

# Algorithmic Aspects of Cubic Function Fields

R. Scheidler\*

Department of Mathematics & Statistics  
University of Calgary  
2500 University Drive N.W.  
Calgary, Alberta T2N 1N4, Canada  
rscheidl@math.ucalgary.ca

**Abstract.** This paper presents an investigative account of arbitrary cubic function fields. We present an elementary classification of the signature of a cubic extension of a rational function field of finite characteristic at least five; the signature can be determined solely from the coefficients of the defining curve. We go on to study such extensions from an algorithmic perspective, presenting efficient arithmetic of reduced ideals in the maximal order as well as algorithms for computing the fundamental unit(s) and the regulator of the extension.

## 1 Introduction

The arithmetic of algebraic curves over finite fields is a subject of considerable interest, due to its mathematical importance as well as its applications to cryptography. Since general-purpose methods tend to be computationally inefficient, the discussion of fast algorithms has so far predominantly focused on elliptic and hyperelliptic curves. In addition, the arithmetic of purely cubic curves  $y^3 = D(x)$  has been investigated in considerable detail [12, 10, 11, 2]; Picard curves represent a special case thereof. Several other particular classes of curves have also been studied from an algorithmic point of view, such as superelliptic curves (curves of the form  $y^n = D(x)$ ) [5] and  $C_{ab}$  curves [1].

In this paper, we investigate arbitrary cubic extensions of a rational function field of finite characteristic. We give a simple technique for finding the signature (and thus the unit rank) of a cubic extension when the characteristic is at least five; the signature can be determined solely from the coefficients of the defining curve. We also investigate efficient arithmetic of reduced fractional ideals in the maximal order of the field and show how to use this arithmetic to find the fundamental unit(s) and the regulator of the extension. Our method is based on a procedure that was originally developed by Voronoi for cubic number fields [14] and was recently adapted to purely cubic function fields [12, 6].

## 2 Cubic Function Fields and Curves

Let  $k = \mathbb{F}_q$  be a finite field of characteristic not equal to 3, and denote by  $\bar{k}$  its algebraic closure. Consider an absolutely irreducible nonsingular affine plane

---

\* Research supported by NSERC of Canada.

curve  $\mathcal{C}_0$  defined by an equation  $H(x, y) = 0$  where  $H \in k[x][Y]$  is a bivariate polynomial of degree 3 in  $Y$  which is irreducible over  $\bar{k}(x)$ ; write  $H(x, Y) = SY^3 + UY^2 + VY + W$  with  $S, U, V, W \in k[x]$ ,  $SW \neq 0$ . Then the function field  $K$  of  $\mathcal{C}_0$  over  $k$  is a cubic extension of the rational function field  $k(x)$  with minimal polynomial  $H(x, Y)$ ; that is,  $K = k(x, y)$ .

It is easy to verify that under the transformation  $(x, y) \rightarrow (x, S^{-1}(y - U/3))$ ,  $\mathcal{C}_0$  is birationally equivalent to the curve  $\mathcal{C}_1 : y^3 - Ay + B = 0$  where

$$A = \frac{U^2}{3} - SV, \quad B = S^2W - \frac{SUV}{3} + \frac{2U^3}{27}.$$

Furthermore, the singular points on  $\mathcal{C}_1$  are exactly the points  $(a, U(a)/3) \in \bar{k}^2$  where  $S(a) = 0$ . If  $Q^2$  divides  $A$  and  $Q^3$  divides  $B$  for some  $Q \in k[x]$ , then all points of the form  $(a, 0)$  with  $Q(a) = 0$  are singular, and  $\mathcal{C}_1$  is birationally equivalent to the curve  $y^3 - (A/Q^2)y + (B/Q^3) = 0$ . For brevity, we call a (possibly singular) curve  $\mathcal{C}$  a *standard model* for  $K/k(x)$  if  $\mathcal{C}$  is of the form  $y^3 - Ay + B = 0$  with  $A, B \in k[x]$ ,  $B \neq 0$ , and for no  $Q \in k[x]$  does  $Q^2$  divide  $A$  and  $Q^3$  divide  $B$ . We also say that such a curve, and its function field, are in *standard form*. Clearly, every absolutely irreducible nonsingular affine plane curve over  $k$  of degree 3 in  $y$  is birationally equivalent to a standard model.

A standard model is *purely cubic* if  $A = 0$ . Note that if  $q \equiv 1 \pmod{3}$  — this can always be accomplished by adjoining a primitive cube root of unity to  $k$  if necessary — then by Kummer theory, a cubic extension  $K/k(x)$  has a purely cubic model if and only if it is a Galois extension (see Lemma 2.1 of [6]). If  $q \equiv -1 \pmod{3}$ , it is not clear which cubic extensions over the field  $\mathbb{F}_q(x)$  have purely cubic representations.

For a curve  $y^3 - Ay + B = 0$  in standard form with function field  $K$ , the polynomial  $f = f(Y) = Y^3 - AY + B \in k[x][Y]$  is the minimal polynomial of  $K/k(x)$ . It has three distinct roots  $y_0 = y, y_1 = y', y_2 = y''$  in an algebraic extension of  $k(x)$  of degree at most 6. For any  $\alpha = a + by + cy^2 \in K$  with  $a, b, c \in k(x)$ , denote by  $\alpha' = a + by' + c(y')^2$  and  $\alpha'' = a + by'' + c(y'')^2$  the *conjugates* of  $\alpha$ . The *norm* of  $\alpha$  is  $N(\alpha) = \alpha\alpha'\alpha'' \in k(x)$  and the *trace* of  $\alpha$  is  $Tr(\alpha) = \alpha + \alpha' + \alpha''$ ; both are rational functions (i.e. in  $k(x)$ ). The *discriminant* of  $f$  is the nonzero polynomial  $D = (y - y')^2(y' - y'')^2(y'' - y)^2 = 4A^3 - 27B^2 \in k[x]$ . We recall that if  $k$  has odd characteristic, then  $K/k(x)$  is a Galois extension if and only if  $D$  is a square; in particular, a purely cubic extension is Galois if and only if  $q \equiv 1 \pmod{3}$ .

We have the following simple characterization of singular points:

**Lemma 2.1.** *Let  $\mathcal{C} : y^3 - Ay + B = 0$  be a standard model of a cubic extension  $K/k(x)$  where  $k$  has characteristic at least 5. Set  $D = 4A^3 - 27B^2$ , and let  $a \in \bar{k}$ . Then  $(a, b)$  is a singular point of  $\mathcal{C}$  for some  $b \in \bar{k}$  if and only if  $D(a) = \frac{\partial D}{\partial x}(a) = 0$  and either  $B(a) \neq 0$  or  $B(a) = \frac{\partial B}{\partial x}(a) = 0$ . In the latter case, we have  $b = A(a) = \frac{\partial^2 D}{\partial x^2}(a) = 0$ .*

*Proof.*  $(a, b) \in \bar{k}^2$  is a singular point of  $\mathcal{C}$  if and only if

$$b^3 - A(a)b + B(a) = 0, \tag{2.1}$$

$$3b^2 - A(a) = 0, \quad (2.2)$$

$$\frac{\partial A}{\partial x}(a)b - \frac{\partial B}{\partial x}(a) = 0. \quad (2.3)$$

Suppose (2.1) – (2.3) hold, then  $A(a) = 3b^2$  and  $B(a) = 2b^3$ ,  $D(a) = 0$ , and  $\frac{\partial D}{\partial x}(a) = 54B(a) \left( \frac{\partial A}{\partial x}(a)b - \frac{\partial B}{\partial x}(a) \right) = 0$ . Furthermore, if  $B(a) = 0$ , then  $b = 0$ , so  $A(a) = 0$ . In this case, (2.3) yields  $\frac{\partial B}{\partial x}(a) = 0$ , and hence  $\frac{\partial^2 D}{\partial x^2}(a) = 0$ .

Conversely, suppose that  $D(a) = \frac{\partial D}{\partial x}(a) = 0$  and either  $B(a) \neq 0$  or  $B(a) = \frac{\partial B}{\partial x}(a) = 0$ . Then  $4A(a)^3 = 27B(a)^2$ , so there exists  $b \in \bar{k}$  with  $A(a) = 3b^2$  and  $B(a) = 2b^3$ . It follows that (2.1) and (2.2) hold. Now  $\frac{\partial D}{\partial x}(a) = 0$  implies  $B(a) \left( \frac{\partial A}{\partial x}(a)b - \frac{\partial B}{\partial x}(a) \right) = 0$ , so if  $B(a) \neq 0$ , then (2.3) holds, and if  $B(a) = \frac{\partial B}{\partial x}(a) = 0$ , then  $b = 0$  and (2.3) holds as well; furthermore, in the latter case,  $A(a) = 0$  and  $\frac{\partial^2 D}{\partial x^2}(a) = 0$ .  $\square$

For  $G, P \in k[x]$ , let  $v_P(G)$  denote the maximal power of  $P$  dividing  $G$ . By Lemma 2.1, the curve  $\mathcal{C}$  is nonsingular if and only if  $v_P(D) \geq 2$  implies  $v_P(B) = 1$  for every irreducible divisor  $P \in k[x]$  of  $D$ . This implies the following:

**Corollary 2.2.** *Let  $\mathcal{C} : y^3 - Ay + B = 0$  be a standard model of a cubic extension  $K/k(x)$  where  $k$  has characteristic at least 5. Set  $D = 4A^3 - 27B^2$ . Then  $\mathcal{C}$  is nonsingular if and only if  $\gcd(D, B)$  is squarefree.*

If  $\Delta$  is the discriminant of  $K/k(x)$  (unique up to nonzero constant square factors), then there exist  $I \in k[x]$  (the *index* or *conductor* of  $y$ ) such that  $D = I^2\Delta$ . The curve  $\mathcal{C}$  is nonsingular if and only if  $I \in k^* = k \setminus \{0\}$ , i.e. if and only if  $D$  and  $\Delta$  agree up to a square factor in  $k$ . Using a result due to Llorente and Nart (see Theorem 2 of [8]) that is readily extendable from cubic number fields to their function field analogue, one can easily compute  $\Delta$  and  $I$  from  $D$ :

**Lemma 2.3.** *Let  $\mathcal{C} : y^3 - Ay + B = 0$  be a standard model of a cubic extension  $K/k(x)$  where  $k$  has characteristic different from 3. If  $\Delta$  is the discriminant of  $K/k(x)$  and  $P \in k[x]$  is any irreducible divisor of  $D = 4A^3 - 27B^2$ , then*

- $v_P(\Delta) = 2$  if and only if  $v_P(A) \geq v_P(B) \geq 1$ ;
- $v_P(\Delta) = 1$  if and only if  $v_P(D)$  is odd;
- $v_P(\Delta) = 0$  otherwise, i.e. if and only if  $v_P(D)$  is even and  $v_P(A) = v_P(B) = 0$ .

The characterization of the “otherwise” case stems from the condition  $v_Q(A) \geq 2$  forcing  $v_Q(B) \leq 2$  for all  $Q \in k[x]$ . The same condition implies in the case where  $v_P(\Delta) = 2$  for any  $P \mid D$  that  $1 \leq v_P(B) \leq 2$ . Note also that if  $v_P(D)$  is odd, then either  $v_P(A) = v_P(B) = 0$  or  $1 = v_P(A) < v_P(B)$ .

### 3 Integral Bases

Let  $f(x, y) = 0$  with  $f = f(Y) = Y^3 - AY + B \in k[x, Y]$  be the standard model of an affine plane curve defining a cubic function field  $K = k(x, y)$ . As before, let  $D = 4A^3 - 27B^2 = I^2\Delta$  where  $I \in k[x]$  is the index of  $y$  and  $\Delta$  is the

discriminant of  $K/k(x)$ . The integral closure of  $k[x]$  in  $K$  is the *ring of regular functions* or *maximal order* of  $K/k(x)$  and is denoted by  $\mathcal{O}$ .  $\mathcal{O}$  is a  $k[x]$ -module of rank 3, and any  $k[x]$ -basis of  $\mathcal{O}$  is called an *integral basis* of  $K/k(x)$ .

Every nonzero ideal  $\mathfrak{a}$  in  $\mathcal{O}$  is a  $k[x]$ -submodule of  $\mathcal{O}$  of rank 3; write  $\mathfrak{a} = [\lambda, \phi, \psi]$  where  $\{\lambda, \phi, \psi\}$  is any  $k[x]$ -basis of  $\mathfrak{a}$ . The *norm*  $N(\mathfrak{a})$  is the (finite) group index  $[\mathcal{O} : \mathfrak{a}]$ ; it is a nonzero constant multiple of the determinant of the 3 by 3 transformation matrix with polynomial entries that maps any integral basis to any  $k[x]$ -basis of  $\mathfrak{a}$ . The *discriminant* of  $\mathfrak{a}$  is  $\Delta(\mathfrak{a}) = N(\mathfrak{a})^2 \Delta$ ; it is unique up to nonzero constant factors. We have  $\Delta(\mathcal{O}) = \Delta$ , and since  $D([1, y, y^2]) = D = I^2 \Delta$ , the norm of the ideal  $k[x, y] = [1, y, y^2]$  is a constant multiple of  $I$ .

Our goal is to find an integral basis of  $K/k(x)$  that is suitable for computation. Voronoi (see [4, pp. 108-112]) first proposed how to do this for cubic number fields.

**Lemma 3.1.** *For any integral basis of  $K$  of the form  $\{1, \phi, \psi\}$  where  $\phi = y + S$  and  $\psi = (y^2 + Ty + U)/I$  with  $S, T, U \in k[x]$ , we have  $3T^2 - A \equiv 0 \pmod{I}$  and  $T^3 - AT + B \equiv 0 \pmod{I^2}$ .*

*Proof.* Since  $\phi\psi, \psi^2 \in \mathcal{O}$ , there must exist  $r, s, t, u, v, w \in k[x]$  such that  $\phi\psi = r\psi + s\phi + t$  and  $\psi^2 = u\psi + v\phi + w$ . An easy but tedious calculation reveals that  $s = (T^2 - U - A)/I$ ,  $u = (T^2 + 2U + A)/I$ , and  $v = (AT - T^3 - B)/I^2$ . So  $2s + u = (3T^2 - A)/I \in k[x]$  and  $-v = (T^3 - AT + B)/I^2 \in k[x]$ .  $\square$

It is clear that a basis of the form described in Lemma 3.1 — and hence a polynomial  $T$  with  $3T^2 - A \equiv 0 \pmod{I}$  and  $T^3 - AT + B \equiv 0 \pmod{I^2}$  — always exists.

**Corollary 3.2.** *Let  $T \in k[x]$  with  $3T^2 - A \equiv 0 \pmod{I}$  and  $T^3 - AT + B \equiv 0 \pmod{I^2}$ . Then the set  $\{1, \rho, \omega\}$  with*

$$\rho = y - T, \quad \omega = \frac{1}{I}(y^2 + Ty + T^2 - A)$$

*is an integral basis of  $K/k(x)$  with  $\rho\omega \in k[x]$ .*

*Proof.* Let  $3T^2 - A = EI$  and  $T^3 - AT + B = FI^2$  with  $E, F \in k[x]$ . We have  $\rho^3 + 3T\rho^2 + EI\rho + FI^2 = 0$  and  $\omega^3 - E\omega^2 + 3FIT - F^2I = 0$ , so  $\rho$  and  $\omega$  are integral over  $k[x]$  and hence lie in  $\mathcal{O}$ . Now  $[1, \rho, I\omega] = [1, y, y^2]$ , so  $I^2\Delta([1, \rho, \omega]) = \Delta([1, \rho, I\omega]) = \Delta([1, y, y^2]) = D = I^2\Delta$  and hence  $\Delta([1, \rho, \omega]) = \Delta = \Delta(\mathcal{O})$ . It follows that  $[1, \rho, \omega] = \mathcal{O}$ . Finally,  $\rho\omega = -FI \in k[x]$ .  $\square$

Note that we can always choose  $T$  so that  $\deg(T) < \deg(I)$ , in which case the above basis is polynomially bounded in the size of the coefficients  $A, B$  of the standard model. We call a basis of the type given in Corollary 3.2 such that  $\deg(T) < \deg(I)$  a *canonical* basis of  $K/k(x)$ . The following identities are easily verified and show that canonical bases are indeed very suitable for computation. Here,  $3T^2 - A = EI$  and  $T^3 - AT + B = FI^2$  with  $E, F \in k[x]$ .

$$\begin{aligned} \rho^2 &= I\omega - 3T\rho - EI, & Tr(\rho) &= -3T, & N(\rho) &= -FI^2, \\ \omega^2 &= E\omega - F\rho - 3FT, & Tr(\omega) &= E, & N(\omega) &= F^2I, \\ \rho\omega &= -FI. \end{aligned}$$

Note that when our curve is nonsingular, i.e.  $I \in k^*$ , then we may take  $I = 1$  and  $T = 0$ , in which case  $E = -A$ ,  $F = B$ ,  $\rho = y$ , and  $\omega = y^2 - A$ . If  $K/k(x)$  is purely cubic, then  $A = 0$ , so we may once again take  $T = 0$ . In this case  $E = 0$ , so  $I$  is the square part and  $F$  the squarefree part of  $B$ . Here,  $\rho = y$  and  $\omega = y^2/I$ .

## 4 Signatures

In order to determine the behavior at infinity of a cubic function field extension (which in turn will reveal the signature), we first require some notation and a simple lemma. For any finite field  $\mathbb{F}_q$ , we denote by  $\mathbb{F}_q\langle x^{-1/e} \rangle$  the field of Laurent series in  $x^{-1/e}$  ( $e \in \mathbb{N}$ ); note that  $k\langle x^{-1} \rangle$  is the completion with respect to the infinite place of  $\mathbb{F}_q(x)$ . If  $\alpha = \sum_{i=-\infty}^m a_i x^{i/e}$  is any nonzero element in  $\mathbb{F}_q\langle x^{-1/e} \rangle$  with  $m \in \mathbb{Z}$ ,  $a_i \in \mathbb{F}_q$  for  $i \leq m$ , and  $a_m \neq 0$ , then  $\text{sgn}(\alpha) = a_m$  is the *sign*,  $\deg(\alpha) = m$  the *degree* (in  $x^{-e}$ ), and  $|\alpha| = q^m = q^{\deg(\alpha)}$  the *absolute value* of  $\alpha$ .

The following simple lemma will prove useful.

**Lemma 4.1.** *Let  $q$  be any prime power,  $p$  a prime not dividing  $q$ , and  $\alpha$  a nonzero element in  $\mathbb{F}_q\langle x^{-1} \rangle$ . If  $\deg(\alpha)$  is divisible by  $p$ , then  $\alpha$  has a  $p$ -th root in  $\mathbb{F}_q(\text{sgn}(\alpha)^{1/p})\langle x^{-1} \rangle$ , otherwise  $\alpha$  has a  $p$ -th root in  $\mathbb{F}_q\langle x^{-1/p} \rangle$ , but in no subfield of Laurent series of  $\mathbb{F}_q\langle x^{-1/p} \rangle$ .*

*Proof.* Let  $\beta = \sum_{i=-\infty}^n b_i x^i \in \overline{\mathbb{F}_q}\langle x^{-1} \rangle$ . Then  $\beta^p = \sum_{i=-\infty}^{pn} c_i x^i$  where  $c_{pn} = b_n^p$  and for  $i \in \mathbb{N}$ ,  $c_{pn-i} = pb_n^{p-1}b_{n-i} + f_i$  where  $f_i$  is a homogeneous polynomial of degree  $p$  in  $b_{n-i+1}, b_{n-i+2}, \dots, b_n$  with coefficients in  $\mathbb{F}_q$ . In particular, if  $\beta^p \in \mathbb{F}_q\langle x^{-1} \rangle$ , i.e.  $c_i \in \mathbb{F}_q$  for  $i \leq pn$ , then inductively,  $b_i \in \mathbb{F}_q(b_n)$  for  $i = n, n-1, n-2, \dots$

Now let  $\alpha \in \mathbb{F}_q\langle x^{-1} \rangle$  and write  $\deg(\alpha) = pn + r$  with  $0 \leq r \leq p-1$ . Set  $\gamma = x^{-r}\alpha$ , so  $\gamma \in \mathbb{F}_q\langle x^{-1} \rangle$  with  $\deg(\gamma) = pn$ . Write  $\gamma = \sum_{i=-\infty}^{pn} c_i x^i$ . Let  $b_n$  be any  $p$ -th root of  $c_{pn}$  and recursively define  $b_{n-i} = (c_{pn-i} - f_i)/pb_n^{p-1} \in \mathbb{F}_q(b_n)$  for  $i \in \mathbb{N}$ , where  $f_i$  is the polynomial in  $b_{n-i+1}, b_{n-i+2}, \dots, b_n$  described above. If we set  $\beta = \sum_{i=-\infty}^n b_i x^i$ , then  $\beta \in \mathbb{F}_q(b_n)\langle x^{-1} \rangle$  and  $\beta^p = \gamma$ . Therefore  $\alpha = (x^{r/p}\beta)^p$ . If  $r = 0$ , then  $\alpha$  has a  $p$ -th root in  $\mathbb{F}_q(\text{sgn}(\alpha)^{1/p})\langle x^{-1} \rangle$ , otherwise the smallest field of Laurent series containing a  $p$ -th root of  $\alpha$  is  $L = \mathbb{F}_q(b_n)\langle x^{-1} \rangle(x^{r/p})$ . Since  $r$  is coprime to  $p$ , we have  $L = \mathbb{F}_q\langle x^{-1} \rangle(x^{1/p})$ . Clearly  $L \subseteq \mathbb{F}_q\langle x^{-1/p} \rangle$ , and since both fields are extensions of degree  $p$  of  $\mathbb{F}_q\langle x^{-1} \rangle$ , they must be equal.  $\square$

If  $F$  is any finite algebraic extension of  $\mathbb{F}_q(x)$  of degree  $n$ , then the place at infinity of  $\mathbb{F}_q(x)$  splits in  $F$  as

$$(\infty) = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_s^{e_s}, \quad (4.1)$$

where  $s \in \mathbb{N}$ , and for  $1 \leq i \leq s$ ,  $\mathfrak{p}_i$  is a place of  $F$  of residue degree  $f_i \in \mathbb{N}$  and ramification index  $e_i \in \mathbb{N}$  with  $\sum_{i=1}^s e_i f_i = n$ . Then the completion of  $F$  with respect to the place  $\mathfrak{p}_i$  is  $F_{\mathfrak{p}_i} = \mathbb{F}_{q^{f_i}}\langle x^{-e_i} \rangle$ . If we sort the pairs  $(e_i, f_i)$ ,  $1 \leq i \leq s$ , in lexicographical order, then the  $2s$ -tuple  $(e_1, f_1, e_2, f_2, \dots, e_s, f_s)$  is the *signature* of  $F/\mathbb{F}_q(x)$ .

We are now ready to determine the signature of a cubic extension. Note that transforming such an extension into standard form as described in Section 1 does not affect the signature.

**Theorem 4.2.** *Let  $\mathcal{C} : f(x, y) = 0$  with  $f(Y) = Y^3 - AY + B \in k[x][Y]$  be a standard model of a cubic extension  $K/k(x)$  where  $k = \mathbb{F}_q$  is a finite field of characteristic at least 5. Set  $D = 4A^3 - 27B^2$ . Then  $K/k(x)$  has signature*

- $(1, 1, 1, 1, 1, 1)$  if
  - $|A|^3 > |B|^2$ ,  $\deg(A)$  even, and  $\text{sgn}(A)$  is a square in  $k$ , or
  - $|A|^3 < |B|^2$ ,  $\deg(B) \equiv 0 \pmod{3}$ ,  $\text{sgn}(B)$  is a cube in  $k$ , and  $q \equiv 1 \pmod{3}$ , or
  - $|A|^3 = |B|^2$ ,  $4\text{sgn}(A)^3 \neq 27\text{sgn}(B)^2$ , and the equation  $t^3 - \text{sgn}(A)t + \text{sgn}(B) = 0$  has three roots in  $k$ , or
  - $|A|^3 = |B|^2$ ,  $4\text{sgn}(A)^3 = 27\text{sgn}(B)^2$ ,  $\deg(D)$  is even, and  $\text{sgn}(D)$  is a square in  $k$ ;
- $(1, 1, 1, 2)$  if
  - $|A|^3 > |B|^2$ ,  $\deg(A)$  even, and  $\text{sgn}(A)$  is not a square in  $k$ , or
  - $|A|^3 < |B|^2$ ,  $\deg(B) \equiv 0 \pmod{3}$ ,  $\text{sgn}(B)$  is a cube in  $k$ , and  $q \equiv -1 \pmod{3}$ , or
  - $|A|^3 = |B|^2$ ,  $4\text{sgn}(A)^3 \neq 27\text{sgn}(B)^2$ , and the equation  $t^3 - \text{sgn}(A)t + \text{sgn}(B) = 0$  has one root in  $k$ , or
  - $|A|^3 = |B|^2$ ,  $4\text{sgn}(A)^3 = 27\text{sgn}(B)^2$ ,  $\deg(D)$  is even, and  $\text{sgn}(D)$  is not a square in  $k$ ;
- $(1, 3)$  if
  - $|A|^3 < |B|^2$ ,  $\deg(B) \equiv 0 \pmod{3}$ , and  $\text{sgn}(B)$  is not a cube in  $k$ , or
  - $|A|^3 = |B|^2$ ,  $4\text{sgn}(A)^3 \neq 27\text{sgn}(B)^2$ , and the equation  $t^3 - \text{sgn}(A)t + \text{sgn}(B) = 0$  has no roots in  $k$ ;
- $(1, 1, 2, 1)$  if
  - $|A|^3 > |B|^2$  and  $\deg(A)$  is odd, or
  - $|A|^3 = |B|^2$  and  $\deg(D)$  is odd (so  $4\text{sgn}(A)^3 = 27\text{sgn}(B)^2$ );
- $(3, 1)$  if  $|A|^3 < |B|^2$  and  $\deg(B) \not\equiv 0 \pmod{3}$ .

*Proof.* Let  $l = \max\{\lceil \deg(A)/2 \rceil, \lceil \deg(B)/3 \rceil\}$  and consider the polynomial  $f_\infty(Y) = x^{-3l}f(x, Yx^l) = Y^3 - A(x)x^{-2l}Y + B(x)x^{-3l} \in k[x^{-1}, Y]$ . If

$$f_\infty(Y) = P_1(Y)^{e_1} P_2(Y)^{e_2} \cdots P_s(Y)^{e_s}$$

is the factorization of  $f_\infty(Y)$  into powers of distinct monic irreducible polynomials in  $k\langle x^{-1} \rangle[Y]$ , where  $s \in \mathbb{N}$ ,  $e_1, e_2, \dots, e_s \in \mathbb{Z}^{\geq 0}$ , and  $P_i$  has degree  $f_i$  in  $Y$  for  $1 \leq i \leq s$ , then with the proper ordering,  $(e_1, f_1, e_2, f_2, \dots, e_s, f_s)$  is the signature of  $K/k(x)$ .

Clearly,  $\theta = \theta(x)$  is a root of  $f_\infty(Y) = 0$  if and only if  $\theta x^l$  is a root of  $f(Y) = 0$ . Hence, in order to determine the signature of  $K/k(x)$ , it suffices to find for each zero  $\alpha$  of  $f$  minimal positive integers  $e$  and  $f$  such that  $\alpha \in \mathbb{F}_{q^f} \langle x^{-e} \rangle$ .

If  $k$  has characteristic at least 5, then the the zeros  $\{y, y', y''\} = \{y_0, y_1, y_2\}$  of  $f$  are given by Cardano's formulae

$$y_i = \frac{1}{3}(u^i \delta_+ + u^{-i} \delta_-) \quad (i = 0, 1, 2), \quad (4.2)$$

where  $u$  is a primitive cube root of unity and  $\delta_+ = y_0 + u^2y_1 + uy_2$ ,  $\delta_- = y_0 + uy_1 + u^2y_2$ . Here

$$\delta_+ = \sqrt[3]{-\frac{3}{2}(9B + \sqrt{-3D})}, \quad \delta_- = \sqrt[3]{-\frac{3}{2}(9B - \sqrt{-3D})}, \quad (4.3)$$

where the cube roots are taken so that  $\delta_+\delta_- = 3A$  (note that this leaves three choices for the cube root of  $\delta_+$ , but different choices for this cube root only lead to a different ordering of the roots  $y_0, y_1, y_2$ ).

For brevity, set  $m = \deg(A)$ ,  $n = \deg(B)$ ,  $a = \text{sgn}(a)$ , and  $b = \text{sgn}(B)$ .

*Case  $|A|^3 < |B|^2$ :* By Lemma 4.1,  $\sqrt{-3D} \in k\langle x^{-1} \rangle$ , implying  $\delta_+^3, \delta_-^3 \in k\langle x^{-1} \rangle$  and hence again by Lemma 4.1,  $\delta_+, \delta_- \in k\langle x^{-1/3} \rangle$ . From (4.3),  $|\delta_+| = q^{n/3} > |\delta_-|$ ,  $\text{sgn}(\delta_+) = -3b^{1/3}$  for some cube root  $b^{1/3}$  of  $b$ , and for  $i = 0, 1, 2$ :  $|y_i| = q^{n/3}$  and  $\text{sgn}(y_i) = -u^i b^{1/3}$  from (4.2).

If  $n \not\equiv 0 \pmod{3}$ , then  $y_i \in k\langle x^{-1/3} \rangle \setminus k\langle x^{-1} \rangle$  for  $i = 0, 1, 2$ , so  $K/k(x)$  has signature  $(3, 1)$ , whereas if  $n \equiv 0 \pmod{3}$ , then by Lemma 4.1,  $y_i \in k(b^{1/3}, u)\langle x^{-1} \rangle$  for  $i = 0, 1, 2$ , so any ramification index  $e_i$  in the signature must be 1. In this case, if  $b$  is not a cube in  $k$ , then  $q \equiv 1 \pmod{3}$  (as otherwise, every element in  $k$  is a cube), so  $u \in k$ ,  $[k(b^{1/3}, u) : k] = 3$ , and the signature is  $(1, 3)$ . On the other hand, if  $b$  is a cube in  $k$ , then  $y_0 \in k\langle x^{-1} \rangle$  and  $y_1, y_2 \in k(u)\langle x^{-1} \rangle$ . Hence, if  $q \equiv 1 \pmod{3}$ , or equivalently,  $u \in k$ , then the signature is  $(1, 1, 1, 1, 1, 1)$ , whereas if  $q \equiv -1 \pmod{3}$ , then  $[k(u) : k] = 2$ , and since  $\text{sgn}(y_1), \text{sgn}(y_2) \in k(u) \setminus k$ , the signature must be  $(1, 1, 1, 2)$ .

*Case  $|A|^3 > |B|^2$ :* Here,  $\delta_+^3, \delta_-^3 \in k\langle x^{1/2} \rangle$ ,  $|\delta_+|^3, |\delta_-|^3 = q^{3m/2}$  and  $\text{sgn}(\delta_+^3) = -\text{sgn}(\delta_-^3) = (-3a)^{3/2}$ . By Lemma 4.1,  $\delta_+, \delta_- \in k\langle x^{-1/2} \rangle$ , so  $y_i \in k\langle x^{-1/2} \rangle$  for  $i = 0, 1, 2$ . Choose the cube root of  $\delta_+$  so that  $\text{sgn}(\delta_+) = -\text{sgn}(\delta_-) = (-3a)^{1/2}$ . Then  $|y_1| = |y_2| = q^{m/2} > |y_0|$ .

If  $m$  is odd, then by Lemma 4.1,  $y_1, y_2 \in k\langle x^{-1/2} \rangle \setminus k\langle x^{-1} \rangle$ , so at least one of the ramification indices in the signature is 2, forcing signature  $(1, 1, 2, 1)$ . Suppose now that  $m$  is even, then  $\delta_+, \delta_- \in k((-3a)^{1/2})\langle x^{-1} \rangle$ . Write  $\delta_+ = \beta + \gamma s$  with  $\beta, \gamma \in k\langle x^{-1} \rangle$  and  $s^2 = -3a$ . Since  $\delta_+^3 = \delta_-^3 = (\delta_-)^3$  where the map  $\bar{\phantom{x}} : k(s) \rightarrow k(s)$  takes  $s$  to  $-s$ , we have  $\delta_- = u^j \overline{\delta_+} = u^j(\beta - \gamma s)$  for some  $j \in \{0, 1, 2\}$ . Since  $3A = \delta_+\delta_- = u^j(\beta^2 - 3a\gamma^2)$ , we have  $u^j \in k$ . If  $j = 0$ , then it is simple to deduce  $y_0 \in k\langle x^{-1} \rangle$  and  $y_1, y_2 \in k(a^{1/2})\langle x^{-1} \rangle$ . If  $j \neq 0$ , then we must have  $q \equiv 1 \pmod{3}$ , so  $u \in k$ , and it is once again easy to see that exactly one among  $y_0, y_1, y_2$  is in  $k\langle x^{-1} \rangle$ , while the other two are in  $k(a^{1/2})\langle x^{-1} \rangle$ . In any case, this yields signature  $(1, 1, 1, 1, 1, 1)$  if  $a$  is a square in  $k$  and  $(1, 1, 1, 2)$  otherwise.

*Case  $|A|^3 = |B|^2$ :* Then  $|A|^3 = |B|^2 = q^{6j}$  for some  $j \in \mathbb{N}$ .

Assume first that  $\deg(D)$  is even. Then  $\delta_+^3$  and  $\delta_-^3$  are Laurent series in  $x^{-1}$  of degree  $3j$  with coefficients in  $\bar{k}$ . By Lemma 4.1,  $\delta_+, \delta_- \in \bar{k}\langle x^{-1} \rangle$ , so the same holds for  $y_0, y_1, y_2$ . Furthermore, at least two among these roots have degree  $j$ , and since  $|y_0y_1y_2| = |B| = q^{3j}$ , they all have degree  $j$ .

Suppose first that  $4a^3 \neq 27b^2$ . Let  $y \in \{y_0, y_1, y_2\}$  and set  $s = \text{sgn}(y)$ . Then  $s^3 - as + b = 0$ . We note that  $3s^2 \neq a$ , as otherwise  $b = as - s^3 = 2s^3$ , implying  $4a^3 = 27b^2$ . For  $i \in \mathbb{N}$ , let  $s_{j-i}$  be the coefficient of  $x^{j-i}$  in  $y$ . By

considering the coefficient of  $x^{3j-i}$  in the equation  $y^3 - Ay + B = 0$ , we see that  $s_{j-i} = (3s^2 - a)^{-1}g$  where  $g$  is a linear combination of products involving the coefficients of  $A$  and  $B$  as well as  $s_{j-i+1}, s_{j-i+2}, \dots, s_{j-1}, s$  ( $i \in \mathbb{N}$ ). A simple induction argument thus shows that  $s_{j-i} \in k(s)$  for all  $i \in \mathbb{N}$ . Hence,  $y_i \in k(\text{sgn}(y_i))\langle x^{-1} \rangle$  where  $\text{sgn}(y_i)$  is a root of the equation  $t^3 - at + b = 0$  for  $i = 0, 1, 2$ . This equation has 0, 1, or 3 distinct roots, yielding respective signatures  $(1, 3)$ ,  $(1, 1, 1, 2)$ , and  $(1, 1, 1, 1, 1, 1)$ .

Now suppose that  $4a^3 = 27b^2$ . Then  $a = 3e^2, b = 2e^3$  where  $e = 3b/2a \in k^*$ , and  $\text{sgn}(\delta_+^3) = \text{sgn}(\delta_-^3) = -27e^3$ . Let  $s$  be a square root of  $-3\text{sgn}(D)$  in some suitable extension of  $k$ . Then by Lemma 4.1,  $\sqrt{-3D} \in k(s)\langle x^{-1} \rangle$ , so  $\delta_+^3, \delta_-^3 \in k(s)\langle x^{-1} \rangle$ . Again by Lemma 4.1,  $\delta_+, \delta_- \in k(s)\langle x^{-1} \rangle$ . Write  $\delta_+ = \beta + \gamma s$  with  $\beta, \gamma \in k\langle x^{-1} \rangle$ . Then we reason completely analogous to the case  $3m > 2n$ ,  $m$  even, that  $K/k(x)$  has signature  $(1, 1, 1, 1, 1, 1)$  if  $\text{sgn}(D)$  is a square in  $k$  and  $(1, 1, 1, 2)$  otherwise.

Assume now that  $\deg(D)$  is odd. Then  $\sqrt{-3D} \in k\langle x^{-1/2} \rangle \setminus k\langle x^{-1} \rangle$ , so  $\delta_+^3, \delta_-^3 \in k\langle x^{-1/2} \rangle \setminus k\langle x^{-1} \rangle$ , and hence  $\delta_+, \delta_- \notin \bar{k}\langle x^{-1} \rangle$ . It follows that at least one of the roots does not lie in  $\bar{k}\langle x^{-1} \rangle$ , so the signature is  $(1, 1, 2, 1)$  or  $(3, 1)$ . But for signature  $(3, 1)$ , we have  $y_i \in k\langle x^{-1/3} \rangle$  for  $i = 0, 1, 2$ , so  $\delta_+ \in k(y_0, y_1, y_2, u) = k(u)\langle x^{-1/3} \rangle$ , and hence  $\delta_+^3 \in k(u)\langle x^{-1/3} \rangle \cap k\langle x^{-1/2} \rangle = k\langle x^{-1} \rangle$ , which is a contradiction. So  $K/k(x)$  must have signature  $(1, 1, 2, 1)$  in this case.  $\square$

We point out that Lee [7] provided an elegant proof of the above theorem that uses the Hilbert class field of  $k(x, \sqrt{\Delta})$ , but it is restricted to square-free  $\Delta$ . One can also apply the transformation  $x \rightarrow x^{-1}$  and investigate the polynomial  $x^{3l}F(Y, x^{-1}) \pmod{x}$ , but this will be inconclusive in certain cases (when  $(0, 0)$  is a singular point of the resulting curve, i.e.  $\deg(A)$  is odd and  $\deg(B) \equiv 1 \pmod{3}$ ).

Using the signature description for purely cubic function fields given in Theorem 2.1 of [12] and the well-known characterization of hyperelliptic function fields (see for example Proposition 14.6 on p. 248 of [9]), we can reformulate and summarize Theorem 4.2 as follows.

**Corollary 4.3.** *Let  $\mathcal{C} : f(x, y) = 0$  with  $f(Y) = Y^3 - AY + B \in k[x][Y]$  be a standard model of a cubic extension  $K/k(x)$  where  $k = \mathbb{F}_q$  is a finite field of characteristic at least 5. Set  $D = 4A^3 - 27B^2$ . Then the following holds:*

- *If  $|D| \neq |B|^2$  — this is exactly the case if either  $|A|^3 > |B|^2$  or  $|A|^3 = |B|^2$  and  $4\text{sgn}(A)^3 = 27\text{sgn}(B)^2$  — then the signature of  $K/k(x)$  is  $(1, 1, S)$  where  $S$  is the signature of the hyperelliptic extension  $k(x)(\sqrt{D})/k(x)$ .*
- *If  $|D| = |B|^2$ , then there are two cases:*
  - *If  $|A|^3 < |B|^2$ , then the signature of  $K/k(x)$  is equal to the signature of the purely cubic extension  $k(x)(\sqrt[3]{D})/k(x)$ .*
  - *If  $|A|^3 = |B|^2$  and  $4\text{sgn}(A)^3 \neq 27\text{sgn}(B)^2$ , then  $K/k(x)$  is unramified (i.e. all the  $e_i$  in the signature of  $K/k(x)$  are equal to 1), and the  $f_i$  in the signature are the degrees (with respect to the indeterminate  $t$ ) of the irreducible factors of the equation  $t^3 - \text{sgn}(A)t + \text{sgn}(B) = 0$  over  $k$ .*

## 5 Unit Group and Regulator

Let  $K = k(x, y)$  be a cubic function field of characteristic different from 3 in standard form with minimal polynomial  $f(Y) = Y^3 - AY + B \in k[x][Y]$ . As before, denote by  $y = y_0, y' = y_1, y'' = y_2$  the roots of  $f(Y)$  (given by (4.2) if  $k$  has odd characteristic). For any  $\theta = a + by + cy^2 \in K$ , write  $\theta^{(i)} = a + by_i + cy_i^2$  for the  $i$ -th conjugate of  $\theta$  ( $0 \leq i \leq 2$ ). The *unit group* of  $K/k(x)$  is the group of units  $\mathcal{O}^*$  of the maximal order  $\mathcal{O}$  of  $K$ . By Dirichlet's Unit Theorem,  $\mathcal{O}^*$  is an infinite Abelian group whose torsion part is  $k^*$  and whose torsion-free part has rank  $s - 1$  where  $s$  is the number of places at infinity in  $K/k(x)$ . The quantity  $r = s - 1$  is called the *unit rank* of  $K/k(x)$ . The following table outlines the possible unit rank scenarios for cubic function fields.

<i>Signature</i>	<i>Unit Rank</i>
(1, 3) or (3, 1)	0
(1, 1, 1, 2) or (1, 1, 2, 1)	1
(1, 1, 1, 1, 1)	2

A set of generators  $\{\epsilon_1, \epsilon_2, \dots, \epsilon_r\}$  of  $\mathcal{O}^*/k^*$  is a system of *fundamental units*. Let  $\{\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_s\}$  be the set of divisors in  $K$  lying above the place at infinity in  $k(x)$  as described in (4.1). For  $1 \leq i \leq s$ , let  $f_i$  denote the residue degree of  $\mathfrak{p}_i$  and  $\nu_i$  the additive valuation associated with  $\mathfrak{p}_i$ . Consider the  $r \times s$  integer matrix

$$M = \begin{pmatrix} -f_1\nu_1(\epsilon_1) & -f_2\nu_2(\epsilon_1) & \dots & -f_s\nu_s(\epsilon_1) \\ -f_1\nu_1(\epsilon_2) & -f_2\nu_2(\epsilon_2) & \dots & -f_s\nu_s(\epsilon_2) \\ \vdots & \vdots & \dots & \vdots \\ -f_1\nu_1(\epsilon_r) & -f_2\nu_2(\epsilon_r) & \dots & -f_s\nu_s(\epsilon_r) \end{pmatrix}.$$

Rosen [9, p. 245] defines the *regulator*  $R_S^{(q)}$  to be the absolute value of the determinant of any of the  $r \times r$  minors obtained by deleting the  $j$ -th column from  $M$  ( $1 \leq j \leq s$ ); it is easy to show that this definition is independent of the minor and the set of fundamental units chosen. While this definition is consistent with the definition of the regulator for an algebraic number field, Schmidt [13] presents a slightly different definition.

Denote by  $\mathcal{S}$  the group generated by  $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_s$ , and let  $\mathcal{S}_0 = \{\mathfrak{d} \in \mathcal{S} \mid f_{\mathfrak{d}} = 0\}$  where  $f_{\mathfrak{d}}$  is the residue degree of  $\mathfrak{d}$ . If  $\mathcal{P}$  denotes the group of principal divisors, then  $\mathcal{S}_0 \cap \mathcal{P}$  is generated by the divisors  $(\epsilon_i)$  of the fundamental units  $\epsilon_i$  for  $1 \leq i \leq s$ . According to Schmidt, the *regulator* of  $K/k(x)$  is the group index  $R = [\mathcal{S}_0 : \mathcal{P} \cap \mathcal{S}_0]$ . By Lemma 4.13 of [9], the two regulators are related via the identity

$$R_S^{(q)} = \frac{f_1 f_2 \cdots f_s}{\gcd(f_1, f_2, \dots, f_s)} R. \quad (5.1)$$

Furthermore, if  $h$  is the class number, i.e. the order of the Jacobian, of  $K/k$ , and  $h'$  the ideal class number of  $K/k(x)$ , then by Theorem 25 of [13],

$$h = \frac{R}{\gcd(f_1, f_2, \dots, f_s)} h' = \frac{R_S^{(q)}}{f_1 f_2 \cdots f_s} h'. \quad (5.2)$$

Specifically, for cubic function fields:

**Theorem 5.1.** *Let  $\mathcal{C} : y^3 - Ay + B = 0$  be a standard model of a cubic extension  $K/k(x)$ . Let  $h$  be the order of the Jacobian of  $K/k$ , and let  $h'$ ,  $R_S^{(q)}$ , and  $R$  denote the ideal class number, the regulator à la Rosen, and the regulator à la Schmidt, of  $K/k(x)$ , respectively. Let  $\{\epsilon_1, \epsilon_2, \dots, \epsilon_r\}$  be a system of fundamental units of  $K/k(x)$ . If  $K/k(x)$  has signature*

- $(1, 1, 1, 1, 1, 1)$ , then  $R = R_S^{(q)} = \left| \det \begin{pmatrix} \deg(\epsilon_1^{(i)}) & \deg(\epsilon_2^{(i)}) \\ \deg(\epsilon_1^{(j)}) & \deg(\epsilon_2^{(j)}) \end{pmatrix} \right|$  where  $i, j \in \{0, 1, 2\}$  with  $i \neq j$ , and  $h = Rh'$ ;
- $(1, 1, 1, 2)$ , then  $R = R_S^{(q)}/2 = |\deg(\epsilon_1)|/2$ , and  $h = Rh'$ ;
- $(1, 3)$  then  $R = R_S^{(q)}/3 = 1$ , and  $h = h'/3$ ;
- $(1, 1, 2, 1)$ , then  $R = R_S^{(q)} = |\deg(\epsilon_1)|$ , and  $h = Rh'$ ;
- $(3, 1)$ , then  $R = R_S^{(q)} = 1$ , and  $h = h'$ .

*Proof.* The relationships between  $R_S^{(q)}$  and  $R$  as well as  $h$  and  $h'$  follow from (5.1) and (5.2), respectively. For the rest, we can reason as in the proof of Theorem 2.1 of [12]: in the cases where there is only one (inert or totally ramified) place at infinity in  $K$ ,  $\mathcal{S}_0$  is trivial and hence  $R = 1$ . For signature  $(1, 1, 1, 1, 1, 1)$ , the formula for  $R$  follows from the fact that the map that permutes the three roots of  $f(Y)$  also permutes the three places at infinity. Finally, if there are two places at infinity in  $K$ , of respective degrees  $f_1 = 1$  and  $f_2 = 1$  or  $2$ , then  $R = |\nu_1(\epsilon_1)|/f_2$ . Since  $f_1 = 1$ , the completion of  $K$  with respect to  $\nu_1$  is equal to  $k\langle x^{-1} \rangle$ , so  $|\nu_1(\epsilon_1)| = |\deg(\epsilon_1)|$ .  $\square$

If  $K/k(x)$  has signature  $(3, 1)$ , i.e. the place at infinity in  $k(x)$  is totally ramified in  $K$ , then the Jacobian of  $K/k$  is in fact isomorphic to the ideal class group of  $K/k(x)$ .

## 6 Fundamental Units

In order to compute the regulator and/or fundamental unit(s) of a cubic function field of nonzero unit rank, we require the notion of ideal reduction. Once again, we let  $K(x, y)$  be a cubic function field of characteristic at least 5 in standard form with minimal polynomial  $f(Y) = Y^3 - AY + B \in k[x, Y]$  and unit rank  $r > 0$ . Possible signatures for  $K/k(x)$  are  $(1, 1, 1, 1, 1, 1)$  if  $r = 2$  and  $(1, 1, 1, 2)$  or  $(1, 1, 2, 1)$  if  $r = 1$ . Let the roots of  $f$  be  $y_0 = y, y_1 = y', y_2 = y''$ . We henceforth write the embedding(s) of  $K$  into  $k\langle x^{-1} \rangle$  multiplicatively. If  $r = 2$ , then there are three such embeddings given by three valuations  $|\cdot|_i$  ( $0 \leq i \leq 2$ ). We write  $|\cdot|_0 = |\cdot|$  and number the valuations so that  $|y|_i = |y_i| = q^{\deg(y_i)}$ , so  $|\theta|_i = |\theta^{(i)}|$  for all  $\theta \in K$  and  $0 \leq i \leq 2$ . If  $r = 1$ , then there is just one embedding of  $K$  into  $k\langle x^{-1} \rangle$  which we write as  $|\cdot|$ . To unify the notation for both unit rank scenarios, we set  $|\theta|_0 = |\theta|$ ,  $|\theta|_1 = |\theta|_2 = |\theta'\theta''|^{1/2}$  for all  $\theta \in K$  in the unit rank 1 case.

The regulator and fundamental unit(s) of  $K/k(x)$  can be computed exactly as described in [12] for the unit rank 1 case and [6] for the case of unit rank 2,

so we only give the minimal necessary background here and recall the algorithm for completeness. We focus our discussion on *fractional* ideals of  $\mathcal{O}$ , i.e. subsets  $\mathfrak{f}$  of  $K$  such that  $d\mathfrak{f}$  is an ideal in  $\mathcal{O}$  for some nonzero  $d \in k[x]$ . In our context, fractional ideals are always nonzero — so they are  $k[x]$ -submodules of  $K$  of rank 3 — and contain 1. A fractional ideal  $\mathfrak{f}$  is *reduced* if for any  $\theta \in \mathfrak{f}$ , the inequalities  $|\theta|_i \leq 1$  for  $i = 0, 1, 2$  imply  $\theta \in k$ . Note that  $\mathcal{O}$  is reduced.

Let  $\{1, \rho, \omega\}$  be a canonical basis of  $K/k(x)$ . For  $\alpha = a + b\rho + c\omega \in K$  with  $a, b, c \in k(t)$ , we let<sup>1</sup>

$$\begin{aligned}\zeta_\alpha &= \alpha' + \alpha'' &= \text{Tr}(\alpha) - \alpha &= (2a - 3bT + cE) - b\rho - c\omega, \\ \xi_\alpha &= \alpha - \frac{1}{3}\text{Tr}(\alpha) &= \frac{1}{3}(2\alpha - \zeta_\alpha) &= (bT - \frac{1}{3}Ec) + b\rho + c\omega, \\ \eta_\alpha &= \alpha' - \alpha'' &= (y' - y'') &= \left(b - \frac{c}{I}\rho\right),\end{aligned}\tag{6.1}$$

where  $E, T$ , and  $I$  (the index of  $y$ ) are as in Corollary 3.2. Note that  $\zeta_\alpha, \xi_\alpha, \eta_\alpha/(y' - y'') \in K$ .

Let  $\{1, \mu, \nu\}$  be a  $k[x]$ -basis of some non-zero reduced fractional ideal  $\mathfrak{f}$  of  $\mathcal{O}$ . Then it is easy to verify that

$$\det \begin{pmatrix} \xi_\mu & \eta_\mu \\ \xi_\nu & \eta_\nu \end{pmatrix}^2 = (\xi_\mu \eta_\nu - \xi_\nu \eta_\mu)^2 = s \Delta(\mathfrak{f})\tag{6.2}$$

for some  $s \in k^*$ . For  $i \in \{0, 1, 2\}$ , the basis  $\{1, \mu, \nu\}$  is said to be  *$i$ -reduced* if

$$|\xi_\mu|_i > |\xi_\nu|_i, \quad |\eta_\mu|_i < 1 \leq |\eta_\nu|_i, \quad |\zeta_\mu|_i < 1, |\zeta_\nu|_i < 1.\tag{6.3}$$

Such a basis always exists and is unique up to nonzero constant factors (Theorem 4.4 in [6]). Since  $|\eta_\mu|_i, |\zeta_\mu|_i < 1$ , we have  $|\mu'|_i, |\mu''|_i < 1$ , so  $|\mu|_i > 1$  since  $\mathfrak{f}$  is reduced and  $\mu \notin k$ . It follows that  $|\xi_\mu|_i = |\mu|_i > 1$  and hence from (6.2) and (6.3),  $|\Delta(\mathfrak{f})| > 1$  and  $|\nu|_i < |\mu|_i \leq |\Delta(\mathfrak{f})|$ . Furthermore,  $|\nu'|_i = |\nu''|_i \geq 1$ .

The following theorem gives the connection between reduced bases and fundamental units. For purely cubic extensions, the relevant discussion of the unit rank 1 case can be found on p. 1255 of [12]; see also Theorem 3.7 in [6] for unit rank 2. The result was proved for arbitrary number fields of unit rank 1 and 2 in [3], and the proofs in that source carry over completely to the function field setting.

**Theorem 6.1.**

1. Suppose  $r = 1$  and set  $\mathfrak{f}_0 = \mathcal{O}$ ,  $\mathfrak{f}_{n+1} = (\mu_n)^{-1}\mathfrak{f}_n$  for  $n \geq 1$  where  $\{1, \mu_n, \nu_n\}$  is a 0-reduced basis of the reduced fractional ideal  $\mathfrak{f}_n$ . Let  $l \in \mathbb{N}$  be the minimal index such that  $\mathfrak{f}_l = \mathfrak{f}_0$ . Then

$$\epsilon = \prod_{i=0}^{l-1} \mu_i$$

<sup>1</sup> The definitions of  $\zeta_\alpha, \xi_\alpha, \eta_\alpha$  can be modified in such a way that the reduction algorithm given below also works in fields of even characteristic, other than  $\mathbb{F}_2$ . Since we excluded the characteristic 2 case up to now, we omit the details here.

is a fundamental unit of  $K/k(x)$ .

2. Suppose  $r = 2$  and set  $\mathfrak{f}_0 = \mathcal{O}$ ,  $\mathfrak{f}_{n+1} = (\alpha_n^{-1})\mathfrak{f}_n$  for  $n \geq 0$  where

$$\alpha_n = \begin{cases} \mu_n & \text{if } |\nu_n|_1 > 1, \\ \nu_n - \text{sgn}(\nu_n) & \text{if } |\nu_n|_1 = 1, \end{cases}$$

and  $\{1, \mu_n, \nu_n\}$  is a 0-reduced basis of the reduced fractional ideal  $\mathfrak{f}_n$ . Let  $p \in \mathbb{Z}^{\geq 0}$  and  $l \in \mathbb{N}$  be minimal such that  $\mathfrak{f}_{p+l} = \mathfrak{f}_p$  and set

$$\epsilon_1 = \prod_{i=p}^{p+l-1} \alpha_i.$$

Now set  $\mathfrak{g}_0 = \mathfrak{f}_p$ ,  $\mathfrak{g}_{n+1} = (\beta_n^{-1})\mathfrak{g}_n$  for  $n \geq 1$  where

$$\beta_n = \begin{cases} \sigma_n & \text{if } |\tau_n|_0 > 1, \\ \tau_n - \text{sgn}(\tau_n) & \text{if } |\tau_n|_0 = 1. \end{cases}$$

and  $\{1, \sigma_n, \tau_n\}$  is a 2-reduced basis of the reduced fractional ideal  $\mathfrak{g}_n$ . Let  $m, h \in \mathbb{Z}^{\geq 0}$  be minimal such that  $\mathfrak{g}_m = \mathfrak{f}_{p+h}$  and set

$$\epsilon_2 = \prod_{j=0}^{m-1} \beta_j \left( \prod_{i=p}^{p+h-1} \alpha_i \right)^{-1}.$$

Then  $\{\epsilon_1, \epsilon_2\}$  is a pair of fundamental units of  $K/k(x)$ .

To find the regulator instead of the fundamental unit(s), we can avoid evaluating the (computationally expensive) products given above. Instead, we simply sum over the degrees of the  $\mu_i$  (for  $r = 1$ ), respectively, the  $\alpha_i, \alpha'_i, \beta_j$ , and  $\beta'_j$  (for  $r = 2$ ). Note that ideal equality as required in the above theorem can be tested by comparing appropriately normalized 0-reduced bases.

Theorem 6.1 implies that in order to determine the fundamental unit(s) of  $K/k(x)$ , we require a way to compute for  $i \in \{0, 1, 2\}$  an  $i$ -reduced basis of a reduced fractional ideal  $\mathfrak{f}$ , where  $\mathfrak{f}$  is given in terms of a  $k[x]$ -basis of the form  $\{1, \tilde{\mu}, \tilde{\nu}\}$  with

$$\begin{aligned} \{\tilde{\mu}, \tilde{\nu}\} &= \{\rho, \omega\} \text{ or} \\ \{\tilde{\mu}, \tilde{\nu}\} &= \{\mu^{-1}, \nu\mu^{-1}\} \text{ or} \\ \{\tilde{\mu}, \tilde{\nu}\} &= \{\theta^{-1}, \mu\theta^{-1}\} \text{ where } \theta = \nu - \text{sgn}(\nu^{(i+1)}), \end{aligned} \tag{6.4}$$

where the last case only occurs for unit rank 2 and  $i = 0$  or  $i = 2$  (in the latter case,  $i+1$  is taken to be 0). Then the desired reduced bases can be computed using the following algorithm (see also Algorithm 7.1 of [12] with the simplification of Algorithm 6.3 in [10] for  $r = 1$ , and Algorithm 4.6 of [6] for  $r = 2$ ):

**Algorithm 6.2.**

*Input:*  $(i, \tilde{\mu}, \tilde{\nu})$  where  $i \in \{0, 1, 2\}$  and  $\tilde{\mu}, \tilde{\nu}$  are given by (6.4).

*Output:*  $(\mu, \nu)$  where  $\{1, \mu, \nu\}$  is an  $i$ -reduced basis of  $\mathfrak{f}$ .

*Algorithm:*

1. Set  $\mu = \tilde{\mu}$ ,  $\nu = \tilde{\nu}$ .
2. If  $|\xi_\mu|_i < |\xi_\nu|_i$  or if  $|\xi_\mu|_i = |\xi_\nu|_i$  and  $|\eta_\mu|_i < |\eta_\nu|_i$ ,  
replace  $\begin{pmatrix} \mu \\ \nu \end{pmatrix}$  by  $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}$ .
3. If  $|\eta_\mu|_i \geq |\eta_\nu|_i$  then
  - 3.1. ( $r = 2$  only.) While  $|\xi_\nu \eta_\nu|_i > |\Delta(f)|^{1/2}$ ,  
replace  $\begin{pmatrix} \mu \\ \nu \end{pmatrix}$  by  $\begin{pmatrix} 0 & 1 \\ -1 & \lfloor \xi_{\mu^{(i)}} / \xi_{\nu^{(i)}} \rfloor \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}$ .
  - 3.2. Replace  $\begin{pmatrix} \mu \\ \nu \end{pmatrix}$  by  $\begin{pmatrix} 0 & 1 \\ -1 & \lfloor \xi_{\mu^{(i)}} / \xi_{\nu^{(i)}} \rfloor \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}$ .
  - 3.3. If  $|\eta_\mu|_i = |\eta_\nu|_i$ ,  
replace  $\begin{pmatrix} \mu \\ \nu \end{pmatrix}$  by  $\begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}$  where  $a = \text{sgn}(\eta_{\mu^{(i)}}) \text{sgn}(\eta_{\nu^{(i)}}^{-1})$ .
4. While  $|\eta_\mu|_i > 1$ , replace  $\begin{pmatrix} \mu \\ \nu \end{pmatrix}$  by  $\begin{pmatrix} \lfloor \eta_{\nu^{(i)}} / \eta_{\mu^{(i)}} \rfloor & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}$ .
5. Replace  $\mu$  by  $\mu - \lfloor \zeta_{\mu^{(i)}} \rfloor / 2$  and  $\nu$  by  $\nu - \lfloor \zeta_{\nu^{(i)}} \rfloor / 2$ .
6. Return  $(\mu, \nu)$ .

Here, for  $\alpha = \sum_{i=-\infty}^m a_i x^i \in k\langle x^{-1} \rangle$ , the expression  $[\alpha] = \sum_{i=0}^m a_i x^i$  denotes the polynomial part of  $\alpha$ .

## 7 Approximations

In order to compute expressions such as  $\lfloor \xi_{\mu^{(i)}} / \xi_{\nu^{(i)}} \rfloor$  or even just  $|\eta_\mu|_i = |\eta_{\mu^{(i)}}|$  in Algorithm 6.2, it is necessary to have a sufficiently good approximation for the basis elements  $\rho, \omega$  (and their conjugates in the unit rank 2 case). These elements lie in  $k\langle x^{-1} \rangle$  and thus have an infinite expansion in  $x^{-1}$ , of which we can only carry finitely many terms. We in turn require sufficiently good approximations for the root(s)  $y_0$  (and in the unit rank 2 case,  $y_1$  and  $y_2$  as well) of  $f(Y) = Y^3 - AY + B$ . In purely cubic fields, this can be accomplished by explicitly extracting a cube root of  $-B$  to a sufficient precision. However, if the extension is not purely cubic, i.e.  $A \neq 0$ , we need to proceed differently; in fact, we essentially use Newton's method.

Analogous to [10] and [6], we define for a nonzero element  $\alpha \in k\langle x^{-1} \rangle$  of degree  $m$  a *relative approximation of precision*  $n \in \mathbb{Z}^{\geq 0}$  to  $\alpha$  to be a truncated Laurent series  $\hat{\alpha}$  with  $|1 - \hat{\alpha}/\alpha| < q^{-n}$ . If  $\alpha = \sum_{i=-\infty}^m a_i x^i$ , then we can set  $\hat{\alpha} = \sum_{i=m-n}^m a_i x^i$ . For purely cubic fields, the analysis in [10] revealed that precision  $n = \deg(\Delta)/2$  for relative approximations to the basis elements  $\rho$  and  $\omega$  was sufficient to guarantee that the reduction algorithm (with  $\rho$  and  $\omega$  replaced by their respective approximations) produces correct results. We suspect that

the same is true for arbitrary cubic fields, but a more careful investigation of this question is warranted and is the subject of future research.

**Theorem 7.1.** *Let  $\alpha \in k\langle x^{-1} \rangle$  be any root of  $f(Y) = Y^3 - AY + B$  ( $A, B \in k[x]$ ,  $AB \neq 0$ ). Set  $l = \max\{0, -\deg(A\alpha^{-2} - 3)\} \in \mathbb{Z}^{\geq 0}$ , and let  $\alpha_0$  be a relative approximation of precision  $l$  to  $\alpha$ . For  $j \in \mathbb{N}$ , define*

$$\alpha_j = \left\lfloor \frac{(2\alpha_{j-1}^3 - B)x^{r_j}}{3\alpha_{j-1}^2 - A} \right\rfloor x^{-r_j} \text{ with } r_j = \max\{0, 2^j - 1 + l - \deg(\alpha)\} \in \mathbb{Z}^{\geq 0}.$$

Then  $\left| 1 - \frac{\alpha}{\alpha_j} \right| \leq q^{-(2^j+1)}$  for all  $j \geq 0$ .

*Proof.* The claim holds for  $j = 0$ . For  $j \geq 0$ , we have

$$|\alpha - \alpha_{j+1}| = \left| \left( \alpha - \frac{2\alpha_j^3 - B}{3\alpha_j^2 - A} \right) + \left( \frac{2\alpha_j^3 - B}{3\alpha_j^2 - A} - \left\lfloor \frac{(2\alpha_j^3 - B)x^{r_{j+1}}}{3\alpha_j^2 - A} \right\rfloor x^{-r_{j+1}} \right) \right|.$$

The expression in the second set of parentheses has absolute value at most  $q^{-r_{j+1}-1} \leq q^{-(2^{j+1}+1)}|\alpha|$ . For the term in the first set of parentheses, write

$$\begin{aligned} \alpha - \frac{2\alpha_j^3 - B}{3\alpha_j^2 - A} &= (\alpha - \alpha_j) + \left( \alpha_j - \frac{2\alpha_j^3 - B}{3\alpha_j^2 - A} \right) = \alpha - \alpha_j + \frac{\alpha_j^3 - A\alpha_j + B}{3\alpha_j^2 - A} \\ &= \alpha - \alpha_j + \frac{(\alpha_j^3 - A\alpha_j + B) - (\alpha^3 - A\alpha + B)}{3\alpha_j^2 - A} \\ &= (\alpha - \alpha_j) \left( 1 - \frac{\alpha_j^2 + \alpha\alpha_j + \alpha^2 - A}{3\alpha_j^2 - A} \right) = -(\alpha - \alpha_j)^2 \frac{\alpha + 2\alpha_j}{3\alpha_j^2 - A}. \end{aligned}$$

Now  $|3\alpha_j^2 - A| = |3(\alpha_j^2 - \alpha^2) + 3\alpha^2 - A|$ . By induction hypothesis and assumption,  $|\alpha_j^2 - \alpha^2| < q^{-l}|\alpha|^2 \leq |3\alpha^2 - A|$ , so since  $|\alpha + 2\alpha_j| = |\alpha|$ , again by induction hypothesis,

$$\left| \alpha - \frac{2\alpha_j^3 - B}{3\alpha_j^2 - A} \right| \leq (q^{-(2^j+1)})^2 |\alpha|^2 \frac{|\alpha|}{|3\alpha^2 - A|} \leq q^{-2^{j+1}-2l} |\alpha|^3 \frac{q^l}{|\alpha|^2} = q^{-(2^{j+1}+l)} |\alpha|.$$

□

**Lemma 7.2.** *Let  $f(Y) = Y^3 - AY + B$  ( $A, B \in k[x]$ ,  $B \neq 0$ ) and let  $y_0, y_1, y_2$  be the zeros of  $f(Y)$  with  $y_0 \in k\langle x^{-1} \rangle$  ( $y_1, y_2 \in k\langle x^{-1} \rangle$  if  $K$  has unit rank 2).*

- *If  $|A|^3 > |B|^2$ , then  $|y_0| = |B|/|A|$ ,  $\text{sgn}(y_0) = \text{sgn}(B)/\text{sgn}(A)$ ,  $|y_1| = |y_2| = |A|^{1/2}$  and  $\text{sgn}(y_1) = -\text{sgn}(y_2) = \text{sgn}(A)^{1/2}$ .*
- *If  $|A|^3 < |B|^2$ , then  $|y_i| = |B|^{1/3}$  and  $\text{sgn}(y_i) = -u^i \text{sgn}(B)^{1/3}$  for  $i = 0, 1, 2$ , where  $u$  is a primitive cube root of unity.*
- *If  $|A|^3 = |B|^2$ , then  $|y_i| = |A|^{1/2}$  and the values of  $\text{sgn}(y_i)$  are the roots of the equation  $t^3 - \text{sgn}(A)t + \text{sgn}(B) = 0$  for  $i = 0, 1, 2$ . If  $4\text{sgn}(A)^3 \neq 27\text{sgn}(B)^2$ , then these roots are distinct, otherwise, the roots are  $-2c, c, c$  where  $c = 3\text{sgn}(B)/2\text{sgn}(A)$ , so  $\text{sgn}(A) = 3c^2$  and  $\text{sgn}(B) = 2c^3$ .*

Lemma 7.2 shows that the quantity  $l$  in Theorem 7.1 is almost always zero, in which case we can determine  $\alpha_0 = \text{sgn}(\alpha)x^{\deg(\alpha)}$  from the lemma. In order to obtain a desired precision  $n$  for our root approximation, we then simply compute  $\alpha_0, \alpha_1, \dots, \alpha_m$  where  $m = \lceil \log_2(n+1) \rceil$ . The only problematic case which requires a better initial approximation  $\alpha_0$  to  $\alpha$  happens when  $|A|^3 = |B|^2$  and  $4\text{sgn}(A)^3 = 27\text{sgn}(B)^2$ . The smaller  $|A\alpha^{-2} - 3|$  is, the closer our situation resembles a repeated root scenario (as expected), with two roots  $y_1, y_2$  of  $f(Y)$  lying close together (and close to one of the square roots of  $A/3$  as well as one of the cube roots of  $B/2$ ). Then  $4A^3 \approx 27B^2$ , i.e.  $|D|$  is small as well (note that  $|D| = |A|^2|y_1 - y_2|^2$  in this case).

Note that in order to determine  $|\eta_\mu|_i$  in step 4 of Algorithm 6.2, we need to compute  $|y' - y''|_i$  by (6.1). If  $|y' - y''|_i \geq |y'|_i$ , this can be done using Lemma 7.2; otherwise, we have  $|y' - y''|_i^2 = |\Delta|(y - y')(y - y'')|_i^{-2}$ , and the denominator can again be computed using Lemma 7.2.

We will present an implementation of the ideas presented here as well as numerical results in a future paper.

## References

1. S. AMRITA, Construction of secure  $C_{ab}$  curves using modular curves. *Proc. Fourth Algorithmic Number Theory Symp. ANTS-IV, Lect. Notes Comp. Sci.* **1838**, Springer, Berlin 2000, 113-126.
2. M. L. BAUER, The arithmetic of certain cubic function fields. *Math. Comp.* **73** (2004), 387-413.
3. J. A. BUCHMANN, A generalization of Voronoi's algorithm I, II. *J. Number Theory* **20** (1985), 177-209.
4. B. N. DELONE & D. K. FADEEV, *The Theory of Irrationalities of the Third Degree. Transl. Math. Monographs* **10**, Amer. Math. Soc., Providence, Rhode Island 1964.
5. S. D. GALBRAITH, S. PAULUS & N. P. SMART, Arithmetic on superelliptic curves. *Math. Comp.* **71** (2002), 393-405.
6. Y. LEE, R. SCHEIDLER & C. YARRISH, Computation of the fundamental units and the regulator of a cyclic cubic function field. *Exper. Math.* **12** (2003), 211-225.
7. Y. LEE, *The unit rank classification of a general cubic function field by its discriminant*. Preprint.
8. P. LLORENTE & E. NART, Effective determination of the decomposition of the rational primes in a cubic field. *Proc. Amer. Math. Soc.* **87** (1983), 579-585.
9. M. ROSEN, *Number Theory in Function Fields*. Springer, New York 2002.
10. R. SCHEIDLER, Reduction in purely cubic function fields of unit rank one. *Proc. Fourth Algorithmic Number Theory Symp. ANTS-IV, Lect. Notes Comp. Sci.* **1838**, Springer, Berlin 2000, 515-532.
11. R. SCHEIDLER, Ideal arithmetic and infrastructure in purely cubic function fields. *J. Théorie Nombres. Bordeaux* **13** (2001), 609-631.
12. R. SCHEIDLER & A. STEIN, Voronoi's algorithm in purely cubic congruence function fields of unit rank 1. *Math. Comp.* **69** (2000), 1245-1266.
13. F. K. SCHMIDT, Analytische Zahlentheorie in Körpern der Charakteristik  $p$ . *Math. Zeitschr.* **33** (1931), 1-32.
14. G. F. VORONOI, *On a Generalization of the Algorithm of Continued Fractions* (in Russian). Doctoral Dissertation, Warsaw 1896.