Reduced Ideals in Function Fields

Nigel P. Smart
Extended Enterprise Laboratory
HP Laboratories Bristol
HPL-98-201
December, 1998

function fields,
divisor class group,
reduced ideals,
cryptography

Let F denote a function field of transcendence degree one over a finite field k. We assume that the field is tamely ramified at infinity, that the valuations at infinity of a set of fundamental units are known and we have $\gcd(f_1, \ldots, f_s) = 1$, where f_i denotes the degree of a place at infinity. In such a situation we describe a simple arithmetic in the divisor class group. One draw back of this arithmetic is that we do not obtain a unique representative for each divisor class. The method makes use of multiplication and reduction of reduced fractional ideals.

REDUCED IDEALS IN FUNCTION FIELDS

N.P. SMART

ABSTRACT. Let F denote a function field of transcendence degree one over a finite field k. We assume that the field is tamely ramified at infinity, that the valuations at infinity of a set of fundamental units are known and we have $\gcd(f_1, \ldots, f_s) = 1$, where f_i denotes the degree of a place at infinity. In such a situation we describe a simple arithmetic in the divisor class group. One draw back of this arithmetic is that we do not obtain a unique representative for each divisor class. The method makes use of multiplication and reduction of reduced fractional ideals.

In this paper we present a notion of reduced ideals for function fields of arbitrary degree, thus generalizing the work of Buchmann, Scheidler, Stein, Thiel and Williams, see [6], [26], [27] and [30]. We show how the notion of reduced ideals can be used to define an efficient arithmetic in the divisor class group of certain function fields. We assume throughout that the functions fields are defined over a finite field of constants. The ability to efficiently compute in the divisor class group of a curve is required in generalizations of discrete logarithm based cryptosystems, coding theory based on algebraic geometric curves, primality testing and is of independent theoretical interest in its own right.

The paper is organized as follows: In section 1 we present the arithmetic of function fields, this is given in enough detail so that the whole paper is mostly self contained. Following this in section 2 we shall cover the basic ideas from the 'geometry of numbers' in the Puiseux expansion fields which we shall require. Much of these first two sections can be found in [29] and [25]. However we differ slightly in some of the notation and this all needs to be fixed for the following sections. Indeed there is some disagreement in the literature about certain definitions, so it is worth while spending some time fixing notation.

In section 3 we present the basics on reduced ideals in function fields that we will require. In section 4 we explain the reduction algorithm, analyze its complexity and give an example of how an ideal is reduced. In section 5 we show how to use this to perform efficient arithmetic in the divisor class group of certain function fields. Finally in section 6 we outline how some of the ideas in this paper can be used to solve other problems in function fields.

Before we begin we comment on some historical notes. The lattice reduction algorithm we shall use is essentially the method of [25], which is itself closely related to the method of [16] and [21]. We shall give a complexity estimate for the number of bit operations of the lattice reduction procedure for lattices in a vector space of Puiseux expansions generated by an ideal of a function field.

1991 *Mathematics Subject Classification.* Primary: 11G20, 14Q05. Secondary: 11Y16, 14H05.
Key words and phrases. function fields, divisor class group, reduced ideals, cryptography.

Lattice reduction techniques have been used before to define discrete logarithm based cryptographic schemes using the group law on the Jacobian of superelliptic curves [14]. Whilst ideal reduction techniques form the basis of the classical methods for defining group laws in the divisor class group of imaginary quadratic function fields, see [8]. A similar approach can be taken in real quadratic function fields, see [22] and [23].

An algorithmic group law can be given in the divisor class group of a function field using the standard *compose* and *reduce* method of imaginary quadratic function fields once one has an effective algorithm for the Riemann-Roch problem, such as that given in [9]. Other techniques to solve this problem, such as [31], also use Puiseux expansions, or more generally Hamburger-Noether expansions. However such techniques do not appear very practical and they often require taking extensions of the base field.

A link between the geometry of numbers in function fields and the Riemann-Roch theorem has been noticed before, see [5]. We shall focus on practical algorithmic questions and want a method which is as efficient and simple to implement as possible.

Our approach is algebraic in flavour rather than geometric, hence it is modeled on the number field situation, rather than the geometry. The following problem then arises: We are unable to mirror the exact treatment of reduced ideals in number fields and hence have found it impossible to present a notion of compact representation. Such a representation, if it exists, would possibly allow us to show that many problems in function fields belong to the complexity class $\mathcal{NP}$, see [30] and [26].

The author would like to thank useful useful email correspondences between S. Galbraith, S. Paulus, R. Scheidler and A. Stein which helped with the writing of part of this paper.

1. Function Field Arithmetic

Let $q = p^r$, for a prime number p and let $k = \mathbb{F}_q$. We let $C(x, y) \in k[x, y]$ denote some irreducible multinomial such that

- $\deg_y f = n$.
- f is monic and separable in y.

We let d denote the degree of C, so if

$$C(x, y) = y^n + \sum_{i=0}^{n-1} a_i(x) y^i, \tag{1}$$

with $a_i(x) \in k[x]$, then

$$d = \max_{i=0,\ldots,n} \{i + \deg a_i(x)\},$$

where $a_n(x) = 1$. The genus g of C is related to d via,

$$g \leq \frac{1}{2}(d-1)(d-2).$$

We set $F = k[x, y]/(C(x, y))$ and interpret F as a finite extension of the field $k[x]$. We define the exact constant field $\tilde{k}$ to be

$$\tilde{k} = \{f \in F : f \text{ is algebraic over } k\}.$$

For a field K (which you should think of as either $k[x]$ or F) we define

$$\begin{aligned}\mathbb{P}(K) &= \text{Set of all places of } K.\\ \mathrm{Div}(K) &= \text{Set of all divisors of } K\\ &= \left\{ \sum_{p\in\mathbb{P}(K)} c_p p : c_p \in \mathbb{Z} \text{ and } c_p = 0 \text{ for all but finitely many } p. \right\}.\end{aligned}$$

We write $\mathbb{P}(K) = \mathbb{P}_f(K) \cup \mathbb{P}_\infty(K)$ with an obvious notation. The degree of $\tilde{k}$ will be a number l which divides n, in fact l will divide the degree of all places in $\mathbb{P}(K)$. Suppose $p \in \mathbb{P}(k[x])$ then we define the following valuations on $k[x]$, which can easily be extended to $k(x)$:

$$v_p(\cdot) : \left\{ \begin{array}{ccc} k[x] & \longrightarrow & \mathbb{Z}\cup\{\infty\} \\ \alpha & \longmapsto & \left\{ \begin{array}{ll} \infty & \text{If } \alpha = 0 \\ -\deg(\alpha) & \text{If } p = \infty. \\ k & \text{If } p = p(x) \text{ and } p(x)^k || \alpha. \end{array} \right. \end{array} \right.$$

Each valuation gives rise to an absolute value, which also extends to $k(x)$:

$$|\cdot|_p : \left\{ \begin{array}{ccc} k[x] & \longrightarrow & \mathbb{R}^{\geq 0} \\ \alpha & \longmapsto & q^{-\deg(p)v_p(\alpha)} \end{array} \right.$$

where $q^{-\infty} = 0$ and $\deg(\infty) = 1$. Note that we have, for $\alpha \in k(x)$,

$$\sum_{p\in\mathbb{P}_f(k[x])} \deg(p) v_p(\alpha) = \deg \alpha = -\deg(\infty) v_\infty(\alpha)$$

and so we obtain the product formula

$$\prod_{p\in\mathbb{P}(k[x])} |\alpha|_p = 1,$$

for all $\alpha \in k(x)$.

We write, for $p \in \mathbb{P}(k[x])$, $\mathcal{O}_p = \{\alpha \in k(x) : v_p(\alpha) \geq 0\}$ and define $\mathcal{O}_F$ to be the integral closure of $k[x]$ in F. A basis for $\mathcal{O}_F$ can be computed using an analogue of the *ROUND-2* algorithm from number fields [10].

We now need to extend the valuations and absolute values defined above on $k[x]$ to $\mathcal{O}_F$ (and hence to F). Firstly we consider $\mathfrak{p} \in \mathbb{P}_f(F)$ which lies above a prime $p \in \mathbb{P}_f(k[x])$. The ideal $\mathfrak{p}$ will have ramification index $e_\mathfrak{p}$ and residue degree $f_\mathfrak{p}$. Such a $\mathfrak{p}$ corresponds to an irreducible factor of degree $n_\mathfrak{p} = e_\mathfrak{p} f_\mathfrak{p}$ of $C(x,y)$ when considered as an element of $\mathcal{O}_p[y]$. Call this factor $C_\mathfrak{p}(x,y)$ and define $K_p = k(x)_p$ and $F_p = K_p[y]/(C_\mathfrak{p}(x,y))$. We then define, for $\alpha \in F$,

$$v_\mathfrak{p}(\alpha) = v_p\left(N_{F_p/K_p}(\alpha)\right)/f_\mathfrak{p}$$

and

$$|\alpha|_\mathfrak{p} = q^{-f_\mathfrak{p}\deg(p)v_\mathfrak{p}(\alpha)}.$$

Note that if $p\mathcal{O}_F = {\mathfrak{p}_1}^{e_1}\ldots{\mathfrak{p}_r}^{e_r}$ then $v_{\mathfrak{p}_i}(p) = v_p\left(p^{e_{\mathfrak{p}_i}f_{\mathfrak{p}_i}}\right)/f_{\mathfrak{p}_i} = e_{\mathfrak{p}_i}$. Also note that if $\alpha \in F$ we have

$$\begin{aligned}\sum_{\mathfrak{p}\in\mathbb{P}_f(F)} \deg(p) f_\mathfrak{p} v_\mathfrak{p}(\alpha) &= \sum_{p\in\mathbb{P}_f(k[x])} \deg(p) v_p\left(N_{F/k(x)}(\alpha)\right)\\ &= \deg\left(N_{F/k(x)}(\alpha)\right). \qquad (2)\end{aligned}$$

where in the first sum p is the element of $\mathbb{P}_f(k[x])$ which lies below the element $\mathfrak{p} \in \mathbb{P}_f(F)$.

We now consider the analogous concepts for $\mathfrak{p} \in \mathbb{P}_\infty(F)$. These places will be particularly important to the discussions which follow so we will go over this case in some detail. Readers who are familiar with Puiseux expansions at infinity should skip to the next section.

We define k by

$$k = \min_{i=0,\dots,n-1} \{\lfloor (\deg a_i(x))/(i-n) \rfloor : a_i(x) \neq 0\},$$

where the $a_i(x)$ are as in equation (1), and then write

$$C_\infty(x,y) = y^n + \sum_{i=0}^{n-1} a_i(x) x^{k(n-i)} y^i \in \mathcal{O}_\infty[y].$$

The splitting of this polynomial over $k(1/x, y)$ gives the required splitting of the place ∞ in F.

As a simple example which follows from Dedekind theory we have the following: Set $z = x^{-1}$ and $f(z,y) = C(1/z, y) \in k[z,y]$. We then compute the factorization

$$f(0,y) = \prod_{i=1}^{s} g_i^{t_i} \text{ with } g_i \in k[y]$$

of $f(0,y)$ into irreducibles and set

$$f^* = \left[\frac{1}{z} \left(f(z,y) - \prod_{i=1}^{s} g_i^{t_i} \right) \right]_{z=0}.$$

If

$$\gcd\left(f^*, \prod_{v_i > 1} g_i \right) = 1$$

then $k[x,y]/(C(x,y))$ is already ∞-maximal and the primes at infinity of F can be read off from the factorization of $f(0,y)$. In particular we have s places at infinity $\infty_1, \dots, \infty_s$ with ramification indices $e_{\infty_i} = t_i$ and residue degrees $f_{\infty_i} = \deg g_i$. As an exercise for the reader one can show that for the elliptic curve $y^2 = x^3 + 1$ there is one ramified place at infinity, whilst for the genus one curve $y^2 = x^4 + 1$ there are two unramified places at infinity.

We now return to the general case and write

$$\infty = \prod_{i=1}^{s} \infty_i^{e_i},$$

with ∞_i having residue degree f_i. We impose an order on the places of F at infinity so that for $1 \leq i < j \leq s$ we have $e_i \leq e_j$ and if $e_i = e_j$ we have $f_i \leq f_j$. The signature of the field $F/k[x]$ is then defined to be the ordered tuple

$$(e_1, f_1; e_2, f_2; \dots; e_s, f_s).$$

We put $n_i = e_i f_i$ and $e = \operatorname{lcm}(e_1, \dots, e_s)$. The units of $\mathcal{O}_F$ are denoted $\mathcal{O}_F^*$ and by an analogue of Dirichlet's Units Theorem these have rank $s - 1$.

We shall assume that the place ∞ of $k[x]$ is tamely ramified in F. In other words the characteristic, p, of k does not divide e. In this situation we obtain n Puiseux expansions at infinity:

$$(\rho_1, \ldots, \rho_n) = (\rho_{1,1}, \ldots, \rho_{1,n_1}; \rho_{2,1}, \ldots, \rho_{2,n_2}; \ldots; \rho_{s,1}, \ldots, \rho_{s,n_s}),$$

with

$$\rho_{i,j} \in k_d\langle x^{1/e_i}\rangle = \left\{ \sum_{j=-\infty}^{m} a_j x^{j/e_i} : m \in \mathbb{Z},\ a_j \in k_d \text{ and } a_m \neq 0 \right\}$$

and $k_d = \mathbb{F}_{q^d}$ for some positive integer d. Such Puiseux expansions can be computed using the method of Newton-Puiseux, see for example [15, Section 7.2]. A word of warning here on notation is probably in order, some authors use negative powers for the above expansions. This should cause no problems to the reader who is aware of it, but it means that some authors introduce various minus signs (or delete them) in some of the formulae below.

If $\alpha \in F$ we obtain n-images of α in $k_d\langle x^{1/e}\rangle$ via

$$\alpha^{(i)} = \alpha(x, \rho_i).$$

Since ρ_i 'is' a root of $C(x, y)$ we obtain

$$N_{F/k[x]}(\alpha) = \prod_{i=1}^{s} \alpha^{(i)} \text{ and } Tr_{F/k[x]}(\alpha) = \sum_{i=1}^{s} \alpha^{(i)}.$$

We set $\deg(\alpha^{(i,j)}) = m_{i,j}/e_i$ with an obvious notation. For fixed i the value of $m_{i,j}$ is constant so we can write m_i/e_i with no ambiguity. We then define $|\alpha^{(i)}| = q^{m_i/e_i}$ and define for ∞_i the valuation and absolute value

$$\begin{aligned} v_{\infty_i}(\alpha) &= -\sum_{i=1}^{n_i} m_i/(e_i f_i) = -m_i, \\ |\alpha|_{\infty_i} &= \prod_{i=1}^{n_i} q^{m_i/e_i} = q^{m_i f_i} = q^{-v_{\infty_i}(\alpha) f_i}. \end{aligned}$$

We then note that

$$\deg\left(N_{F/k[x]}(\alpha)\right) = \sum_{i=1}^{s}\sum_{j=1}^{n_i} \deg \alpha^{(i,j)} = \sum_{i=1}^{s} m_i f_i = -\sum_{i=1}^{s} f_i v_{\infty_i}(\alpha).$$

Then, combining this with equation (2), we obtain the product formula

$$\prod_{\mathfrak{p} \in \mathbb{P}(F)} |\alpha|_{\mathfrak{p}} = 1.$$

It is perhaps worth noting at this point that, unlike the number field situation, there is a large degree of choice as to the possible behaviour at infinity. One can always take another defining equation for the function field, which could give rise to a different splitting behaviour at infinity. One should of course choose the defining equation to make the resulting computations as simple as possible. At present there seems no systematic way of doing this.

2. Geometry of Numbers of Laurent Series

In this section we review the details needed from the 'geometry of numbers' in fields of Laurent series. This was work originally conducted by Mahler, [18], and has found recent applications in determining reduced integral bases of function fields, [25].

Let $L = k_d\langle x^{1/e}\rangle$ to be the field of Puiseux expansions considered above. Setting $z = x^{1/e}$, we can consider L to be the field of Laurent series in z, i.e. $k_d((z))$. Using the n Puiseux expansions at infinity of our curve $C(x,y)$ we obtain an embedding of F into L^n,

$$\ell : \left\{ \begin{array}{ccc} F & \longrightarrow & L^n \\ \alpha & \longmapsto & (\alpha^{(1)}, \ldots, \alpha^{(n)})^t \end{array} \right.$$

The map ℓ is analogous to the n embeddings of a number field of degree n into the complex numbers. As before for an element $\alpha \in k_d((z))$ of the form $\sum_{i=-\infty}^{m} a_i z^i$ we define $|\alpha| = q^{m/e}$.

A function $G : L^n \to \mathbb{R}^{\geq 0}$ is called a length function on L^n if for all $\lambda \in L$ and $\alpha, \beta \in L^n$ we have

- $G(\alpha) = 0$ if and only if $\alpha = 0$.
- $G(\lambda\alpha) = |\lambda| G(\alpha)$.
- $G(\alpha \pm \beta) \leq \max(G(\alpha), G(\beta))$.

Such functions are called special distance functions by Mahler, but we shall not be concerned with non-special distance functions. We assume that $G(\alpha)$ for $\alpha \neq 0$ is always an integral power of $q^{1/e}$. The convex body $C(G)$ is defined to be

$$C(G) = \{\alpha \in L^n : G(\alpha) \leq 1\}.$$

Just as in the case of the standard geometry of number we can define the volume of $C(G)$, which we denote by $V(G)$. In the case where

$$G(x_1, \ldots, x_n) = G_\infty(x_1, \ldots, x_n) = \max(|x_1|, \ldots, |x_n|)$$

we have $V(G) = 1$ and $G(1, \ldots, 1) = 1$.

Let R denote a subring of $k_d[z]$ and $B \in GL_n(L)$ then we define the R-lattice in L^n generated by the columns of B to be the set

$$\Lambda = \Lambda(B, R) = \{B\alpha : \alpha \in R^n\}.$$

If $\Lambda(B,R)$ is an R-lattice and G is a length function on L^n we can define the successive minima of Λ as

$$\begin{array}{rcl} M_i & = & M_i(\Lambda, R, G) \\ & = & \min \left\{ \begin{array}{ll} \lambda \in \mathbb{R} : & \exists R - \text{linearly independent } a_1, \ldots, a_i \in \Lambda \text{ such} \\ & \text{that } G(a_j) \leq \lambda \text{ for } 1 \leq j \leq i \end{array} \right\}. \end{array}$$

The lattice determinant of Λ we denote by $\Delta = \det(B)$.

The main theorem we will require on successive minima is the following

Theorem 1 (Mahler, [18]). *Let $R = k_d[z]$, $B \in GL_n(L)$ and G a length function on L^n. Then there exists a $T \in GL_n(R)$ such that $|\det(T)| = 1$ and if we set $(b_1, \ldots, b_n) = BT$, i.e. b_i are some new basis vectors of the lattice $\Lambda(B,R)$, then*

$$M_i(\Lambda, R, G) = G(b_i)$$

and

$$\prod_{i=1}^{n} M_i = |\Delta|/V(G) \text{ and } M_1 \leq (|\Delta|/V(G))^{1/n}.$$

3. Reduced Ideals in Function Fields

We assume an integral basis $\omega_1, \ldots, \omega_n$ of $\mathcal{O}_F$ has been computed. The discriminant of $\mathcal{O}_F$ is then defined to be

$$D_F = \left(\det(\omega_i^{(j)})_{1\leq i,j\leq r}\right)^2.$$

The discriminant of the curve C is defined to be

$$D_C = \left(\det(y^{(j)\,i})_{1\leq i,j\leq r}\right)^2,$$

so D_F divides D_C and since $C(x,y)$ has degree d we have

$$\deg D_F < \deg D_C \leq d(d-1).$$

A fractional $\mathcal{O}_F$-ideal (hereafter just called an ideal), A, of $\mathcal{O}_F$ can be presented as a pair $A = (d(A), \mathrm{Hnf}(A))$ where $d(A) \in k[x]$ is the 'denominator' and $\mathrm{Hnf}(A) \in M_{n\times n}(k[x])$ is a matrix in Hermite Normal Form. The basis of the ideal, as a $k[x]$-module, is then given by

$$\frac{1}{d(A)}(\omega_1, \ldots, \omega_n)\mathrm{Hnf}(A).$$

The norm of the ideal is equal to

$$N(A) = [\mathcal{O}_F : d(A)A]/d(A)^n = det(\mathrm{Hnf}(A))/d(A)^n.$$

If we look at the image in L^n of the ideal A then it forms a lattice of determinant $N(A)D_F^{1/2}$.

Using algorithms similar to those in number fields, see [10], one can add, multiply and divide ideals of $\mathcal{O}_F$. The only problem comes with the reduction theory of ideals. In number fields the concept of reduced ideal uses the concept of ideal minima. Many of the ideas in the number field setting can be found in [30].

In function fields similar ideas have been used before in very special cases, see [26], [27] and [28]. Indeed the reduction theory of ideals for elliptic function fields gives rise to the standard group law on elliptic curves. In [14] a similar approach is taken for the case of super-elliptic function fields. However the approach taken below is slightly different from that in [14].

For $\alpha \in F$ let $\underline{\alpha}$ denote its image in L^n under the map ℓ. Let G_∞ denote the length function on L^n given earlier by

$$G_\infty(\alpha) = \max_{1\leq i\leq n} |\alpha^{(i)}|.$$

As noted earlier we have $V(G_\infty) = 1$ and $G_\infty(\underline{1}) = 1$. An element μ of the $\mathcal{O}_F$-ideal A will be called a minimum of A if there does not exist a non-zero $\alpha \in A$ with

$$G_\infty(\underline{\alpha}) < G_\infty(\underline{\mu}).$$

If 1 is a minimum of A then the ideal is said to be reduced. This is a different notion of minimum than is usually used in number fields, however it appears more suited to the function field situation due the theorem of Mahler above, we shall return to this point at the end of this section.

Proposition 2. *Let A denote an ideal with minimum μ. Then $B = (1/\mu)A$ is a reduced ideal equivalent to A.*

Proof. Clearly $1 \in B$ and B is equivalent to A. We shall assume that B is not reduced, hence there exists a non-zero $\beta \in B$ with $\max|\beta^{(i)}| < 1$. Let $\alpha = \mu\beta \in A$, then we have

$$\max|\alpha^{(i)}| \leq \max|\mu^{(i)}| \cdot \max|\beta^{(i)}| < \max|\mu^{(i)}|.$$

Now since $\alpha \neq 0$, we see that μ could not have been a minimum of A. Which is the desired contradiction. □

The ideal $\mathcal{O}_F$ is clearly reduced as it contains the element 1 and if it was not reduced then it would contain an element α such that $\max|\alpha^{(i)}| < 1$. But if this was true then $|N_{F/k[x]}(\alpha)| < 1$, which would imply that α was equal to zero, since $\alpha \in \mathcal{O}_F$. Hence $\mathcal{O}_F$ is reduced.

We now show that minima of ideals cannot be too large.

Lemma 3. *If μ is a minimum of the ideal A then*

$$|N(\mu)| \leq G_\infty(\underline{\mu})^n \leq |N(A)||D_F|^{1/2}.$$

Proof. Note that the lattice determinant of the image of A under ℓ is $N(A)D_F^{1/2}$. Suppose μ is a minimum of the ideal A and

$$G_\infty(\underline{\mu})^n > |N(A)||D_F|^{1/2}$$

then, by Mahler's convex body theorem, Theorem 1, there is an element $\alpha \in A$ with

$$G_\infty(\underline{\alpha}) < G_\infty(\underline{\mu})$$

which contradicts the minimality of μ. The result follows on noticing that

$$|N(\mu)| = \prod_{i=1}^{n} |\mu^{(i)}| \leq G_\infty(\underline{\mu})^n.$$

□

Using this lemma we can show that reduced ideals have upper and lower bounds on their norms:

Lemma 4. *If A is a reduced ideal then*

$$|D_F|^{-1/2} \leq |N(A)| \leq 1.$$

Proof. For all ideals A and $\alpha \in A$ we have $|N(\alpha)| \geq |N(A)|$. Then, since 1 is a minimum of A, we have $1 \in A$ and so

$$1 = |N(1)| \geq |N(A)|.$$

But by Lemma 3 we have

$$|D_F|^{-1/2} = G_\infty(\underline{1})^n |D_F|^{-1/2} \leq |N(A)|.$$

□

Lemma 5. *Let A denote a reduced ideal, given by $A = (d(A), \mathrm{Hnf}(A))$ and $\mathrm{Hnf}(A) = (a_{i,j})$ then*

$$0 \leq |a_{i,j}| \leq |d(A)| \leq |D_F|^{1/2}.$$

Proof. Since A is reduced we have $\mathcal{O}_F \subset A$ and $[A : \mathcal{O}_F]A \subset \mathcal{O}_F$. Hence

$$|d(A)| \leq |[A : \mathcal{O}_F]| \leq 1/N(A) \leq |D_F|^{1/2}.$$

Since $d(A)\omega_i \in d(A)A$, as A is reduced, we then notice that $a_{i,i}$ divides $d(A)$. The result follows since $|a_{i,j}| \leq |a_{i,i}|$ as $(a_{i,j})$ is in Hermite Normal Form. □

We can hence bound the number of bits needed to represent a reduced ideal.

Corollary 1. *If A is a reduced ideal then we can represent A using*

$$O\left(n^2 \left(\log_q |D_F|\right) \log q\right) = O(d^4 \log q).$$

bits.

Proof. The degree of $d(A)$ and the $a_{i,j}$ needed to represent A is bounded by $m = \frac{1}{2}\log_q |D_F|$. So we need to give at most $O(n^2)$ polynomials of degree at most m. Clearly each polynomial requires $O(m \log_2 q)$ bits. Now since $n \leq d$ and $\log_q |D_F| = \deg D_F \leq d(d-1)$ the result follows. □

We now return to discussing the difference between our notion of minima of ideals and the 'standard' notion in number fields. In number fields an element μ in an ideal A is called a minimum (we shall call it an NF-minimum to avoid confusion) if there does not exist a non-zero element $\alpha \in A$ with

$$|\alpha^{(i)}| < |\mu^{(i)}|.$$

Lemma 6. *An ideal minimum, in our sense, is an NF-minimum.*

Proof. Let A denote an ideal with minimum α and suppose that α is not an NF-minimum. Then there exists a $\beta \in A$ such that

$$|\beta^{(i)}| < |\alpha^{(i)}|$$

for all i. Hence $\max|\beta^{(i)}| < \max|\alpha^{(i)}|$ and so α could not have been a minimum of A. This contradiction proves our assertion. □

If the function field, F, has one place at infinity then the two notions of minima are clearly equivalent, and hence the two associated notions of reduced ideals are also equivalent. However for general function fields, where there is more than one place at infinity, the two notions can be different. Hence in this paper we are using a different notion of minima and reduced ideals than that used in the case of pure cubic function fields in [27]. The notion of NF-minima seems to be required to find compact representations, but it is unclear how to find such minima in the general function field context using lattice basis reduction. The advantage of our notion of minima is that it allows us to find minima and reduced ideals quite painlessly using lattice basis reduction techniques, as we shall now show.

4. The Ideal Reduction Algorithm

In this section we give the algorithm for ideal reduction, based on the lattice reduction techniques of [16], [21] and [25]. We let $A = (d(A), \mathrm{Hnf}(A))$ denote a fractional ideal of $\mathcal{O}_F$. We let $a_1, \ldots, a_n$ denote an $\mathbb{F}_q[x]$ basis of A and $\underline{a_1}, \ldots, \underline{a_n}$ the basis of the associated lattice in L^n, where $L = k_d\langle x^{1/e}\rangle$.

We need to define the following functions on L^n:

$$V : \begin{cases} L^n & \longrightarrow & \mathbb{Z} \cup \{\infty\} \\ \alpha & \longmapsto & \begin{cases} e \max\{\deg(\alpha^{(i)})\} & \alpha \neq 0 \\ -\infty & \alpha = 0 \end{cases} \end{cases}$$

and

$$\theta_k : \begin{cases} L^n & \longrightarrow & k_d^n \\ \left(\sum_{j=-\infty}^{m} a_{i,j} x^{j/e}\right)_{1 \leq i \leq n} & \longmapsto & (a_{i,k})_{1 \leq i \leq n} \end{cases}$$

The orthogonality defect of the basis of A is defined to be

$$OD(a_1, \ldots, a_n) = \frac{1}{e} \sum_{j=1}^{n} V(\underline{a_i}) - \deg(\det(\underline{a_1}, \ldots, \underline{a_n})).$$

Lemma 7. *For any basis $a_1, \ldots, a_n$ of A we have that $eOD(a_1, \ldots, a_n) \in \mathbb{Z}_{\geq 0}$ and $OD(a_1, \ldots, a_n) = 0$ if and only if the vectors $\underline{a_1}, \ldots, \underline{a_n}$ are the successive minima of the lattice in L^n given by $\ell(A)$.*

Proof. Clearly $eOD(a_1, \ldots, a_n) \in \mathbb{Z}$. Now since

$$\det(\underline{a_1}, \ldots, \underline{a_n}) = \sum_{\sigma \in S_n} \epsilon(\sigma) \underline{a_1}^{(\sigma(1))} \ldots \underline{a_n}^{(\sigma(n))}$$

we obtain

$$\begin{aligned} \deg(\det(\underline{a_1}, \ldots, \underline{a_n})) &\leq \max_{\sigma \in S_n} \left\{ \sum_{j=1}^{n} \deg(\underline{a_j}^{(\sigma(j))}) \right\} \\ &\leq \sum_{j=1}^{n} \max_{1 \leq i \leq n} \{\deg(\underline{a_j}^{(i)})\} = \frac{1}{e} \sum_{j=1}^{n} V(\underline{a_j}). \end{aligned}$$

Hence $OD(a_1, \ldots, a_n) \geq 0$.

The orthogonality defect, $OD(a_1, \ldots, a_n)$, will achieve its minimal value when the vectors $\underline{a_1}, \ldots, \underline{a_n}$ correspond to the successive minima of the lattice, since $\log_q G_\infty(\underline{\alpha}) = V(\underline{\alpha})/e$. It follows that the minimal value of the orthogonality defect will be zero for the successive minima as,

$$\prod_{i=1}^{n} M_i = |\Delta| = |\det(\underline{a_1}, \ldots, \underline{a_n})|$$

□

We can now give our reduction algorithm: On input of a basis $a_1, \ldots, a_n$ for A the following algorithm outputs a reduced basis $b_1, \ldots, b_n$ such that b_1 is a minimum of A.

Reduction Algorithm for the ideal A

1. Set $b_i = a_i$ for all i.
2. Repeat
3. Reorder $b_1, \ldots, b_n$ such that $V(\underline{b_i}) \leq V(\underline{b_{i+1}})$ for all i.
4. Set $b = 0$.
5. For $c = 0, \ldots, e-1$ do
6. Compute $k = \#\left\{i \in \{1, \ldots, n\} : V(\underline{b_i}) \equiv c \pmod{e}\right\}$ and $i_1 < i_2 < \ldots < i_k$ such that $V(\underline{b_{i_j}}) \equiv c \pmod{e}$.
7. Compute $S = \{\theta_{V(\underline{b_{i_m}})}(\underline{b_{i_m}}) : 1 \leq m \leq k\}$.
8. If $k > 1$ and S is $\mathbb{F}_q$-linearly dependent
9. Since S is $\mathbb{F}_q$-linearly dependent we can find $j \in \{1, \ldots, k-1\}$ and $(\alpha_1, \ldots, \alpha_j, 0, \ldots, 0) \in \mathbb{F}_q^k$ with $\alpha_j = 1$ and $\sum_{m=0}^{j} \alpha_m \theta_{V(\underline{b_{i_m}})}(\underline{b_{i_m}}) = 0$.
10. Set $t_m = V(\underline{b_{i_j}}) - V(\underline{b_{i_m}}) \geq 0$ for $0 \leq m < j$.
11. Replace b_{i_j} by $b_{i_j} + \sum_{m=0}^{j-1} \alpha_m x^{t_m/e} b_{i_m} \in A$.
12. Set $b = 1$.
13. Until $b = 0$.

Lemma 8. *The above algorithm is correct and terminates.*

Proof. Clearly, since $t_m \equiv 0 \pmod{e}$, the output of the above algorithm is another basis of A. On passing through the main repeat loop one of two conditions can be satisfied either $b = 0$ or $b = 1$ and the value of $OD(b_1, \ldots, b_n)$ has been decreased by at least $1/e$. Hence after at most $eOD(b_1, \ldots, b_n)$ loops the algorithm must terminate. If is also clear that if $b = 0$ at the end of the main loop then the value of $V(\underline{b_i})$ for all i cannot be decreased any more. Hence $OD(b_1, \ldots, b_n)$ has achieved its minimal value. But we know that a basis of successive minima exists, by Mahler's convex body theorem, so $OD(b_1, \ldots, b_n) = 0$ on termination. □

We shall now estimate the complexity of the above algorithm. Clearly we can assume for this purpose that the ideal A is integral i.e. $d(A) = 1$. We write $\mathrm{Hnf}(A) = (a_{i,j})$ and set $h = \deg N(A)$. Clearly we have $0 \leq \deg a_{i,j} \leq h$. Let $\mathcal{V}$ denote

$$\mathcal{V} = \max_{i=1}^{n} V(\underline{a_i}),$$

and notice that throughout the algorithm, for all i, we have $V(\underline{b_i}) \leq \mathcal{V}$. For the integral basis $\omega_1, \ldots, \omega_n$ of $\mathcal{O}_F$ let W denote the value of $\max\{\deg \omega_i^{(j)}\}$.

By Mahler's theorem we know that we can choose an integral basis ω_i such that

$$1 = G(\omega_1) \leq G(\omega_2) \leq \ldots \leq G(\omega_n) = q^W$$

and

$$\prod_{i=1}^{n} G(\omega_i) = |\Delta_F|^{1/2}.$$

Hence $W \leq \frac{1}{2} \log_q |\Delta_F| = m \leq d(d-1)/2$. From now on we assume such a reduced integral basis has been computed, using for instance the method in [25].

We have

$$\begin{aligned}\mathcal{V} &\leq \max_{1\leq i,j\leq n}\left\{\deg\left(\sum_{k=1}^{n} a_{k,i}\omega_k^{(j)}\right)\right\}\\ &\leq \max\{\deg a_{k,i}\} + W \leq h+m.\end{aligned}$$

Firstly we need to estimate the accuracy of the Puiseux expansions which will need to be taken. Clearly this is bound up with the size of the first successive minima, since a first successive minima will correspond to the vector of Puiseux expansions which is closest to zero.

Lemma 9. *Let A denote an integral ideal of F and let $\alpha \in A$ be chosen such that $\underline{\alpha}$ is the first successive minima of the image of A under ℓ. Then if $G_\infty(\underline{\alpha}) = q^{s/e}$, i.e. $V(\underline{\alpha}) = s$, then*

$$s \geq \frac{eh}{n}.$$

Proof. Let

$$\alpha^{(i)} = \sum_{j=-\infty}^{s_i} a_{i,j}x^{j/e}.$$

We then have, $s = \max\{s_i\}$, and so

$$\begin{aligned}s &\geq \frac{1}{n}\sum_{i=1}^{n} s_i = \frac{e}{n}\sum_{i=1}^{n}\deg(\alpha^{(i)}) = \frac{e}{n}\deg(N_{F/k(x)}(\alpha))\\ &\geq \frac{e}{n}\deg N(A) = \frac{eh}{n}.\end{aligned}$$

□

Theorem 10. *Let A denote an integral ideal of F, then to determine a reduced basis of A we require*

$$O(en^2(h+m))$$

evaluations of Puiseux expansions and

$$O(n^3(h+m)^3)$$

operations in k.

Proof. Let $\underline{\alpha}$, as above, denote the first successive minimum of the lattice $\ell(A)$. In the above algorithm we have, by the previous lemma,

$$t_m = V(\underline{b_{i_j}}) - V(\underline{b_{i_m}}) \leq V(\underline{b_{i_j}}) - V(\underline{\alpha}) \leq \mathcal{V} - \frac{eh}{n} \leq \mathcal{V} \leq h+m.$$

Notice that we also have

$$OD(a_1,\ldots,a_n) \leq \frac{n}{e}\mathcal{V}.$$

As we have noticed before the main repeat loop is executed at most $eOD(a_1,\ldots,a_n)$ times, which means it is executed at most $n\mathcal{V} \leq n(h+m)$ times.

Let D denote the maximum of the degrees of the polynomials defining the basis as we pass through the algorithm. These degrees increase by at most $t_m/e \leq (h+m)/e$ on each replacement of b_{i_j} by a new value. A maximum of $n\mathcal{V}e \leq n(h+m)e$ such replacements are carried out. Hence $D \leq h + n(h+m)^2$.

Each loop requires $O(en)$ evaluations of Puiseux expansions. The total number of operations in k needed to detect a single linear dependency is $O(n^2)$ and the

number of operations in k needed to calculate a new value of b_{i_j} is $O(nD)$, which is less than $O(n(h+n(h+m)^2)) = O(n^2(h+m)^2)$.

Hence the total algorithm requires $O(en^2(h+m))$ evaluations of Puiseux expansions and $O(n^3(h+m)^3$ operations in k. □

We now give the complexity of our method for multiplying and reducing two reduced ideals.

Theorem 11. *Let A and B denote two reduced ideals. Then a reduced ideal C equivalent to $A \times B$ can be computed in $O(d^{10})$ operations in k.*

Proof. First note that $e \leq n \leq d$ and $\log_q |D_F| \leq d(d-1)$.

By Lemma 5 the polynomials needed to define A and B are bounded in degree by $m = \frac{1}{2}\log_q |D_F|$. We first compute $D = A \times B$ by the usual Hermite Normal Form technique. If we set $D = (d(D), \mathrm{Hnf}(D))$ then $d(D)$ is of degree $2m$ and is computed in $O(m^2)$ operations.

To compute $\mathrm{Hnf}(D)$ we first compute the product $\alpha_i\beta_j$ where α_i is a basis element of A and β_j is a basis element of B. This requires $O(n^2)$ multiplications in F and so requires $O(n^4m^2)$ operations in $\mathbb{F}_q$.

The Hermite Normal Form of the resulting $n \times n^2$ matrix can be computed in $O(n^3m^2)$ operations in $\mathbb{F}_q$. The resulting matrix $\mathrm{Hnf}(D) = (d_{i,j})$ is in Hermite normal form and consists of polynomials of degree at most $2m$.

To find the reduced ideal equivalent to D we reduce the integral ideal given by $(1, \mathrm{Hnf}(D))$. Applying Theorem 10 we see, since we have $h \leq 2m$, that this requires

$$O(en^2(h+m)) = O(d^5)$$

evaluations of Puiseux series and

$$O(n^3(h+m)^3) = O(d^9)$$

operations in k.

But each Puiseux expansion need only be computed to order $O(x^0)$. So we need to compute at most $\mathcal{V}$ terms of each Puiseux expansion, with $\mathcal{V}$ defined as above. But, also as above, we have $\mathcal{V} \leq h+m \leq 3m = O(d^2)$. To compute each Puiseux expansion we compute

$$\sum_{i=1}^{n} d_{i,j}(\rho^{(k)})^{i-1}.$$

Since $\deg d_{i,j} \leq 2m = O(d^2)$, this takes $O(d^5)$ operations in k. So evaluating all the Puiseux expansions takes $O(d^{10})$ operations in k.

The final division step needed to compute the reduced ideal and the associated Hermite Normal Form computation to put the reduced ideal into the standard form have negligible complexity in comparison to the rest of the computation. □

Example. We end this section by giving an example of how an ideal is reduced: Let $k = \mathbb{F}_3$ and let F be given by the curve

$$C(x,y) : y^3 + (2x^3 + x + 1)y^2 + (2x+1)y + 2 = 0.$$

The function field F has genus 3 and and the three Puiseux expansions of y at infinity are given by

$$\begin{aligned}
\rho^{(1)} &= z^6 + 2z^2 + 2 + z^{-4} + 2z^{-6} + z^{-8} + z^{-12} + z^{-16} + O(z^{-18}),\\
\rho^{(2)} &= w^6 z^{-3} + z^{-4} + w^6 z^{-5} + 2z^{-6} + w^6 z^{-7} + z^{-8} + w^6 z^{-9} + O(z^{-12}),\\
\rho^{(3)} &= w^2 z^{-3} + z^{-4} + w^2 z^{-5} + 2z^{-6} + w^2 z^{-7} + z^{-8} + w^2 z^{-9} + O(z^{-12}).
\end{aligned}$$

where $w^2 + w + 2 = 0$ and $z = x^{1/2}$. Consider the $\mathcal{O}_F$-ideal, I, of norm $x^3 + 1$, generated over $k[x]$ by the elements

$$\alpha_1 = x^3 + 1,\ \alpha_2 = 2 + y,\ \alpha_3 = 2 + y^2.$$

The initial values of the function V for these elements is $V(\alpha_1) = 6$, $V(\alpha_2) = 6$ and $V(\alpha_3) = 12$, and the orthogonality defect is $OD(\alpha_1, \alpha_2, \alpha_3) = 4.5$. We shall show that this ideal is principal by reducing it to the trivial ideal. If we apply our method for ideal reduction we perform the following transformation of these basis elements: First set $\beta_1 = \alpha_1$, $\beta_2 = \alpha_2$ and then

$$\beta_3 = \alpha_3 - (x^3 + 2x - 1)\alpha_2 - \alpha_1.$$

The value of $V(\beta_3)$ is 3, and no smaller element can be found in the ideal, since we have $OD(\beta_1, \beta_2, \beta_3) = 0$. Hence β_3 is a minimum of the ideal and is given by

$$\beta_3 = 2x + (2x^3 + x + 1)y + y^2.$$

So a reduced ideal equivalent to I is given by $A = (1/\beta_3)I$. We have

$$\begin{aligned}
\left(\frac{\beta_1}{\beta_3}\right) &= 2 + (x^3 + 2x + 1)y + 2y^2,\\
\left(\frac{\beta_2}{\beta_3}\right) &= 2y.
\end{aligned}$$

So we have the following matrix representation of the reduced ideal,

$$A = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 2 & x^3 + 2x + 1 \\ 0 & 0 & 2 \end{pmatrix}.$$

Putting this into Hermite Normal Form we see that it is equal to the identity matrix. Hence the initial ideal was principal and generated by β_3.

5. The divisor class group

We assume that the curve is such that there is at least one point, P_0, on $C(x, y)$ which is defined over k. By Hasse's theorem if k is large enough there will always be such a point. In addition the existence of P_0 will imply that F will contain a place of degree one and so $\tilde{k} = k$.

Following the proof of Lemma 1 and Theorem 2 of [14] we can prove.

Theorem 12. *Let C be a non-singular curve over k of genus g with a given k-rational point P_0. Let $D \in \mathrm{Div}_k^0(C)$. Then there is a unique effective divisor E over k of minimal degree $m \leq g$ such that $E - \infty P_0$ is equivalent to D.*

We let $\mathrm{Pic}_k^0(C)$ denote the group $\mathrm{Div}_k^0(C)$ modulo principal divisors. In the next few paragraphs we shall give a method to compute in the divisor class group of curves, however we shall lose the property of having a unique representative for

divisor classes. However the representatives we shall use will be 'reduced' in the sense that a bounded number of bits are needed to represent such divisor classes.

We shall make use of the following result, also from [14]

Theorem 13. *Let C be a curve and let $S = \{\infty_1, \ldots, \infty_s\}$ denote the set of places of F lying above the place at infinity of $k[x]$. Let Cl denote the ideal class group of $\mathcal{O}_F$ and* Ker *denote the subgroup of* $\mathrm{Pic}_k^0(C)$ *generated by all degree zero divisors with support in S. If $f = \gcd(f_1, \ldots, f_s) = 1$ then we have the following exact sequence:*

$$1 \to \mathrm{Ker} \to \mathrm{Pic}_k^0(C) \to Cl \to 1.$$

Proof. We define the map

$$\begin{array}{ccc} \mathrm{Pic}_k^0(C) & \longrightarrow & Cl, \\ \sum_{\mathfrak{p}} n_{\mathfrak{p}} \mathfrak{p} & \longmapsto & \prod_{\mathfrak{p} \not\in S} \mathfrak{p}^{n_{\mathfrak{p}}}. \end{array}$$

where we have associated the prime divisor $\mathfrak{p}$ with the prime ideal $\mathfrak{p}$ in a natural way. This map is a surjective group homomorphism if $f = 1$ and has kernel equal to Ker. □

In the special case which was considered in [14] the group Ker was trivial and so $\mathrm{Pic}_k^0(C)$ was isomorphic to the class group. In addition the notion of reduction in the class group used in [14] produced a unique representative. Hence the group law in [14] was from a set of unique reduced divisors to a set of unique reduced divisors.

For the rest of this paper we shall assume that $f = \gcd(f_1, \ldots, f_s) = 1$. If we let h denote the order of Cl and R denote the order of Ker in the lemma above, we have

$$\#\mathrm{Pic}_k^0(C) = hR = H.$$

The number R is sometimes called the regulator of $\mathcal{O}_F$. The numbers h and H are the ideal and divisor class numbers respectively.

As noted earlier we have that $\mathcal{O}_F^*$ is a group of rank $r = s-1$. A set of generators of $\mathcal{O}_F^*$ is called a set of fundamental units. We let $\epsilon_1, \ldots, \epsilon_r$ denote such a set of fundamental units of $\mathcal{O}_F^*$. If we consider the matrix

$$\mathcal{R} = \begin{pmatrix} f_1 v_{\infty_1}(\epsilon_1) & \ldots & f_1 v_{\infty_1}(\epsilon_r) \\ \vdots & & \vdots \\ f_r v_{\infty_r}(\epsilon_1) & \ldots & f_r v_{\infty_r}(\epsilon_r) \end{pmatrix},$$

the absolute value of the determinant of $\mathcal{R}$ is denoted $\mathcal{R}\mathrm{eg}$. There are $r+1$ different matrices of the form $\mathcal{R}$, depending on the ordering of the v_i we have chosen. However, the value of $\mathcal{R}\mathrm{eg}$ does not depend on the choice of which valuations we take in constructing the matrix $\mathcal{R}$ nor does it depend on the choice of fundamental units we have made.

The number $\mathcal{R}\mathrm{eg}$ is also sometimes called the regulator of $\mathcal{O}_F$. This is very confusing since in general $R \neq \mathcal{R}\mathrm{eg}$, luckily they are related by the following lemma:

Lemma 14. *With the notation above we have*

$$\mathcal{R}\mathrm{eg} = R \prod_{i=1}^{r+1} f_i.$$

Proof. We have

$$\mathrm{div}(\epsilon_j) = \sum_{i=1}^{r+1} v_{\infty_i}(\epsilon_j)\infty_i,$$

but since ϵ_j has degree zero we also have

$$\sum_{i=1}^{r+1} f_i v_{\infty_i}(\epsilon_j) = 0.$$

Putting these last two equations together we obtain

$$f_{r+1}\mathrm{div}(\epsilon_j) = \sum_{i=1}^{r} v_{\infty_i}(\epsilon_j)\left(f_{r+1}\infty_i - f_i\infty_{r+1}\right).$$

Now let $\alpha = \sum_{i=1}^{r+1} a_i\infty_i \in \mathrm{Ker}$, since α also has degree zero we have

$$f_{r+1}a_{r+1} = -\sum_{i=1}^{r} f_i a_i.$$

Hence we can write

$$f_{r+1}\alpha = \sum_{i=1}^{r} a_i\left(f_{r+1}\infty_i - f_i\infty_{r+1}\right).$$

So the order of Ker, which we have denoted by R, is given by

$$R = |\det((v_{\infty_i}(\epsilon_j))_{1\le i,j\le r})|/f_{r+1}.$$

But clearly, from the definition of $\mathcal{R}\mathrm{eg}$, we have

$$\mathcal{R}\mathrm{eg} = |\det((v_{\infty_i}(\epsilon_j))_{1\le i,j\le r})|\prod_{i=1}^{r} f_i.$$

So the result follows. □

We assume that a set of fundamental units for $\mathcal{O}_F^*$ have been computed and so we can compute a unique set of coset representatives for the group Ker. We fix such a unique set of coset representatives and, by abuse of notation, also refer to this set as Ker. In fact all we actually require is the computation of the valuations at infinity of a set of fundamental units. This is often easier to compute than an actual set of fundamental units. This is because, without a compact representation of elements, a fundamental unit may not be representable in a polynomial amount of time or space.

We can now present our method for computing in the divisor class group of F. We represent each element of $\mathrm{Pic}_k^0(C)$ as a pair, (k, I), where $k \in \mathrm{Ker}$ and I is a reduced ideal of $\mathcal{O}_F$. We first note that such a representation may not be unique since there may not be a unique reduced ideal in a given ideal class. To write such an element down requires $O(d^4 \log q)$ bits for the reduced ideal I and $(\log R)^s$ bits for k.

To add two such pairs, (k_1, I_1) and (k_2, I_2) we first compute $J = I_1 \times I_2$, which can be computed using the standard Hermite Normal Form style techniques. Using the reduction algorithm we then determine a minimum, α, of J. Then we compute the ideal $I_3 = J/(\alpha)$, which will be reduced.

Finally we construct the element

$$k = (v_{\infty_1}(\alpha), \ldots, v_{\infty_r}(\alpha)) \in \mathbb{Z}^r,$$

and then compute

$$k_3 = (k_1 + k_2 - k) \in \text{Ker}.$$

This reduction of $k_1 + k_2 - k$ to an element in Ker is accomplished using the known valuations of the fundamental units. The reduction is performed by computing the nearest lattice point to $k_1 + k_2 - k$, for the lattice generated by the valuations of the fundamental units. The nearest lattice point can be found either using the Fincke-Pohst algorithm, [12], or heuristically using LLL, [17]. Hence we have

$$(k_1, I_1) + (k_2, I_2) = (k_3, I_3).$$

6. Applications

6.1. **Cryptography.** Using the above efficient addition law one can implement all the standard cryptographic protocols based on a discrete logarithm problem. These all require a unique representative of elements in the underlying group. One can use the above addition law to perform efficiently the group exponentiation and then use the slower Riemann-Roch techniques at the end to produce the final result.

This is rather like using projective representation in elliptic curve systems. There are many representations in projective coordinates of a given elliptic curve point, but addition is easier in projective coordinates. One only returns to affine (and hence unique) coordinates at the end of the computation.

6.2. **Group Structure and Discrete Logarithm Computation.** Using the notion of ideal reduction one can trivially generalize the method of Hafner-McCurley, see [13] and [20], to the divisor class group of the curves in this paper. One can then find the group structure of the divisor class group and solve discrete logarithms in such groups.

Alternatively using the methods for computing valuations at infinity we can generalize the NFS type method, which is explained in [1], [2] and [14], to find the group structure. Combining this technique with the ideal reduction method one can solve discrete logarithms as in [14].

To make these methods work we require a factor base of 'small' primes which generate the ideal class group. The results of [14] and [19] show us that for the Hafner-McCurley type method we can take all places of norm less than q^d where d is given by

$$\frac{2\log(4g-2)}{\log q},$$

while for the NFS type method we take all places of residue degree one and norm less than q^d where d is the smallest prime number greater than

$$\max\left\{n, \frac{2\log(4g-2)}{\log q}\right\}.$$

We note that in polynomial time one can compute the order of the divisor class group, using one of the generalizations of Schoof's algorithm, see [4] and [24].

6.3. **Unit Group Computation.** Using the group structure algorithm one can compute the unit group of $\mathcal{O}_F$ and a set of fundamental units of $\mathcal{O}_F$. This can be done in the usual way. However a major problem remains of actually writing down the units, since no compact representation of elements of general function fields is currently available. However we note that for the method of addition in the divisor

class group presented in this paper we only require the valuations at infinity of a set of fundamental units. This can be computed and presented in a compact way.

References

[1] L. Adleman. The function field sieve. In [3], 108–121.

[2] L. Adleman, J. De Marrais, and M.-D. Huang. A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields. In [3], 28–40.

[3] L.M. Adleman and M-D. Huang, editors. *ANTS-1 : Algorithmic Number Theory.* Springer-Verlag, LNCS 877, 1994.

[4] L. Adleman and M.-D. Huang. Counting rational points on curves and abelian varieties over finite fields. In [11], 1–16.

[5] J.V. Armitage. Algebraic functions and an analogue of the Geometry of Numbers: The Riemann-Roch Theorem. *Arch. Math.*, **18**, 383–93, 1967.

[6] J. Buchmann, C. Thiel and H.C. Williams. Short representation of quadratic integers. In *Computational Algebra and Number Theory*, A. van der Poorten and W. Bosma, editors, Mathematics and its Applications, **325**, Dordrecht/Boston/London, 159–186, 1995.

[7] J. Buhler, editor. *ANTS-3 : Algorithmic Number Theory.* Springer-Verlag, LNCS 1423, 1998.

[8] D.G. Cantor. Computing in the Jacobian of a hyperelliptic curve. *Math. Comp.*, **48**, 95–101, 1987.

[9] J. Coates. Construction of rational functions on a curve. *Proc. Cam. Phil. Soc.*, **68**, 105–123, 1970.

[10] H. Cohen. *A Course In Computational Algebraic Number Theory.* Springer-Verlag, GTM 138, 1993.

[11] H. Cohen, editor. *ANTS-2 : Algorithmic Number Theory.* Springer-Verlag, LNCS 1122, 1996.

[12] U. Fincke and M. Pohst. Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. *Math. Comp.*, **44**, 463–471, 1985.

[13] R. Flassenberg and S. Paulus. Sieving in function fields. *Preprint*, 1997.

[14] S.D. Galbraith, S. Paulus and N.P. Smart. Arithmetic on super-elliptic curves. Preprint, 1998.

[15] F. Kirwan. *Complex Algebraic Curves.* LMS Student Texts 23, Cambridge University Press, 1992.

[16] A.K. Lenstra. Factoring multivariate polynomials over finite fields. *J. of Computer and System Sciences*, **30**, 235–248, 1985.

[17] A.K. Lenstra, H.W. Lenstra, and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, **261**, 515–534, 1982.

[18] K. Mahler. An analogue to Minkowski's geometry of numbers in a field of series. *Annals of Math.*, **42**, 488–522, 1941.

[19] V. Müller, A. Stein and C. Thiel. Computing discrete logarithms in real quadratic function fields of large genus. Preprint 1997.

[20] S. Paulus. An algorithm of sub-exponential type computing the class group of quadratic orders over principal ideal domains. In [11], 243–257.

[21] S. Paulus. Lattice basis reduction in function fields. In [7], 567–575.

[22] S. Paulus and H.-G. Rück. Real and imaginary quadratic representations of hyperelliptic function fields. *To appear in Math. Comp.*

[23] S. Paulus and A. Stein. Comparing real and imaginary arithmetics for divisor class groups of hyperelliptic curves. In [7], 576–591.

[24] J. Pila. Frobenius maps of abelian varieties and finding roots of unity in finite fields. *Math. Comp.*, **55**, 745–763, 1996.

[25] M. Pohst and M. Schörnig. On integral basis reduction in global function fields. In [11], 273–283.

[26] R. Scheidler. Compact representation in real quadratic congruence function fields. In [11], 323–336.

[27] R. Scheidler and A. Stein. Unit computation in purely cubic function fields of unit rank 1. In [7], 592–606.

[28] R. Scheidler, A. Stein and H.C. Williams. Key-exchange in real quadratic congruence function fields. *Designs, Codes and Cryptography* **7**, 153–174, 1996.

[29] M. Schörnig Untersuchungen konstruktiver Probleme in globalen Funktionenkörpen. Phd Thesis, Technischen Universität Berlin, 1996.
[30] C. Thiel. Under the assumption of the Generalized Riemann Hypothesis verifying the class number belongs to $\mathcal{NP} \cap$ co–$\mathcal{NP}$. In [3], 234–247.
[31] E. J. Volcheck. Computing in the Jacobian of a plane algebraic curve. In [3], 221–233.

Hewlett-Packard Laboratories,Filton Road, Stoke Gifford,Bristol, BS12 6QZ, U.K.
E-mail address: nsma@hplb.hpl.hp.com