\{|\xi_{\mu^{-1}}\eta_{\nu\mu^{-1}}|, |\xi_{\nu\mu^{-1}}\eta_{\mu^{-1}}|\} = |\Delta(\mathfrak{f})|^{1/2}.$$

*If* $\mathfrak{f}_n$ *is nonreduced and* $\mathfrak{f}_1$ *is the product of two reduced fractional ideals, then*

$$\max\left\{|\eta_{\mu^{-1}}|, \frac{|\eta_{\nu\mu^{-1}}|}{|\nu'|}\right\} < |\Delta(\mathfrak{f})\Delta|^{1/4},$$

$$\max\left\{|\xi_{\mu^{-1}}|, \frac{|\xi_{\nu\mu^{-1}}|}{|\nu'|}\right\} \leq q^{-3}|\Delta(\mathfrak{f})\Delta|^{1/2}.$$

$$\max\left\{|\xi_{\mu^{-1}}\eta_{\mu^{-1}}|, \frac{\xi_{\nu\mu^{-1}}\eta_{\nu\mu^{-1}}|}{|\nu'|^2}\right\} \leq q^{-2}|\Delta(\mathfrak{f})\Delta|^{1/2}.$$

2. *Let* $\{1, \alpha, \beta\}$ *be a canonical basis of a fractional ideal* $\mathfrak{f}$*. Then*

$$\left|\frac{\rho}{d(\mathfrak{f})}\right| \leq |\xi_\alpha|, |\eta_\alpha| \leq |\rho|, \quad \left|\frac{\omega}{d(\mathfrak{f})}\right| \leq \max\{|\xi_\beta|, |\eta_\beta|\} \leq |\omega|.$$

*If* $\mathfrak{f}$ *is reduced, then* $|\xi_\alpha|, |\eta_\alpha| > |\omega|^{-1}$*,* $\max\{|\xi_\beta|, |\eta_\beta|\} > |\rho|^{-1}$.

*If* $\mathfrak{f}$ *is the product of two reduced fractional ideals, then*

$$|\xi_\alpha|, |\eta_\alpha| \geq \frac{q^2}{|\Delta|^{1/2}|\omega|}, \quad \max\{|\xi_\beta|, |\eta_\beta|\} \geq \frac{q^2}{|\Delta|^{1/2}|\rho|}.$$

*Proof:*

1. We have by (4.3) $|\eta_{\mu^{-1}}| \leq |\mu'|^{-1}$, $|\xi_{\mu^{-1}}| \leq \max\{|\mu|^{-1}, |\mu'|^{-1}\}$, $|\eta_{\nu\mu^{-1}}| \leq |\nu'||\mu'|^{-1}$, and $|\xi_{\nu\mu^{-1}}| \leq \max\{|\nu||\mu|^{-1}|, |\nu'||\mu'|^{-1}\}$. Since $|\nu| \leq \max\{1, |\xi_\mu|\} \leq \max\{1, |\mu|\}$, we have $|\nu||\mu|^{-1} \leq \max\{1, |\mu|^{-1}\} \leq |\nu'|\max\{|\mu|^{-1}, |\mu'|^{-1}\}$.

   A simple computation reveals that

$$\eta_{\mu^{-1}} = -\frac{\eta_\mu}{\mu'\mu''}, \quad \eta_{\nu\mu^{-1}} = \frac{\eta_\nu\zeta_\mu - \eta_\mu\zeta_\nu}{2\mu'\mu''}.$$

   Since $\max\{|\zeta_\mu|, |\eta_\mu|\} = |\mu'|$, one of $\eta_{\mu^{-1}}$ and $\eta_{\nu\mu^{-1}}/\eta_\nu$ has absolute value $|\mu'|^{-1}$.

   Now by (4.4) $|\xi_{\mu^{-1}}\eta_{\nu\mu^{-1}} - \xi_{\nu\mu^{-1}}\eta_{\mu^{-1}}| = |\Delta(\mathfrak{f})|^{1/2}$, so $|\Delta(\mathfrak{f})|^{1/2}$ cannot exceed both summands in absolute value. By (4.4), an upper bound on the absolute values of both terms is given by

$$\frac{|\nu'|}{|\mu'|\min\{|\mu|, |\mu'|\}} = \frac{|\Delta(\mathfrak{f}_n)|^{1/2}}{|\mu'\xi_\mu|\min\{|\mu|, |\mu'|\}} = |\Delta(\mathfrak{f})|^{1/2}\frac{\max\{|\mu|, |\mu'|\}}{|\xi_\mu|}$$

since $\Delta(\mathfrak{f}) = N(\mu)^{-2}\Delta(\mathfrak{f}_n)$.

If $\mathfrak{f}_n$ is reduced, then $|\mu| > 1$, so $|\xi_\mu| = \max\{|\mu|, |\mu'|\} = |\mu|$ and $|\nu| \le \max\{1, |\xi_\nu|\} < |\mu|$. Furthermore,

$$\zeta_{\mu^{-1}} = \frac{\zeta_\mu}{\mu'\mu''}, \quad \zeta_{\nu\mu^{-1}} = \frac{\zeta_\mu\zeta_\nu - 3\eta_\mu\eta_\nu}{2\mu'\mu''}.$$

If $|\zeta_\mu| = |\mu'|$, then $|\eta_{\nu\mu^{-1}}| = |\nu'||\mu'|^{-1}$ and $|\xi_{\mu^{-1}}| = |2\mu^{-1} - \zeta_{\mu^{-1}}| = |\mu'|^{-1}$. If $|\eta_\mu| = |\mu'|$, then $|\eta_{\mu^{-1}}| = |\mu'|^{-1}$ and $|\xi_{\nu\mu^{-1}}| = |2\nu\mu^{-1} - \zeta_{\nu\mu^{-1}}| = |\nu'||\mu'|^{-1}$. Finally, $|\mu'|^2 = |N(\mu)||\mu|^{-1} \ge |N(\mu)||\Delta(\mathfrak{f}_n)|^{-1/2} = |\Delta(\mathfrak{f})|^{-1/2}$ and $|\nu'||\mu'|^{-1} = |\Delta(\mathfrak{f}_n)|^{1/2}|\mu\mu'|^{-1} < |\Delta(\mathfrak{f}_n)|^{1/2}|N(\mu)| = |\Delta(\mathfrak{f})|^{1/2}$.

If $\mathfrak{f}_n$ is nonreduced, then $|\mu| \le 1$. If $\mathfrak{f}_1$ is the product of two reduced ideals, then by part 3 of Proposition 3.1, $|\Delta(\mathfrak{f}_n)| \ge \Delta(\mathfrak{f}_1)| \ge q^4|\Delta|^{-1}$. Then $|\mu'|^2 \ge |N(\mu)| = |\Delta(\mathfrak{f})^{-1}\Delta(\mathfrak{f}_n)|^{1/2} \ge q^2|\Delta(\mathfrak{f})\Delta|^{-1/2}$ and $\min\{|\mu|, |\mu'|\} \ge q^{-1}|N(\mu)| \ge q^3|\Delta(\mathfrak{f})\Delta|^{-1/2}$.

2. Let $\alpha = s^{-1}s'(u + \rho)$, $\beta = s^{-1}s''(v + w\rho + \omega)\}$. Then $\xi_\alpha = \eta_\alpha = s's^{-1}\rho$, $\xi_\beta = s''s^{-1}(w\rho + \omega)$, $\eta_\beta = s''s^{-1}(w\rho - \omega)$ with $|w| < |s'|$. Since $|s's''| \le |s| = |d(\mathfrak{f})|$ and $|\rho| \le |\omega|$, the first set of bounds follows. If $\mathfrak{f}$ is reduced, then $|d(\mathfrak{f})| < |\Delta|^{1/2} = |\rho\omega|$ by part 4 of Proposition 3.1. If $\mathfrak{f}$ is the product of two reduced fractional ideals, then $|d(\mathfrak{f})| \le |N(\mathfrak{f})|^{-1} \le q^2|\Delta|$ by parts 2 and 3 of Proposition 3.1.

□

We point out that in the situation where Algorithm 4.1 is applied to the product $\mathfrak{f}$ of two reduced fractional ideals (as is the case in the infrastructure scenario, for example), the input is a canonical basis and not of the form $\{\mu^{-1}, \nu\mu^{-1}\}$.

We now proceed to investigate the workings of ideal basis reduction in more detail; in particular, we will see how the sizes of the quantities $\xi_\mu$, $\xi_\nu$, $\eta_\mu$, and $\eta_\nu$ change throughout Algorithm 4.1. We point out that after step 2 of the algorithm, $|\xi_\nu| \le |\xi_\mu|$ and $|\eta_\nu| \le |\eta_\mu|$.

**Lemma 5.3**

1. *In step 3.1 of Algorithm 4.1, $\xi_\mu$ and $\eta_\mu$ do not increase in absolute value in the first iteration and decrease in absolute value in each subsequent iteration. $\xi_\nu$ and $\eta_\nu$ decrease in absolute value in each iteration. Furthermore, $|\xi_\mu| > |\xi_\nu|$ and $|\eta_\mu| > |\eta_\nu|$ after each iteration.*
2. *Step 3.2 of Algorithm 4.1 decreases $\xi_\mu$, $\xi_\nu$, and $\eta_\mu$, but does not decrease $\eta_\nu$ in absolute value. After execution, $|\xi_\mu| > |\xi_\nu|$ and $|\eta_\mu| \le |\eta_\nu|$.*
3. *Step 3.3 of Algorithm 4.1 leaves the absolute values of $\xi_\mu$, $\xi_\nu$, and $\eta_\nu$ unchanged, but decreases $\eta_\mu$ in absolute value. After execution, $|\xi_\mu| > |\xi_\nu|$ and $|\eta_\mu| < |\eta_\nu|$.*

*Proof:* Let $\{\alpha, \beta\}$ be the input and $\{\mu, \nu\}$ the output of any iteration of step 3.1, step 3.2, or step 3.3.

Since $|\xi_\nu \eta_\nu| > |\Delta(\mathfrak{f})|^{1/2}$ if and only if $|\xi_\mu/\xi_\nu - \eta_\mu/\eta_\nu| < 1$, or equivalently, if and only if $\lfloor \xi_\mu/\xi_\nu \rfloor = \lfloor \eta_\mu/\eta_\nu \rfloor$, we have in step 3.1

$$\begin{aligned} \xi_\mu &= \xi_\beta, & \xi_\nu &= -\xi_\alpha + \left\lfloor \frac{\xi_\alpha}{\xi_\beta} \right\rfloor \xi_\beta, \\ \eta_\mu &= \eta_\beta, & \eta_\nu &= -\eta_\alpha + \left\lfloor \frac{\eta_\alpha}{\eta_\beta} \right\rfloor \eta_\beta. \end{aligned}$$

Therefore $|\xi_\nu| < |\xi_\beta| = |\xi_\mu|$ and $|\eta_\nu| < |\eta_\beta| = |\eta_\mu|$. From step 2 of the algorithm, in the first iteration $|\xi_\alpha| \geq |\xi_\beta|$ and $|\eta_\alpha| \geq |\eta_\beta|$, so $|\xi_\mu| \leq |\xi_\alpha|$ and $|\eta_\mu| \leq |\eta_\alpha|$. In subsequent iterations, we have $|\xi_\alpha| > |\xi_\beta|$ and $|\eta_\alpha| > |\eta_\beta|$, so $|\xi_\mu| = |\xi_\beta| < |\xi_\alpha|$ and $|\eta_\mu| = |\eta_\beta| < |\eta_\alpha|$.

In step 3.2, the transformations on $\xi_\mu, \xi_\nu, \eta_\mu$ are the same as in step 3.1, so each of these quantities decrease in absolute value, and we still have $|\xi_\mu| \geq |\xi_\nu|$. Furthermore,

$$|\eta_\nu| = \left| \left( -\eta_\alpha + \left\lfloor \frac{\eta_\alpha}{\eta_\beta} \right\rfloor \eta_\beta \right) - \left( \left\lfloor \frac{\eta_\alpha}{\eta_\beta} \right\rfloor - \left\lfloor \frac{\xi_\alpha}{\xi_\beta} \right\rfloor \right) \eta_\beta \right|.$$

The first term in the difference has absolute value less than $|\eta_\beta|$, while the second term is at least $|\eta_\beta|$ in absolute value because $|\lfloor \eta_\alpha/\eta_\beta \rfloor - \lfloor \xi_\alpha/\xi_\beta \rfloor| \geq 1$. So $|\eta_\nu| \geq |\eta_\beta| = |\eta_\mu|$.

In step 3.3, we have $\nu = \beta$, so $\xi_\nu$ and $\eta_\nu$ are unchanged. Furthermore, if $a = \operatorname{sgn}(\eta_\alpha \eta_\beta^{-1})$, then $|\xi_\mu| = |\xi_\alpha - a\xi_\beta| = |\xi_\alpha|$ as $|\xi_\alpha| > |\xi_\beta| = |\xi_\nu|$. Finally, since $a = \lfloor \eta_\alpha/\eta_\beta \rfloor$, $|\eta_\mu| < |\eta_\beta| = |\eta_\nu|$. □

**Lemma 5.4**

1. *In the first loop of step 4 of Algorithm 4.1, $\xi_\mu$ and $\xi_\nu$ decrease in absolute value in each iteration, while $\eta_\mu$ and $\eta_\nu$ increase in absolute value in each iteration.*
2. *In the seconds loop of step 4 of Algorithm 4.1, $\xi_\mu$ and $\xi_\nu$ increase in absolute value in each iteration, while $\eta_\mu$ and $\eta_\nu$ decrease in absolute value in each iteration.*
3. *Throughout step 4, $|\xi_\mu| > |\xi_\nu|$ and $|\eta_\mu| < |\eta_\nu|$. At most one of the while loops in step 4 is entered, and after the last iteration of either of the loops, $|\xi_\mu| > |\xi_\nu|$ and $|\eta_\mu| < 1 \leq |\eta_\nu|$.*

*Proof:* Once again, let $\{\alpha, \beta\}$ be the input and $\{\mu, \nu\}$ the output of any iteration of either of the while loops of step 4. By Lemma 5.3, $|\xi_\alpha| > |\xi_\beta|$ and $|\eta_\alpha| < |\eta_\beta|$ before step 4 is entered, and at most one of the loops is entered.

Since the first loop of step 4 uses the same transformation as step 3.1, $\xi_\mu$ and $\xi_\nu$ display the same behavior as in that step. Furthermore, $|\eta_\mu| = |\eta_\beta| < |\eta_\alpha|$ and $|\eta_\nu| = |\lfloor \xi_\alpha/\xi_\beta \rfloor \eta_\beta -$

$\eta_\alpha| > |\eta_\beta| = |\eta_\mu|$. In the second loop of step 4, $|\xi_\mu| = |\lfloor \eta_\beta/\eta_\alpha \rfloor \xi_\alpha - \xi_\beta| > |\xi_\alpha| = |\xi_\nu|$ and $|\eta_\mu| < |\eta_\alpha| = |\eta_\nu|$. It is also clear from the conditions of the while loops that $|\eta_\mu| < 1 \leq |\eta_\nu|$, once execution of step 4 is completed. □

The previous two lemmata show that $|\eta_\nu|$ takes on its largest value throughout the algorithm either after step 3.2 or after the first loop of step 4 if that value is less than 1 after step 3.2. Since in both cases $|\eta_\nu \xi_\mu| = |\Delta(\mathfrak{f})|^{1/2}$, and we generally at least expect $|\xi_\mu| \geq |d(\mathfrak{f})|^{-1}$, we usually have by parts 1 and 2 of Proposition 3.1 $|\eta_\nu| \leq |d||\Delta(\mathfrak{f})|^{1/2} \leq |\Delta|^{1/2}$ for this maximal value.

# 6 Complexity of Ideal Basis Reduction

We now investigate how often each of the while loops in the basis reduction algorithm.

**Proposition 6.1** *Let $\mathfrak{f} = [1, \mu, \nu]$ where $\mu, \nu$ are the inputs of Algorithm 4.1. Assume that $|\xi_\mu| \geq |\xi_\nu|$ and $|\eta_\mu| \geq |\eta_\nu|$, so step 2 has been executed. Denote by $r$, $s$, and $t$ the number of iterations of step 3.1, the first loop in step 4, and the second loop in step 4, respectively. Then*

$$r \leq \max\left\{0, \frac{1}{2}\left(\deg(\xi_\nu \eta_\nu) - \frac{1}{2}\deg(\Delta(\mathfrak{f})) + 1\right)\right\},$$

$$r + s \leq \max\{0, \deg(\xi_\nu) - \frac{1}{2}\deg(\Delta(\mathfrak{f}))\}, \quad r + t \leq \max\{0, \deg(\eta_\nu) + 1\}.$$

*Proof:* Let $\{\mu_0, \nu_0\}$ be the first input and $\{\mu_i, \nu_i\}$ the output after iteration $i$ $(1 \leq i \leq r)$ of step 3.1. From part 1 of Lemma 5.3 $|\xi_{\nu_i}| < |\xi_{\nu_{i-1}}|$ and $|\eta_{\nu_i}| < |\eta_{\nu_{i-1}}|$, so inductively $|\xi_{\nu_i}| \leq q^{-i}|\xi_\nu|$ and $|\eta_{\nu_i}| \leq q^{-i}|\eta_\nu|$ for $1 \leq i \leq r$. Then $|\Delta(\mathfrak{f})|^{1/2} \leq q^{-1}|\xi_{\nu_{r-1}}\eta_{\nu_{r-1}}| \leq q^{1-2r}|\xi_\nu\eta_\nu|$, so $q^r \leq (|\xi_\nu\eta_\nu||\Delta(\mathfrak{f})|^{-1/2}q)^{1/2}$.

Again, let $\{\mu_0, \nu_0\}$ be the first input and $\{\mu_i, \nu_i\}$ the output after iteration $i$ $(1 \leq i \leq s)$ of the first loop of step 4. Then $|\eta_{\nu_0}| < 1$. Analogous to the previous part, we infer from Lemma 5.4 that $|\eta_{\nu_i}| \geq q^i|\eta_{\nu_0}|$ for $1 \leq i \leq s$, and $|\eta_{\nu_{s-1}}| < 1 \leq |\eta_{\nu_s}|$. Then $1 \geq q|\eta_{\nu_{s-1}}| \geq q^s|\eta_{\nu_0}|$. Here, $\nu_0$ is the $\nu$ value output by step 3.3 and hence by 3.2 (since 3.3 leaves it unchanged). Thus, the corresponding $\eta_\nu$ is the quantity $\eta_{\nu_{r+1}}$, where we interpret step 3.2 as the $(r+1)$-st iteration of the loop in step 3.1. Now $|\eta_{\nu_{r+1}}| = |\Delta(\mathfrak{f})|^{1/2}|\xi_{\nu_r}|^{-1} \geq q^r|\Delta(\mathfrak{f})|^{1/2}|\xi_\nu|^{-1}$. Thus, $q^{r+s} \leq |\xi_\nu||\Delta(\mathfrak{f})|^{-1/2}$.

In the second loop of step 4 of Algorithm 4.1, we have $|\eta_{\mu_i}| \leq q^{-i}|\eta_{\mu_0}|$ for $1 \leq i \leq t$, and $|\eta_{\mu_t}| < 1 \leq |\eta_{\mu_{t-1}}|$. Then $1 \leq |\eta_{\nu_{t-1}}| \leq q^{-(t-1)}|\eta_{\mu_0}|$, where $|\mu_0|$ is $\mu$ value output by step 3.3. The corresponding $|\eta_{\mu_0}|$ is at most equal to $|\eta_{\mu_{r+1}}|$. Then $|\eta_{\mu_{r+1}}| = |\eta_{\nu_r}| \leq q^{-r}|\eta_\nu|$, so $q^{r+t} \leq q|\eta_\nu|$. □

**Corollary 6.2** *Let $r$, $s$, and $t$ be as in Lemma 5.2. Let $\mathfrak{f}$ be the input ideal and $\{1, \mu, \nu\}$ the input basis of Algorithm 4.1. Assume that $|\xi_\mu| \geq |\xi_\nu|$ and $|\eta_\mu| \geq |\eta_\nu|$, so step 2 has been executed.*

1. *Suppose $\mathfrak{f} = \mathfrak{f}_{n+1}$ for some $n \in \mathbb{N}$, where $\mathfrak{f}_1$ is a fractional ideal, $\mathfrak{f}_{n+1} = (\mu_n^{-1})\mathfrak{f}_n$ with $\{1, \mu_n, \nu_n\}$ a reduced basis of $\mathfrak{f}_n$ ($n \in \mathbb{N}$).*
   *If $\mathfrak{f}_n$ is reduced, then $r = s = 0, \quad t \leq \frac{1}{4}\deg(\Delta(\mathfrak{f})) + 1$.*
   *If $\mathfrak{f}_n$ is nonreduced and $\mathfrak{f}_1$ is the product of two reduced fractional ideals, then*
   $$r \leq \frac{1}{4}\deg(\Delta) - \frac{1}{2}, \quad r + s \leq \frac{1}{2}\deg(\Delta) - 3, \quad r + t \leq \frac{1}{4}\deg(\Delta(\mathfrak{f})\Delta) + 1.$$
2. *Suppose $\{1, \mu, \nu\}$ is a canonical basis of $\mathfrak{f}$. Then*
   $$r \leq \frac{1}{2}(\deg(d(\mathfrak{f})) + 1), \quad r + s \leq \max\{0, \deg(d(\mathfrak{f})) - \deg(\omega)\}, \quad r + t \leq \deg(\rho) + 1.$$
   *If $\mathfrak{f} = \mathcal{O}$, i.e. $\nu = \rho$ and $\mu = \omega$, then $r = s = 0, \quad t \leq \deg(\rho) + 1$.*
   *If $\mathfrak{f}$ is reduced, then $r \leq \frac{1}{4}\deg(\Delta), \quad r + s < \deg(\rho), \quad r + t \leq \deg(\rho) + 1$.*
   *If $\mathfrak{f}$ is the product of two reduced fractional ideals, then*
   $$r < \frac{1}{2}\deg(\Delta), \quad r + s \leq \frac{1}{2}\deg(\Delta) + \deg(\rho) - 2, \quad r + t \leq \deg(\rho) + 1.$$

*Proof:* Part 1 follows directly from the bounds in Lemma 5.2. For part 2, let $\{1, \alpha, \beta\}$ be a canonical basis of $\mathfrak{f}$ with $\alpha = s's^{-1}\rho$ and $\beta = s''s^{-1}(w\rho + \omega)$. Since $|\rho| \leq |\omega|$, $|\xi_\alpha\eta_\alpha||\Delta(\mathfrak{f})|^{-1/2} \leq |s'\rho||s''\omega|^{-1} \leq |s| = |d(\mathfrak{f})|$, $|\xi_\alpha||\Delta(\mathfrak{f})|^{-1/2} = |s||s''\omega|^{-1} \leq |d(\mathfrak{f})||\omega|^{-1}$, and $|\eta_\alpha| \leq |\rho|$. Once again by Proposition 3.1, $|d(\mathfrak{f})| < |\Delta|^{1/2}$ if $\mathfrak{f}$ is reduced and $|d(\mathfrak{f})| \leq q^{-2}|\Delta|$ if $\mathfrak{f}$ is the product of two reduced ideals. If $\nu = \rho$ and $\mu = \omega$, then $|\xi_\nu\eta_\nu| = |\rho|^2 \leq |\Delta|^{1/2} = |\Delta(\mathcal{O})|^{1/2}$ and $|\xi_\nu| < |\Delta|^{1/2}$. □

Corollary 6.2 reveals that if the input ideal $\mathfrak{f}$ of Algorithm 4.1 is either equal to $\mathcal{O}$ (with basis $\{1, \rho, \omega\}$), or is of the form $\mathfrak{f} = \mathfrak{f}_{n+1} = (\mu_n^{-1})\mathfrak{f}_n$ where $\mathfrak{f}_n$ is reduced and $\{1, \mu_n, \nu_n\}$ is a reduced basis of $\mathfrak{f}_n$, then step 3.1, the first while loop in step 4, and step 6 can be omitted. This is the case, in particular, if the regulator or the fundamental unit of $K/k(x)$ are computed by generating the recursion $\mathfrak{f}_{n+1} = (\mu_n^{-1})\mathfrak{f}_n$ with $\mathfrak{f}_1 = \mathfrak{f}_{p+1} = \mathcal{O}$.

**Algorithm 6.3** *(Basis reduction, input ideal of special form)*

*Input:* $\tilde{\mu}$, $\tilde{\nu}$ *where* $\{1, \tilde{\mu}, \tilde{\nu}\}$ *is a basis of some fractional ideal* $\mathfrak{f}$. *Here,* $\{\tilde{\mu}, \tilde{\nu}\} = \{\rho, \omega\}$ *or* $\{\tilde{\mu}, \tilde{\nu}\} = \{\phi^{-1}, \theta\phi^{-1}\}$ *where* $\{1, \phi, \theta\}$ *is a reduced basis of a reduced fractional ideal.*

*Output:* $\mu$, $\nu$ *where* $\{1, \mu, \nu\}$ *is a reduced basis of* $\mathfrak{f}$.

*Algorithm:*

1. *Set* $\mu = \tilde{\mu}$, $\nu = \tilde{\nu}$.
2. *If* $|\xi_\mu| < |\xi_\nu|$ *or if* $|\xi_\mu| = |\xi_\nu|$ *and* $|\eta_\mu| < |\eta_\nu|$, *replace*

$$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \quad by \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}.$$

3. *If* $|\eta_\mu| \geq |\eta_\nu|$
   3.1. *Replace*

$$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \quad by \quad \begin{pmatrix} 0 & 1 \\ -1 & \lfloor \xi_\mu/\xi_\nu \rfloor \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}.$$

   3.2. *If* $|\eta_\mu| = |\eta_\nu|$, *replace*

$$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \quad by \quad \begin{pmatrix} 1 & -sgn(\eta_\mu \eta_\nu^{-1}) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}.$$

4. *While* $|\eta_\mu| \geq 1$, *replace*

$$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \quad by \quad \begin{pmatrix} \lfloor \eta_\nu/\eta_\mu \rfloor & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}.$$

5. *Replace* $\mu$ *by* $\mu - \lfloor \zeta_\mu \rfloor/2$ *and* $\nu$ *by* $\nu - \lfloor \zeta_\nu \rfloor/2$.

# 7 Precision Required for Ideal Basis Reduction

When computing absolute values as well as integer parts of quotients as required in basis reduction algorithm, the relevant quantities of the form $b\rho \pm c\omega$ need to be approximated to sufficient "precision" with a Puiseux series in $k\langle x^{-1}\rangle$ that is truncated at some suitable negative power of $x$. Our numerical experiments in [2] show that increasing the precision or even using variable precision does not have a significant impact on the running time of the algorithm; for example, a reduction in precision from $\deg(D)$ to $\deg(D)/2$ made a difference of only 5-10 percent in computation time. Nevertheless, it is desirable to have a lower bound on the minimal precision required; in [2], where we implemented Algorithm 4.1 for reduced ideals only, we relied exclusively on heuristics and numerical evidence in determining our precision.

We define a *relative approximation of precision* $n \in \mathbb{N}_0$ to an element $\alpha = \sum_{i=-m}^{\infty} a_i x^{-i} \in k\langle x^{-1}\rangle$ to be $\hat{\alpha}_n = \sum_{i=-m}^{n-\deg(\alpha)} a_i x^{-i}$. Then $|1 - \hat{\alpha}/\alpha| < q^{-n}$, or equivalently, $|\alpha - \hat{\alpha}| < q^{\deg(\alpha)-n}$. To approximate a quantity of the form $\theta = b\rho + c\omega$ with $b, c \in k(x)$, such as $\xi_\mu$, $\xi_\nu$, $\eta_\mu$, and $\eta_\nu$, we generate relative approximations $\hat{\rho}_n$ and $\hat{\omega}_n$ of sufficient precision $n$ to $\rho$ and $\omega$, respectively, and approximate $\theta$ by $\hat{\theta} = b\hat{\rho}_n + c\hat{\omega}_n$. $\hat{\rho}_n$ is precomputed by explicitly extracting a cube root of $D \in k[x]$ so that the coefficients of $x^{\deg(D)/3}, \ldots, x, 1, x^{-1}, \ldots, x^{n-\deg(D)/3}$ are correct, and $\hat{\omega}_n$ is given by the following lemma.

**Lemma 7.1** *Let $\hat{\rho}_n$ be a relative approximation of precision $n$ to $\rho$. Then $\hat{\omega}_n = \lfloor x^{n-\deg(\omega)}\hat{\rho}_n^2/H \rfloor x^{\deg(\omega)-n}$ is a relative approximation of precision $n$ to $\omega$.*

*Proof:* Set $F = \lfloor x^{n-\deg(\omega)}\hat{\rho}_n^2/H \rfloor \in k[x]$ and let $\theta = x^{n-\deg(\omega)}\hat{\rho}_n^2/H - F \in k\langle x^{-1}\rangle$, so $|\theta| < 1$. Then

$$|\omega - \hat{\omega}_n| = \left| \frac{\rho^2}{H} - x^{\deg(\omega)-n}\left( x^{n-\deg(\omega)}\frac{\hat{\rho}_n^2}{H} - \theta \right) \right| = \left| \frac{\rho^2}{H} - \frac{\hat{\rho}_n^2}{H} + x^{\deg(\omega)-n}\theta \right|.$$

Now $|\rho^2 - \hat{\rho}_n^2| = |\rho + \hat{\rho}_n||\rho - \hat{\rho}_n| < q^{2\deg(\rho)-n}$, so $|\rho^2 - \hat{\rho}_n^2||H|^{-1} < q^{2\deg(\rho)-\deg(H)-n} = q^{\deg(\omega)-n}$. Furthermore, $|x^{\deg(\omega)-n}\theta| < q^{\deg(\omega)-n}$. It follows that $|1 - \hat{\omega}_n/\omega| < q^{-n}$. $\square$

Henceforth, we denote by $\hat{\rho}_n$ and $\hat{\omega}_n$ relative approximations of some precision $n \in \mathbb{N}$ to $\rho$ and $\omega$, respectively. For $\theta = a + b\rho + c\omega$ with $a, b, c \in k(x)$, we set

$$\hat{\theta} = a + b\hat{\rho}_n + c\hat{\omega}_n, \quad \hat{\xi}_\theta = b\hat{\rho}_n + c\hat{\omega}_n, \quad \hat{\eta}_\theta = b\hat{\rho}_n - c\hat{\omega}_n, \quad \hat{\zeta}_\theta = 2a - b\hat{\rho}_n - c\hat{\omega}_n.$$

The following lemma gives lower bounds on the precision required to compute absolute values and integer parts of certain Puiseux series correctly.

**Lemma 7.2** *Let $\theta, \phi \in k(x)$.*

1. *If $m \in \mathbb{Z}$ and $q^{n+m} \geq \max\{|\xi_\theta|, |\eta_\theta|\}$, then $|\xi_\theta| = q^m$ if and only if $|\hat{\xi}_\theta| = q^m$, $|\xi_\theta| \leq q^m$ if and only if $|\hat{\xi}_\theta| \leq q^m$, and $|\xi_\theta| < q^m$ if and only if $|\hat{\xi}_\theta| < q^m$.*
2. *If $q^n \geq \max\left\{1, \left|\frac{\eta_\theta}{\xi_\theta}\right|\right\}$, then $|\xi_\theta| = |\hat{\xi}_\theta|$.*
3. *If $q^n \geq \max\{|\xi_\theta|, |\eta_\theta|\}$, then $\lfloor \theta \rfloor = \lfloor \hat{\theta} \rfloor$ and $\lfloor \zeta_\theta \rfloor = \lfloor \hat{\zeta}_\theta \rfloor$.*
4. *If $|\xi_\theta| \geq |\xi_\phi|$ and $q^n \geq \max\left\{1, \left|\frac{\xi_\theta}{\xi_\phi}\right|, \left|\frac{\eta_\theta}{\xi_\phi}\right|, \left|\frac{\xi_\theta\eta_\phi}{\xi_\phi^2}\right|\right\}$, then $\left\lfloor \frac{\xi_\theta}{\xi_\phi} \right\rfloor = \left\lfloor \frac{\hat{\xi}_\theta}{\hat{\xi}_\phi} \right\rfloor$.*

*Proof:* If $\theta = a + b\rho + c\omega$ with $a, b, c \in k[x]$, then

$$\begin{aligned} |\theta - \hat{\theta}| &= |\xi_\theta - \hat{\xi}_\theta| = |\zeta_\theta - \hat{\zeta}_\theta| \\ &= |b(\rho - \hat{\rho}_n) + c(\omega - \hat{\omega}_n)| < \max\{|b\rho|, |c\omega|\}q^{-n} = \max\{|\xi_\theta|, |\eta_\theta|\}q^{-n}. \end{aligned}$$

This immediately yields parts 1–3. For part 4, we have

$$\frac{\hat{\xi}_\theta}{\hat{\xi}_\phi} = \frac{\xi_\theta}{\xi_\phi} + \frac{\xi_\theta(\xi_\phi - \hat{\xi}_\phi)}{\xi_\phi\hat{\xi}_\phi} + \frac{\hat{\xi}_\theta - \xi_\theta}{\hat{\xi}_\phi}.$$

Suppose that $|\xi_\theta| \geq |\xi_\phi|$ and $q^n \geq \max\{1, |\xi_\theta/\xi_\phi|, |\eta_\theta/\xi_\phi|, |\xi_\theta\eta_\phi/\xi_\phi^2|\}$. Then

$$\left|\frac{\xi_\theta(\xi_\phi - \hat{\xi}_\phi)}{\xi_\phi\hat{\xi}_\phi}\right| < \frac{|\xi_\theta|}{|\xi_\phi|^2}\max\{|\xi_\phi|, |\eta_\phi|\}q^{-n} \leq 1;$$

similarly, $|(\hat{\xi}_\theta - \xi_\theta)/\hat{\xi}_\phi| < 1$. So $\lfloor \xi_\theta/\xi_\phi \rfloor = \lfloor \hat{\xi}_\theta/\hat{\xi}_\phi \rfloor$. □

We are now able to give lower bounds on $n$ for the different steps of Algorithm 4.1. We consider a precision of $n$ to be sufficient if in any identity or condition on a quantity $\theta$, $\theta$ can be replaced by a relative approximation $\hat{\theta}$ of precision $n$ to $\theta$. For example, $n$ is sufficient for step 3.1 of Algorithm 4.1 if $|\xi_\nu\eta_\nu| > |\Delta)(\mathfrak{f})|^{1/2}$ exactly if $|\hat{\xi}_\nu\hat{\eta}_\nu| > |\Delta(\mathfrak{f})|^{1/2}$ and if $\lfloor \xi_\mu/\xi_\nu \rfloor = \lfloor \hat{\xi}_\mu/\hat{\xi}_\nu \rfloor$ in every iteration of the loop.

**Lemma 7.3** *Let $\mathfrak{f}$ be the input ideal and $\{1, \mu, \nu\}$ the input basis of Algorithm 4.1 Define $\{\alpha, \beta\} = \{\gamma, \delta\} = \{\mu, \nu\}$ such that $|\xi_\alpha| \geq |\xi_\beta|$ and $|\eta_\gamma| \geq |\eta_\delta|$. Let $r$, $s$, and $t$ be as in Proposition 6.1. Then a precision of $n$ is sufficient for*

1. *step 2 and the if condition at the start of step 3 if* $q^n \geq \max\left\{\left|\frac{\eta_\gamma}{\xi_\alpha}\right|, \left|\frac{\xi_\alpha}{\eta_\gamma}\right|\right\}$;
2. *step 3.1 if* $q^n \geq \max\left\{\left|\frac{\xi_\alpha}{\xi_\beta}\right|, \left|\frac{\xi_\alpha}{\eta_\gamma}\right|, \left|\frac{\eta_\gamma}{\xi_\beta}\right|, \frac{|\xi_\beta|^2}{|\Delta(\mathfrak{f})|^{1/2}}, \frac{|\xi_\beta\eta_\delta|}{|\Delta(\mathfrak{f})|^{1/2}}, q^{l_r-2}\frac{|\eta_\delta|^2}{\Delta(\mathfrak{f})|^{1/2}}\right\}$ *where* $q^{l_r} = \left|\frac{\xi_{\mu_r}}{\xi_{\nu_r}}\right|$ *for* $r \geq 1$;
3. *step 3.2 if* $q^n \geq \max\left\{\left|\frac{\xi_\alpha}{\xi_\beta}\right|, \left|\frac{\eta_\gamma}{\xi_\beta}\right|, \left|\frac{\xi_\alpha\eta_\delta}{\xi_\beta^2}\right|, q^{l_r}, q^{2l_r-2}\frac{|\eta_\delta|^2}{\Delta(\mathfrak{f})|^{1/2}}\right\}$;
4. *step 3.3 if* $q^n \geq \max\left\{1, \frac{|\xi_\beta|^2}{|\Delta(\mathfrak{f})|^{1/2}}\right\}$;
5. *the first while loop of step 4 if* $q^n \geq \max\left\{|\Delta(\mathfrak{f})|^{1/2}, |\xi_\beta|, q^l, \frac{q^{2l_{s-1}-2}}{|\Delta(\mathfrak{f})|^{1/2}}\right\}$ *where* $q^l = \max_{0\leq i\leq s-1}\left\{\left|\frac{\xi_{\mu_i}}{\xi_{\nu_i}}\right|\right\}$ *and* $q^{l_{s-1}} = \left|\frac{\xi_{\mu_{s-1}}}{\xi_{\nu_{s-1}}}\right|$;
6. *the second while loop of step 4 if* $q^n \geq \max\left\{q^m, q^{m_t}|\Delta(\mathfrak{f})|^{1/2}\right\}$ *where* $q^m = \max_{0\leq j\leq t-1}\left\{\left|\frac{\eta_{\nu_j}}{\eta_{\mu_j}}\right|\right\}$ *and* $q^{m_t} = \left|\frac{\eta_{\nu_t}}{\eta_{\mu_t}}\right|$;
7. *steps 5 and 6 if* $q^n \geq \max\{q^{m_t}, |\Delta(\mathfrak{f})|^{1/2}\}$.

*Proof:* We use the results of Lemma 7.2 and the same notation as in the proof of Proposition 6.1.

1. Since $q^n \geq \max\{1, |\eta_\alpha/\xi_\alpha|\}$, $|\xi_\alpha| = |\hat{\xi}_\alpha|$, and since $q^n \geq \max\{|\xi_\beta/\xi_\alpha|, |\eta_\beta/\xi_\alpha|\}$, $|\xi_\nu| < |\xi_\mu|$ if and only if $|\hat{\xi}_\nu| < |\hat{\xi}_\nu|$. Finally, $q^n \geq \max\{|\eta_\delta/\eta_\gamma|, |\xi_\delta/\eta_\gamma|\}$ implies $|\eta_\mu| < |\eta_\nu|$ if and only if $|\hat{\eta}_\mu| < |\hat{\eta}_\nu|$ and $|\eta_\mu| \geq |\eta_\nu|$ if and only if $|\hat{\eta}_\mu| \geq |\hat{\eta}_\nu|$.
2. We have $\alpha = \gamma = \mu_0$ and $\beta = \delta = \nu_0$, $|\xi_{\nu_i}| \leq |\xi_\beta|$, $|\eta_{\nu_i}| \leq |\eta_\delta|$, and $|\xi_{\nu_i}\eta_{\nu_i}| > |\Delta(\mathfrak{f})|^{1/2} \geq |\xi_{\nu_r}\eta_{\nu_r}|$ for $0 \leq i \leq r-1$. Furthermore, $|\xi_{\mu_i}/\xi_{\nu_i}| = |\eta_{\mu_i}/\eta_{\nu_i}|$, so $|\eta_{\nu_i}/\xi_{\nu_i}| = |\eta_\delta/\xi_\beta| = |\eta_\gamma/\xi_\alpha|$ for $0 \leq i \leq r-1$.

   Hence, since $q^n \geq \max\{1, |\eta_\gamma/\xi_\alpha|, |\xi_\alpha/\eta_\gamma|\}$, $|\xi_{\nu_i}| = |\hat{\xi}_{\nu_i}|$, and $|\eta_{\nu_i}| = |\hat{\eta}_{\nu_i}|$ for $0 \leq i \leq r-1$. Also, if $r \geq 1$, then
   $$\left|\frac{\eta_{\nu_r}}{\xi_{\nu_r}}\right| = q^{l_r}\left|\frac{\eta_{\nu_r}\eta_{\nu_{r-1}}}{\xi_{\nu_{r-1}}\eta_{\nu_{r-1}}}\right| \leq q^{l_r-2}\frac{|\eta_\delta|^2}{|\Delta(\mathfrak{f})|^{1/2}},$$
   so $|\xi_{\nu_r}| = |\hat{\xi}_{\nu_r}|$. Furthermore, since
   $$q^n \geq \max\left\{\frac{|\xi_\beta\eta_\delta|}{|\Delta(\mathfrak{f})|^{1/2}}, \frac{|\xi_\beta|^2}{|\Delta(\mathfrak{f})|^{1/2}}\right\} \geq \frac{|\xi_{\nu_i}|}{|\Delta(\mathfrak{f})|^{1/2}}\max\{|\eta_{\nu_i}|, |\xi_{\nu_i}|\},$$
   then $|\eta_{\nu_i}| \leq |\Delta(\mathfrak{f})|^{1/2}/|\xi_{\nu_i}|$ if and only if $|\hat{\eta}_{\nu_i}| \leq |\Delta(\mathfrak{f})|^{1/2}/|\xi_{\nu_i}|$ for $0 \leq i \leq r$.

   Finally, if $r \geq i \geq 1$, then $|\xi_{\mu_i}/\xi_{\nu_i}| < |\xi_{\nu_{i-1}}\eta_{\nu_i}|/|\Delta(\mathfrak{f})|^{1/2} < |\xi_\beta\eta_\delta|/|\Delta(\mathfrak{f})|^{1/2}$ and $|\eta_{\mu_i}/\xi_{\nu_i}| < |\eta_\delta|^2/|\Delta(\mathfrak{f})|^{1/2}$. Also, $|\xi_{\mu_i}\eta_{\nu_i}/\xi_{\nu_i}|^2 = |\eta_{\nu_i}/\xi_{\nu_i}|$ for $0 \leq i \leq r-1$. Hence, $q^n \geq \max\{|\xi_\alpha/\xi_\beta|, |\eta_\gamma/\xi_\beta|, |\xi_\beta\eta_\delta|/|\Delta(\mathfrak{f})|^{1/2}, |\eta_\delta|^2/|\Delta(\mathfrak{f})|^{1/2}\}$ implies $\lfloor\xi_{\mu_i}/\xi_{\nu_i}\rfloor = \lfloor\hat{\xi}_{\mu_i}/\hat{\xi}_{\nu_i}\rfloor$ for $0 \leq i \leq r-1$.
3. If $r \geq 1$, then $|\xi_{\mu_r}/\xi_{\nu_r}| = q^{l_r}$,
   $$\left|\frac{\eta_{\mu_r}}{\xi_{\nu_r}}\right| = q^{l_r}\left|\frac{\eta_{\nu_{r-1}}^2}{\xi_{\nu_{r-1}}\eta_{\nu_{r-1}}}\right| < q^{l_r}\frac{|\eta_\delta|^2}{|\Delta(\mathfrak{f})|^{1/2}},$$
   $$\left|\frac{\xi_{\mu_r}\eta_{\nu_r}}{\xi_{\nu_r}^2}\right| = q^{2l_r}\left|\frac{\eta_{\nu_r}\eta_{\nu_{r-1}}}{\xi_{\nu_{r-1}}\eta_{\nu_{r-1}}}\right| \leq q^{2l_r-2}\frac{|\eta_\delta|^2}{|\Delta(\mathfrak{f})|^{1/2}}.$$
4. $|\xi_{\nu_{r+1}}/\eta_{\nu_{r+1}}| = |\xi_{\nu_r}\xi_{\nu_{r+1}}|/|\Delta(\mathfrak{f})|^{1/2} < |\xi_\beta|^2/|\Delta(\mathfrak{f})|^{1/2}$ and $|\xi_{\nu_r}/\eta_{\nu_{r+1}}| = |\xi_{\nu_r}|^2/|\Delta(\mathfrak{f})|^2 \leq |\xi_\beta|^2/|\Delta(\mathfrak{f})|^{1/2}$. So if $q^n \geq \max\{1, |\xi_\beta|/|\Delta(\mathfrak{f})|^{1/2}\}$, then $|\eta_{\nu_{r+1}}| = |\hat{\eta}_{\nu_{r+1}}|$ and $|\eta_{\nu_r}| = |\eta_{\nu_{r+1}}|$ if and only if $|\hat{\eta}_{\nu_r}| = |\eta_{\nu_{r+1}}|$.
5. We have $|\eta_{\nu_i}| < 1 \leq |\eta_{\nu_s}|$, so $|\xi_{\mu_i}| > |\Delta(\mathfrak{f})|^{1/2} \geq |\xi_{\mu_s}|$ for $0 \leq i \leq s-1$. Since $q^n \geq \max\{1, |\xi_\beta|\} \geq \max\{|\eta_{\nu_i}|, |\xi_{\nu_i}| : 0 \leq i \leq s-1\}$, $|\eta_{\nu_i}| < 1$ if and only if $|\hat{\eta}_{\nu_i}| < 1$. Also $|\xi_{\nu_s}/\eta_{\nu_s}| \leq |\Delta(\mathfrak{f})|^{1/2}$, so $q^n \geq \max\{1, |\Delta(\mathfrak{f})|^{1/2}\}$ yields $|\eta_{\nu_s}| = |\hat{\eta}_{\nu_s}|$.

   Now $|\xi_{\mu_i}/\xi_{\nu_i}| \leq q^l$ for $0 \leq i \leq s-1$, and for $0 \leq i \leq s-2$:
   $$\left|\frac{\eta_{\mu_i}}{\xi_{\nu_i}}\right| < \left|\frac{\eta_{\nu_i}}{\xi_{\mu_{i+1}}}\right| < \frac{1}{|\Delta(\mathfrak{f})|^{1/2}}, \qquad \left|\frac{\xi_{\mu_i}\eta_{\nu_i}}{\xi_{\nu_i}^2}\right| = \frac{|\Delta(\mathfrak{f})|^{1/2}}{\xi_{\mu_{i+1}}^2} < \frac{1}{|\Delta(\mathfrak{f})|^{1/2}}$$

and
$$\left|\frac{\eta_{\mu_{s-1}}}{\xi_{\nu_{s-1}}}\right| \le \frac{q^{l_{s-1}-2}}{|\xi_{\mu_{s-1}}|} \le \frac{q^{l_{s-1}-3}}{|\Delta(\mathfrak{f})|^{1/2}},$$
$$\left|\frac{\eta_{\nu_{s-1}}\xi_{\mu_{s-1}}}{\xi^2_{\nu_{s-1}}}\right| = \frac{|\Delta(\mathfrak{f})|^{1/2}}{|\xi_{\nu_{s-1}}|^2} = q^{2l_{s-1}}\frac{|\Delta(\mathfrak{f})|^{1/2}}{|\xi_{\mu_{s-1}}|^2} \le \frac{q^{2l_{s-1}-2}}{|\Delta(\mathfrak{f})|^{1/2}}.$$

It follows that $\lfloor \xi_{\mu_i}/\xi_{\nu_i}\rfloor = \lfloor \hat{\xi}_{\mu_i}/\hat{\xi}_{\nu_i}\rfloor$ for $0 \le i \le s-1$.

6. Here, for $0 \le j \le t-1$, $|\eta_{\nu_j}| > |\eta_{\mu_j}| \ge 1 > |\eta_{\mu_t}|$, so $|\xi_{\mu_j}| < |\xi_{\mu_t}| \le |\Delta(\mathfrak{f})|^{1/2}$. If $q^n \ge \max\{1, |\Delta(\mathfrak{f})|^{1/2}\} \ge \max\{1, |\xi_{\mu_j}/\eta_{\mu_j}| : 0 \le j \le t-1\}$, then $|\eta_{\mu_j}| = |\hat{\eta}_{\mu_j}|$ for $0 \le j \le t-1$. Also, $|\xi_{\mu_t}/\eta_{\mu_t}| = q^{m_t}|\xi_{\mu_t}/\eta_{\nu_t}| \le q^{m_t}|\Delta(\mathfrak{f})|^{1/2}$, so if $q^m \ge \max\{1, q^{m_t}|\Delta(\mathfrak{f})|^{1/2}\}$, then $|\eta_{\mu_t}| = |\hat{\eta}_{\mu_t}|$.

   Now for $0 \le j \le t-1$, $|\eta_{\nu_j}/\eta_{\mu_j}| \le q^m$, $|\xi_{\nu_j}/\eta_{\mu_j}| \le |\xi_{\mu_j}| < |\Delta(\mathfrak{f})|^{1/2}$, and $|\xi_{\mu_j}\eta_{\nu_j}/\eta^2_{\mu_j}| \le |\Delta(\mathfrak{f})|^{1/2}$.

7. If $q^n \ge \max\{1, |\Delta(\mathfrak{f})|^{1/2}\} \ge \{|\eta_\mu|, |\xi_\mu|\}$, then $\lfloor \zeta_\mu \rfloor = \lfloor \hat{\zeta}_\mu \rfloor$. If $q^n \ge \max\{q^{m_t}, |\Delta(\mathfrak{f})|^{1/2}\}$ $\ge \max\{|\eta_\nu|, |\xi_\nu|\}$, then $\lfloor \zeta_\nu \rfloor = \lfloor \hat{\zeta}_\nu \rfloor$.

   Now $|\xi_\nu/\eta_\nu| < |\xi_\mu| \le |\Delta(\mathfrak{f})|^{1/2}$, so if $q^n \ge \max\{1, |\Delta(\mathfrak{f})|^{1/2}\}$, then $|\eta_\nu| = |\hat{\eta}_\nu|$, and $|\xi_\nu| = |\eta_\nu|$ if and only if $|\hat{\xi}_\nu| = |\eta_\nu|$. Finally, if $q^n \ge \max\{q^{m_t}, |\Delta(\mathfrak{f})|^{1/2}\} \ge \max\{|\eta_\nu|, |\xi_\nu|\}$, then $|\eta_\nu| = 1$ if and only if $|\hat{\eta}_\nu| = 1$.

□

**Corollary 7.4** *Let $\mathfrak{f}$ be the input ideal and $\{1, \mu, \nu\}$ the input basis of Algorithm 4.1 or Algorithm 6.3. Define $\{\alpha, \beta\} = \{\gamma, \delta\} = \{\mu, \nu\}$ such that $|\xi_\alpha| \ge |\xi_\beta|$ and $|\eta_\gamma| \ge |\eta_\delta|$. Let $l$, $l_r$, $l_{s-1}$, $m$, and $m_t$ be as in Lemma 7.3.*

1. *If* $q^n \ge \max\left\{|\xi_\beta|, \left|\frac{\xi_\alpha}{\xi_\beta}\right|, \left|\frac{\eta_\gamma}{\xi_\beta}\right|, \left|\frac{\xi_\alpha}{\eta_\gamma}\right|, \left|\frac{\xi_\alpha\eta_\delta}{\xi_\beta^2}\right|, \frac{|\xi_\beta|^2}{|\Delta(\mathfrak{f})|^{1/2}}, \frac{|\xi_\beta\eta_\delta|}{|\Delta(\mathfrak{f})|^{1/2}}, \frac{q^{l_r-2}|\eta_\delta|^2}{|\Delta(\mathfrak{f})|^{1/2}}, \frac{q^{2l_{s-1}-2}}{\Delta(\mathfrak{f})|^{1/2}},\right.$ $\left. q^l, q^m, q^{m_t}, q^{m_t}|\Delta(\mathfrak{f})|^{1/2}, \right\}$, *then a precision of $n$ is sufficient for Algorithm 4.1.*
2. *If* $q^n \ge \max\left\{\left|\frac{\xi_\alpha}{\xi_\beta}\right|, \left|\frac{\eta_\gamma}{\xi_\beta}\right|, \left|\frac{\xi_\alpha}{\eta_\gamma}\right|, \left|\frac{\xi_\alpha\eta_\delta}{\xi_\beta^2}\right|, \frac{|\xi_\beta|^2}{|\Delta(\mathfrak{f})|^{1/2}}, q^m, q^{m_t}|\Delta(\mathfrak{f})|^{1/2}\right\}$, *then a precision of $n$ is sufficient for Algorithm 6.3.*

We point out that the values $q^l$, $q^{l_r}$, $q^{l_{s-1}}$, $q^m$, and $q^{m_t}$ are almost always very small. In general, we expect the case where $\mathfrak{f}$ is the product of two reduced ideals to require the highest precision, since in this case, $|N(\mathfrak{f})|^{-1}$ (and hence the upper bound on $|d(\mathfrak{f})|$ by part 2 of Proposition 3.1) is largest. Even in this situation, it is very likely that the required precision is not too large, say no more than $\deg(\Delta)$; however, only numerical experiments will tell. The scenario of Algorithm 6.3 requires significantly less precision: here, we expect $\deg(\Delta)/2$ to be sufficient, and this bound is supported by numerical evidence (see [2]).

# 8 Conclusion and Outlook

We have provided a complete analysis of the algorithm for computing a reduced basis of a fractional ideal in a purely cubic function field of unit rank 1. The number of iterations of each while loop of the algorithm is bounded by a fraction of $\deg(\Delta)$. The quantities $|\xi_\mu|$, $|\xi_\nu|$, $|\eta_\mu|$, and $|\eta_\nu|$ appear not to grow too large throughout our computations; in fact, we expect the bounds of Lemma 5.2 to significantly exceed the actual sizes of these quantities. Finally, the precision required to compute absolute values and quotients appears to be a fraction of $\deg(\Delta)$ as well.

As mentioned in section 1, our two algorithms serve two purposes. If Algorithm 6.3 is repeatedly applied, starting and terminating with $\mathfrak{f} = \mathcal{O}$, it generates all the reduced principal fractional ideals in $\mathcal{O}$ and thus produces the fundamental unit and/or the regulator of $K/k(x)$ as illustrated in [2]. Algorithm 4.1 can be used to determine from a given nonreduced fractional ideal an equivalent reduced one. In particular, if the input ideal is the product of two reduced principal ideals, then the infrastructure of the set of reduced fractional principal ideals guarantees that the method finds a reduced principal fractional ideal "close" to the product ideal very quickly, namely after at most $3(\deg(\Delta) + 4)/8$ applications of Algorithm 4.1. This phenomenon allows for a rapid movement through this set, thereby speeding up regulator and fundamental unit computation significantly. The technique can be extended to yield the ideal class number of $K/k(x)$ and hence the order of the group of $k$-rational points on the Jacobian of $K$. Work on this problem is currently in progress.

If $q \equiv -1 \pmod 3$, then a representation of unit rank 1 can always be achieved for any purely cubic extension $K/k(x)$ by applying a simple change of variable; in particular, any purely cubic extension of unit rank 0 (i.e. when $\deg(D)$ is not a multiple of 3) can always be converted to one of unit rank 1 over the same field of rational functions $k(x)$. The methods outlined above can also undoubtedly be generalized to arbitrary cubic function fields of unit rank 1; once again, this is currently being explored. In addition, we are in the process of investigating the case of even characteristic. It remains to be seen which elements of Algorithms 4.1 and 6.3 (if any) are of use in cubic extensions of unit rank 2, and to what extent our techniques can be extended to unit rank 1 extensions of degree higher than 3. Much of the reduction theory remains valid here, but Algorithm 4.1 needs to be replaced by an entirely different reduction procedure.

## References

[1] R. Scheidler, *Ideal Arithmetic and Infrastructure in Purely Cubic Function Fields.* To appear in *J. Th. Nombr. Bordeaux.*

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

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

[4] G. F. Voronoi, *On a Generalization of the Algorithm of Continued Fractions* (in Russian). Doctoral Dissertation, University of Warsaw (Poland) 1896.