J. Symbolic Computation (2000) **30**, 309–323
doi:10.1006/jsco.2000.0372
Available online at http://www.idealibrary.com on IDEAL

Finding a Basis of a Linear System with Pairwise Distinct Discrete Valuations on an Algebraic Curve*

RYUTAROH MATSUMOTO[†§] AND SHINJI MIURA[‡]

[†] *Sakaniwa Lab., Department of Electrical and Electronic Engineering, Tokyo Institute of Technology, Ookayama 2-12-1, Meguro-ku, Tokyo, 152-8552 Japan*
[‡] *Sony Corporation Information & Network Technologies Laboratories, Kitashinagawa 6-7-35, Shinagawa-ku, Tokyo, Japan*

Under the assumption that we have defining equations of an affine algebraic curve in special position with respect to a rational place Q, we propose an algorithm computing a basis of $\mathcal{L}(D)$ of a divisor D from an ideal basis of the ideal $\mathcal{L}(D+\infty Q)$ of the affine coordinate ring $\mathcal{L}(\infty Q)$ of the given algebraic curve, where $\mathcal{L}(D+\infty Q) := \bigcup_{i=1}^{\infty} \mathcal{L}(D+iQ)$. Elements in the basis produced by our algorithm have pairwise distinct discrete valuations at Q, which is convenient in the construction of algebraic geometry codes. Our method is applicable to a curve embedded in an affine space of arbitrary dimension, and involves only the Gaussian elimination and the division of polynomials by the Gröbner basis for the ideal defining the curve.

1. Introduction

For a divisor D on an algebraic curve, there exists the associated linear space $\mathcal{L}(D)$. Recently we showed how to apply the Feng–Rao bound and decoding algorithm (Feng and Rao, 1993) for the Ω-construction of algebraic geometry codes to the $\mathcal{L}$-construction, and showed examples in which the $\mathcal{L}$-construction gives better linear codes than the Ω-construction on the same curve in a certain range of parameters (Matsumoto and Miura, 2000). In order to apply the Feng–Rao algorithm to an algebraic geometry code from the $\mathcal{L}$-construction, it is convenient to have a basis of the differential space $\Omega(-D+mQ)$ whose elements have pairwise distinct discrete valuations at the place Q, and finding such a basis of $\Omega(-D+mQ)$ reduces to the problem of finding a basis of $\mathcal{L}(D')$ whose elements have pairwise distinct discrete valuations at Q. However, no general algorithm capable of finding such a basis of $\mathcal{L}(D')$ in all cases of interest in coding theory has been proposed yet. In this paper we present an algorithm computing such a basis.

An affine algebraic curve with one rational place Q at infinity is easy to handle and used extensively in the literature (Ganong, 1979; Porter, 1988; Miura, 1992, 1994, 1997, 1998; Porter *et al.*, 1992; Saints and Heegard, 1995). For a divisor D we define $\mathcal{L}(D+\infty Q) := \bigcup_{i=1}^{\infty} \mathcal{L}(D+iQ)$. An affine algebraic curve is said to be *in special position with respect to a place Q of degree one* if its affine coordinate ring is $\mathcal{L}(\infty Q)$ and the pole orders of

*The results in this paper are partly presented without proof in the conference proceedings of 13th AAECC Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes, Hawaii, USA, November 15–19, 1999 (Matsumoto and Miura, 1999)

§E-mail: ryutaroh@ss.titech.ac.jp, WWW: http://tsk-www.ss.titech.ac.jp/~ryutaroh/

0747–7171/00/030309 + 15 $35.00/0

coordinate variables generate the Weierstrass semigroup at Q (Definition 3.1). Under the assumption that we are given defining equations of an affine algebraic curve in special position with respect to Q, we point out that a divisor can be represented as an ideal of $\mathcal{L}(\infty Q)$, and we propose an efficient algorithm to compute a basis of $\mathcal{L}(D)$.

For effective divisors A and B with $\operatorname{supp} A \cap \operatorname{supp} B = \emptyset$ and $Q \notin \operatorname{supp} A \cup \operatorname{supp} B$, there is a close relation between the linear space $\mathcal{L}(A - B + nQ)$ and the fractional ideal $\mathcal{L}(A - B + \infty Q)$ of $\mathcal{L}(\infty Q)$, namely

$$\mathcal{L}(A - B + nQ) = \{f \in \mathcal{L}(A - B + \infty Q) \mid v_Q(f) \geq -n\},$$

where v_Q denotes the discrete valuation at Q. When $A = 0$, by this relation we can compute a basis of $\mathcal{L}(-B + nQ)$ from a generating set of $\mathcal{L}(-B + \infty Q)$ as an ideal of $\mathcal{L}(\infty Q)$ under a mild assumption.

When $A > 0$, we find an effective divisor E such that $-E + n'Q$ is linearly equivalent to $A - B + nQ$, then find a basis of $\mathcal{L}(-E + n'Q)$ from a generating set of the ideal $\mathcal{L}(-E + \infty Q)$, then find a basis of $\mathcal{L}(A - B + nQ)$ from that of $\mathcal{L}(-E + n'Q)$ using the linear equivalence. Computing an ideal basis of $\mathcal{L}(-E + \infty Q)$ from $A - B + nQ$ involves computation of ideal quotients in the Dedekind domain $\mathcal{L}(\infty Q)$, but by clever use of the properties of an affine algebraic curve in special position, our method involves only the Gaussian elimination and a small number of division of polynomials by the Gröbner basis for the ideal defining the curve. Moreover while the other algorithms (Brill and Nöther, 1874; Coates, 1970; Davenport, 1981; Le Brigand and Risler, 1988; Huang and Ierardi, 1994; Volcheck, 1994, 1995; Haché and Le Brigand, 1995; Berry, 1998) except Grayson and Stillman (1998) are applicable only to a plane algebraic curve, our method is applicable to a curve embedded in an affine space of arbitrary dimension. Though the algorithm given in Grayson and Stillman (1998) can be applied to an arbitrary projective nonsingular variety whose homogeneous coordinate ring satisfies Serre's normality criterion S_2 (a definition of S_2 can be found in Eisenbud, 1995, Theorem 11.5), their method involves Buchberger's algorithm that sometimes takes very long computation time.

In Section 2, we clarify the relation between an ideal of the affine coordinate ring of an affine algebraic curve with one rational place at infinity and the linear space $\mathcal{L}(D)$ associated with a divisor D on the curve, and show an algorithm that reduces basis computation of $\mathcal{L}(D)$ to computation of ideal quotients in the affine coordinate ring. In Section 3, we show that an affine algebraic curve with one rational place at infinity has a Gröbner basis with nice structure with respect to a suitable monomial order. In Section 4, we show efficient algorithms computing ideal quotients and a basis of $\mathcal{L}(D)$ from a generating set of the ideal corresponding to D. In Section 5, we give an example computing a basis of $\mathcal{L}(D)$ on the affine algebraic curve in the four-dimensional affine space.

2. Theoretical Basis for Computation

First we fix notations used in this paper. K denotes an arbitrary perfect field. We consider an algebraic function field F/K of one variable. $\mathbf{P}_F$ denotes the set of places in F/K. For a place P, O_P (resp. v_P) denotes the discrete valuation ring (resp. discrete valuation) corresponding to P. Other notations follow those in Stichtenoth's (1993) textbook unless otherwise specified.

In this section, we introduce theorems which play important roles in ideal computation

in the affine coordinate ring of an affine algebraic curve and computation of a basis of $\mathcal{L}(D)$. Hereafter we fix a place Q of degree one in F/K.

2.1. Relation between fractional ideals of a nonsingular affine coordinate ring and divisors in a function field

Definition 2.1. For a divisor D in F/K, we define

$$\mathcal{L}(D+\infty Q) := \bigcup_{i=0}^{\infty} \mathcal{L}(D+iQ).$$

Then $\mathcal{L}(\infty Q)$ is a Dedekind domain, and the set of maximal ideals of $\mathcal{L}(\infty Q)$ is $\{\mathcal{L}(-P+\infty Q) \mid P \in \mathbf{P}_F \setminus \{Q\}\}$. Thus each nonzero ideal can be written uniquely as a product of elements in $\{\mathcal{L}(-P+\infty Q) \mid P \in \mathbf{P}_F \setminus \{Q\}\}$.

Proposition 2.2. *For a divisor D in F/K with $Q \notin \operatorname{supp}(D)$, $\mathcal{L}(-D+\infty Q)$ is a fractional ideal in $\mathcal{L}(\infty Q)$. We have*

$$\mathcal{L}(-D+\infty Q) = \prod_{P \in \mathbf{P}_F} \mathcal{L}(-P+\infty Q)^{v_P(D)}.$$

Proof. $\mathcal{L}(-D+\infty Q)$ being a fractional ideal is trivial. $\mathcal{L}(-D+\infty Q) \supseteq \prod_{P\in\mathbf{P}_F} \mathcal{L}(-P+\infty Q)^{v_P(D)}$ is also obvious.

We shall show that any fractional ideal properly containing $\prod_{P\in\mathbf{P}_F} \mathcal{L}(-P+\infty Q)^{v_P(D)}$ is not $\mathcal{L}(-D+\infty Q)$, which proves the assertion. If I is a fractional ideal properly containing

$$\prod_{P \in \mathbf{P}_F} \mathcal{L}(-P+\infty Q)^{v_P(D)},$$

then there exists a place $R \neq Q$ such that

$$I \supseteq \mathcal{L}(-R+\infty Q)^{-1} \prod_{P \in \mathbf{P}_F} \mathcal{L}(-P+\infty Q)^{v_P(D)}.$$

We set

$$A - B = D - R$$

with both A and B effective divisors and $\operatorname{supp} A \cap \operatorname{supp} B = \emptyset$. For each $S \in \operatorname{supp} A$, we choose t_S by the strong approximation theorem of discrete valuation (Stichtenoth, 1993, Theorem I.6.4) such that

$$\begin{aligned} &v_S(t_S) = 1, \\ &v_P(t_S) = 0, \qquad \forall P \in (\operatorname{supp} A \cup \operatorname{supp} B) \setminus \{S\}, \\ &v_P(t_S) \geq 0, \qquad \forall P \neq Q. \end{aligned}$$

Then $t_S \in \mathcal{L}(-S+\infty Q)$. For each $S \in \operatorname{supp} B$, we choose t_S such that

$$\begin{aligned} &v_S(t_S) = -1, \\ &v_P(t_S) = 0, \qquad \forall P \in (\operatorname{supp} A \cup \operatorname{supp} B) \setminus \{S\}, \\ &v_P(t_S) \geq 0, \qquad \forall P \notin \{Q, S\}. \end{aligned}$$

Then $t_S \in \mathcal{L}(-S+\infty Q)^{-1}$.

$$\prod_{S\in\operatorname{supp} A} t_S^{v_S(A)} \prod_{S\in\operatorname{supp} B} t_S^{v_S(B)} \in \mathcal{L}(-R+\infty Q)^{-1} \prod_{P\in\mathbf{P}_F} \mathcal{L}(-P+\infty Q)^{v_P(D)} \setminus \mathcal{L}(-D+\infty Q). \quad \square$$

COROLLARY 2.3. *Let f be a nonzero element in $\mathcal{L}(\infty Q)$, and $\langle f\rangle$ be the ideal of $\mathcal{L}(\infty Q)$ generated by f. Then*

$$\langle f\rangle = \mathcal{L}(-(f)_0+\infty Q) = \mathcal{L}(-(f)+\infty Q).$$

PROOF. The second equality is obvious. Let D be a divisor such that $\mathcal{L}(-D+\infty Q) = \langle f\rangle$ and $v_Q(D) = 0$. Then $(f)_0 \geq D$. Suppose that there exists a place $P \neq Q$ such that $(f)_0 - P \geq D$. Then by the strong approximation theorem (Stichtenoth, 1993, Theorem I.6.4) we can find an element $g \in \mathcal{L}(-D+\infty Q)$ with $v_P(g) < v_P(f)$, which is a contradiction. $\square$

When I and J are ideals of a ring R, $I : J$ denotes the ideal quotient $\{x \in R \mid xJ \subseteq I\}$.

COROLLARY 2.4. *For two divisors D, E with support disjoint from Q,*

$$\mathcal{L}(-D+\infty Q)\mathcal{L}(-E+\infty Q) = \mathcal{L}(-(D+E)+\infty Q),$$

$$\mathcal{L}(-D+\infty Q) + \mathcal{L}(-E+\infty Q) = \mathcal{L}\left(-\sum_{P\neq Q} \min\{v_P(D), v_P(E)\}P + \infty Q\right),$$

$$\mathcal{L}(-D+\infty Q) \cap \mathcal{L}(-E+\infty Q) = \mathcal{L}\left(-\sum_{P\neq Q} \max\{v_P(D), v_P(E)\}P + \infty Q\right),$$

$$\mathcal{L}(-D+\infty Q) : \mathcal{L}(-E+\infty Q) = \mathcal{L}\left(-\sum_{P\neq Q} \max\{0, v_P(D) - v_P(E)\}P + \infty Q\right).$$

PROOF. The assertion follows from Zariski and Samuel (1975, Theorem 11, Section 5.6). $\square$

COROLLARY 2.5. *Suppose that an ideal $I \subset \mathcal{L}(\infty Q)$ is generated by elements $x_1, \ldots, x_m$. Then I^n is generated by $x_1^n, \ldots, x_m^n$.*

PROOF. Let $\langle x_i\rangle$ be the ideal generated by x_i and $\langle x_i\rangle = \mathcal{L}(-D_i+\infty Q)$. Then

$$I = \mathcal{L}\left(-\sum_{P\neq Q} \min\{v_P(D_i) \mid i = 1, \ldots, m\}P + \infty Q\right).$$

Thus

$$I^n = \mathcal{L}\left(-\sum_{P\neq Q} n\min\{v_P(D_i) \mid i = 1, \ldots, m\}P + \infty Q\right)$$

$$
\begin{aligned}
&= \mathcal{L}\left(-\sum_{P \neq Q} \min\{v_P(nD_i) \mid i = 1, \ldots, m\} P + \infty Q \right) \\
&= \langle x_1^n \rangle + \cdots + \langle x_m^n \rangle \\
&= \langle x_1^n, \ldots, x_m^n \rangle. \quad \square
\end{aligned}
$$

By the facts described so far, we can show a preliminary version of our method for obtaining a basis of $\mathcal{L}(D)$. Let D be a divisor given by

$$D := A - B + nQ,$$

where A and B are effective, $\operatorname{supp} A \cap \operatorname{supp} B = 0$ and $Q \notin \operatorname{supp} A \cup \operatorname{supp} B$. Suppose that generating sets of the ideals $\mathcal{L}(-A + \infty Q)$ and $\mathcal{L}(-B + \infty Q)$ are given. If $A = 0$, then

$$\mathcal{L}(D) = \{x \in \mathcal{L}(-B + \infty Q) \mid v_Q(x) \geq -n\}.$$

From this equation if we have a basis of $\mathcal{L}(-B + \infty Q)$ as a K-linear space with pairwise distinct pole orders at Q, then finding a basis of $\mathcal{L}(D)$ from that of $\mathcal{L}(-B + \infty Q)$ is just selecting elements in the basis of $\mathcal{L}(-B + \infty Q)$ with pole orders $\leq n$. We shall show how to compute such a basis of $\mathcal{L}(-B + \infty Q)$ from a generating set of the ideal $\mathcal{L}(-B + \infty Q)$ in Theorem 4.2.

If $A \neq 0$, then choose a nonzero element $f \in \mathcal{L}(-A + \infty Q)$. Let $\langle f \rangle$ be the ideal generated by f in $\mathcal{L}(\infty Q)$, and

$$I = (\langle f \rangle \mathcal{L}(-B + \infty Q)) : \mathcal{L}(-A + \infty Q).$$

Then

$$
\begin{aligned}
I &= \mathcal{L}(-(f) + \infty Q)\mathcal{L}(-B + \infty Q) : \mathcal{L}(-A + \infty Q) \\
&= \mathcal{L}(A - B - (f) + \infty Q).
\end{aligned}
$$

Since $\mathcal{L}(A - B - (f) + \infty Q)$ is an ordinary ideal of $\mathcal{L}(\infty Q)$, we can compute a basis $\{b_1, \ldots, b_l\}$ of $\mathcal{L}(A - B + nQ - (f))$. Then $b_1/f, \ldots, b_l/f$ is a basis of $\mathcal{L}(D) = \mathcal{L}(A - B + nQ)$. Next we need to compute an ideal quotient in our method. We shall show in Section 4 how to compute an ideal quotient by using only linear algebra.

2.2. MODULES OVER $\mathcal{L}(\infty Q)$

In this subsection we shall study how we can represent an $\mathcal{L}(\infty Q)$-submodule of F.

PROPOSITION 2.6. (HØHOLDT ET AL., 1998, PROOF OF PROPOSITION 3.12) *For a K-subspace W of $\mathcal{L}(\infty Q)$, suppose that there is a subset $\{\alpha_j\}_{j \in v_Q(W \setminus \{0\})} \subset W$ such that $v_Q(\alpha_j) = j$. Then $\{\alpha_j\}_{j \in v_Q(W \setminus \{0\})}$ is a K-basis of W.*

Let $a \in -v_Q(\mathcal{L}(\infty Q) \setminus K)$. Fix an element $x \in F$ such that $(x)_\infty = aQ$.

PROPOSITION 2.7. *For an ideal M of $\mathcal{L}(\infty Q)$, we set $b_i := \min\{j \in -v_Q(M \setminus \{0\}) \mid j \bmod a = i\}$ for $i = 0, \ldots, a-1$. Choose elements $y_i \in M$ such that $v_Q(y_i) = -b_i$. Then $\{y_0, y_1, \ldots, y_{a-1}\}$ generates M as a $K[x]$-module.*

PROOF. It is obvious that

$$\sum_{i=0}^{a-1} K[x]y_i \subseteq M.$$

The set $\{x^j y_i \mid 0 \leq i \leq a-1, 0 \leq j\}$ generates M as a K-vector space by Proposition 2.6, because

$$\begin{aligned} -v_Q(M \setminus \{0\}) &= \{ja + b_i \mid 0 \leq i \leq a-1, 0 \leq j\} \\ &= -v_Q(\{x^j y_i \mid 0 \leq i \leq a-1, 0 \leq j\}). \quad \square \end{aligned}$$

PROPOSITION 2.8. *Notations as in Proposition* 2.7. *If a K-subspace W generates M as a $K[x]$-module; that is, $M = K[x]W$, then we can find the elements y_i in W for $i = 0, \ldots, a-1$.*

PROOF. We can write y_i as

$$y_i = \sum_j a_j x^{n_j} w_j,$$

where $a_j \in K$, $n_j \geq 0$ and $w_j \in W$. Consider terms $a_l x^{n_l} w_l$ such that $v_Q(a_l x^{n_l} w_l) = v_Q(y_i)$. Suppose there is no l such that $n_l = 0$. Then we have

$$v_Q(y_i) = v_Q(x) + v_Q\left(\sum_l a_l x^{n_l - 1} w_l\right),$$

which contradicts the maximality of $v_Q(y_i)$. Thus there is an l such that $n_l = 0$ and we can take $a_l w_l$ as y_i. $\square$

3. Gröbner Bases for an Affine Algebraic Curve with a Unique Rational Place at Infinity

An affine algebraic curve with a unique rational place at infinity is convenient and has been treated by several authors (Ganong, 1979; Porter, 1988; Miura, 1992, 1994, 1997, 1998; Porter *et al.*, 1992; Saints and Heegard, 1995). In this section we review and extend the results in Miura (1997, 1998) and Saints and Heegard (1995).

DEFINITION 3.1. (SAINTS AND HEEGARD, 1995, DEFINITION 11) Let $I \subset K[X_1, \ldots, X_t]$ be an ideal defining an affine algebraic curve, $R := K[X_1, \ldots, X_t]/I$, F be the quotient field of R, and Q be a place of degree one in F/K. Then the affine algebraic curve defined by I is said to be *in special position with respect to Q* if the following conditions are met:

(1) The pole divisor of $X_i \bmod I$ is a multiple of Q for each i.
(2) The pole orders of $X_1 \bmod I$, $X_2 \bmod I, \ldots$, $X_t \bmod I$ at Q generate the Weierstrass semigroup $\{i \mid \mathcal{L}(iQ) \neq \mathcal{L}((i-1)Q)\}$ at Q. In other words, for any $j \in \{i \mid \mathcal{L}(iQ) \neq \mathcal{L}((i-1)Q)\}$ there exists nonnegative integers $l_1, \ldots, l_t$ such that

$$j = \sum_{i=1}^{t} -l_i v_Q(X_i \bmod I).$$

The Weierstrass form of elliptic curves can be considered as a special case of curves in special position.

PROPOSITION 3.2. *Notations as in Definition* 3.1. *Then,* $R = \mathcal{L}(\infty Q)$ *and the affine algebraic curve defined by* I *is nonsingular.*

PROOF. It is clear that $R \subseteq \mathcal{L}(\infty Q)$. Choose nonzero $f \in \mathcal{L}(\infty Q)$. Let $g_{v_Q(f)}$ be an element in R such that $v_Q(g_{v_Q(f)}) = v_Q(f)$, and $c_{v_Q(f)}$ be the element in K such that $v_Q(f - c_{v_Q(f)} g_{v_Q(f)}) > v_Q(f)$. For $v_Q(f) < i \leq 0$ we define g_i and c_i as follows: let $g_i = 0$ if $v_Q(f - (c_{v_Q(f)} g_{v_Q(f)} + \cdots + c_{i-1} g_{i-1})) > i$ and let g_i be an element in R such that $v_Q(g_i) = i$ otherwise. Let c_i be an element in K such that $v_Q(f - (c_{v_Q(f)} g_{v_Q(f)} + \cdots + c_i g_i)) > i$. Then the valuation of $f - (c_{v_Q(f)} g_{v_Q(f)} + \cdots + c_0 g_0)$ at Q is greater than 0. Thus $f - (c_{v_Q(f)} g_{v_Q(f)} + \cdots + c_0 g_0) = 0$ and $f = c_{v_Q(f)} g_{v_Q(f)} + \cdots + c_0 g_0 \in R$, which proves $R = \mathcal{L}(\infty Q)$.

Note next that $\mathcal{L}(\infty Q)$ is the intersection of the discrete valuation rings in F except that of Q. Thus $\mathcal{L}(\infty Q)$ is a holomorphy ring and integrally closed in F (Stichtenoth, 1993, Corollary III.2.8). An affine coordinate ring of an affine algebraic curve is integrally closed in its quotient field if and only if the affine algebraic curve is nonsingular. □

If an algebraic curve is not in special position, then the proposed method cannot be applied to it. We can put an arbitrary algebraic curve into special position using Gröbner bases if we know elements in the function field which have their unique pole at some place Q of degree one and their pole orders generate the Weierstrass semigroup $-v_Q(\mathcal{L}(\infty Q) \setminus \{0\})$ (Saints and Heegard, 1995, p. 1739). However we have to remark that finding such elements is difficult in general. For example, for the towers of function fields found by Garcia and Stichtenoth (1995, 1996), such elements have been found only in a few cases (Haché, 1996; Pellikaan, 1997; Voss and Høholdt, 1997).

In another direction, it is convenient to have a class of algebraic curves known to be in special position. Miura (1997, 1998) found a necessary and sufficient condition for a nonsingular nonrational affine plane curve to be in special position. An affine algebraic set defined by $F(X, Y) = 0$ is a nonsingular nonrational affine algebraic curve in special position with respect to Q if and only if it is nonsingular and

$$F(X, Y) = \alpha_{b,0} X^b + \alpha_{0,a} Y^a + \sum_{ai+bj<ab} \alpha_{i,j} X^i Y^j,$$

where $\alpha_{i,j} \in K$, both $\alpha_{b,0}$ and $\alpha_{a,0}$ are nonzero and a and b are relatively prime positive integers.[†] In this case $v_Q(X \bmod F(X, Y)) = -a$ and $v_Q(Y \bmod F(X, Y)) = -b$. Then he generalized the necessary and sufficient condition for plane curves to be in special position to curves in affine space of arbitrary dimension (Miura, 1997, 1998). Høholdt *et al.* (1998, Example 3.22) also characterized a class algebraic curves in special position with a telescopic Weierstrass semigroup.

Hereafter we use the theory of Gröbner bases. Basic facts in the theory are explained in Cox *et al.* (1996). We introduce the Garcia–Stichtenoth curve used as an example in this paper.

[†]Although all published proofs of this fact are in Japanese, an English version can be found in Matsumoto (1998).

EXAMPLE 3.3. Garcia and Stichtenoth (1995) discovered the tower of algebraic function fields over a finite field that has many rational places, and attains Drinfeld–Vladut bound. The third member F_3 in the tower over the finite field $\mathbf{F}_4$ with four elements is defined by

$$F_3 = \mathbf{F}_4(y_1, z_2, z_3), z_2^2 + z_2 + y_1^3 = 0, z_3^2 + z_3 + (z_2/y_1)^3 = 0.$$

Replacing z_2 with y_1y_2 and z_3 with y_2y_3, we obtain an affine model of F_3 as

$$F_3 = \mathbf{F}_4(y_1, y_2, y_3), y_1y_2^2 + y_2 + y_1^2 = 0, y_2y_3^2 + y_3 + y_2^2 = 0.$$

Let us put the affine algebraic curve defined by the equations $y_1y_2^2 + y_2 + y_1^2 = 0$, $y_2y_3^2 + y_3 + y_2^2 = 0$ into special position. The number of poles of y_1 in F_3 is known to be 1 (Garcia and Stichtenoth, 1995). Let Q be the pole of y_1. Voss and Høholdt (1997) found that

$$\mathcal{L}(\infty Q) = \mathbf{F}_4[y_1, y_1y_2, (y_1y_2 + 1)y_2y_3, y_1^2y_2y_3],$$

and the pole divisors of the generators are

$$(y_1)_\infty = 4Q, (y_1y_2)_\infty = 6Q, ((y_1y_2 + 1)y_2y_3)_\infty = 9Q, (y_1^2y_2y_3)_\infty = 11Q.$$

From this information, we can compute a defining equations of $\mathcal{L}(\infty Q)$ by Eisenbud (1995, Proposition 15.30). Consider the ideal J of $\mathbf{F}_4[Y_1, Y_2, Y_3, X_1, X_2, X_3, X_4]$ generated by

$$Y_1Y_2^2 + Y_2 + Y_1^2, Y_2Y_3^2 + Y_3 + Y_2^2, X_1 - Y_1, X_2 - Y_1Y_2,$$
$$X_3 - (Y_1Y_2 + 1)Y_2Y_3, X_4 - Y_1^2Y_2Y_3,$$

where $X_1, \ldots, X_4$, $Y_1, \ldots, Y_3$ are variables over $\mathbf{F}_4$. Let $I := J \cap \mathbf{F}_4[X_1, X_2, X_3, X_4]$. Then $\mathcal{L}(\infty Q)$ is isomorphic to $\mathbf{F}_4[X_1, X_2, X_3, X_4]/I$. The reduced Gröbner basis for I with respect to the lexicographic monomial order $X_4 > X_3 > X_2 > X_1$ is

$$X_1^3 + X_2 + X_2^2, X_1^3X_2 + X_3 + X_2X_3 + X_3^2, X_2X_3 + X_1X_4,$$
$$X_1^2X_3 + X_4 + X_2X_4, X_1^5 + X_1^2X_2 + X_1^2X_3 + X_3X_4,$$
$$X_1^4 + X_1X_2 + X_1^4X_2 + X_1X_2X_3 + X_4^2.$$

Since the Weierstrass semigroup $-v_Q(\mathcal{L}(\infty Q) \setminus \{0\})$ is generated by $4, 6, 9, 11$ (Voss and Høholdt, 1997), the affine algebraic curve defined by the ideal I is in special position with respect to Q.

Hereafter, $I \subset K[X_1, \ldots, X_t]$ denotes an ideal defining an algebraic curve in special position with respect to a place Q of degree one of the function field F of the curve, unless otherwise stated. We fix a monomial order $\prec$ on $K[X_1, \ldots, X_t]$ induced by the discrete valuation at Q. $\mathbf{N}_0$ denotes the set of nonnegative integers.

DEFINITION 3.4. We define $X_1^{m_1}X_2^{m_2}\cdots X_t^{m_t} \prec X_1^{n_1}X_2^{n_2}\cdots X_t^{n_t}$ if

$$-v_Q(X_1^{m_1}\cdots X_t^{m_t} \bmod I) < -v_Q(X_1^{n_1}\cdots X_t^{n_t} \bmod I),$$

or

$$-v_Q(X_1^{m_1}\cdots X_t^{m_t} \bmod I) = -v_Q(X_1^{n_1}\cdots X_t^{n_t} \bmod I)$$

and $(m_1, \ldots, m_t) <_T (n_1, \ldots, n_t)$ with some total order $<_T$ on $\mathbf{N}_0^t$, which satisfies following conditions:

(1) $(m_1, \ldots, m_t) <_T (n_1, \ldots, n_t)$ whenever $m_1 > n_1$.

(2) If $(m_1, \ldots, m_t) <_T (n_1, \ldots, n_t)$, then $(m_1, \ldots, m_t) + (l_1, \ldots, l_t) <_T (n_1, \ldots, n_t) + (l_1, \ldots, l_t)$ for all $(l_1, \ldots, l_t) \in \mathbf{N}_0^t$.

Definition 3.5. LM denotes the leading monomial of a polynomial with respect to a monomial order. Let $J \subset K[X_1, \ldots, X_t]$ be a nonzero ideal. The delta set $\Delta(J)$ of J with respect to the monomial order is

$$\Delta(J) := \{(n_1, \ldots, n_t) \in \mathbf{N}_0^t \mid X^{n_1} \cdots X^{n_t} \notin \mathrm{LM}(J)\}.$$

For the delta set of an ideal J, the following is known, where X^N denotes $X_1^{n_1} \cdots X_t^{n_t}$ for $N = (n_1, \ldots, n_t)$.

Proposition 3.6. (Cox et al., 1999, p. 229) *$\{X^N \bmod J \mid N \in \Delta(J)\}$ forms a K-basis of $K[X_1, \ldots, X_t]/J$ as a K-vector space.*

The delta set of the defining ideal I of an algebraic curve in special position with respect to a place Q has nice properties. For simplicity we hereafter assume that $v_Q(X_i \bmod I) \neq 0$ for each i.

Definition 3.7.

$$B(\prec) := \{N \in \mathbf{N}_0^t \mid v_Q(X^L \bmod I) = v_Q(X^N \bmod I) \text{ implies } X^N \preceq X^L\}.$$

For each $0 \leq i \leq -v_Q(X_1 \bmod I) - 1$,

$$b_i := \min\{j \in -v_Q(\mathcal{L}(\infty Q) \setminus \{0\}) \mid j \bmod -v_Q(X_1 \bmod I) = i\}.$$

$$T(\prec) := \{N \in B(\prec) \mid \exists i, -v_Q(X^N \bmod I) = b_i\}.$$

Note that if $N, L \in B(\prec)$ and $N \neq L$, then $v_Q(X^N \bmod I) \neq v_Q(X^L \bmod I)$. This implies $\#T(\prec) = -v_Q(X_1 \bmod I)$.

The next proposition is a generalization of Miura (1997, Lemma 5.9 (2) and Lemma 5.13 (1)).

Proposition 3.8.

$$\Delta(I) = B(\prec),$$
$$B(\prec) = \{L + (n, 0, \ldots, 0) \mid L \in T(\prec), n \in \mathbf{N}_0\}.$$

Proof. We first show that $B(\prec) \subseteq \Delta(I)$. Assume that there exists some $N \in B(\prec)$ not belonging to $\Delta(I)$. Then by Proposition 3.6

$$X^N \bmod I = \sum_{L \in \Delta(I)} \alpha_L X^L \bmod I.$$

By the triangle inequality of discrete valuation (Stichtenoth, 1993, Lemma I.1.10), there exists a term $\alpha_L X^L$ in the right-hand side of the above equation such that $v_Q(\alpha_L X^L \bmod I) \leq v_Q(X^N \bmod I)$. Thus the polynomial

$$X^N - \sum_{L \in \Delta(I)} \alpha_L X^L$$

belongs to I but the exponent of its leading monomial belongs to $\Delta(I)$, which is a contradiction.

Conversely, since

$$\{v_Q(X^N \bmod I) \mid N \in B(\prec)\} = v_Q(\mathcal{L}(\infty Q) \setminus \{0\}),$$

by Proposition 2.6 there is no element in $\Delta(I) \setminus B(\prec)$.

To prove the second equality, let $i = j \bmod -v_Q(X_1 \bmod I)$ and $T_i \in T(\prec)$ with $-v_Q(X^{T_i}) = b_i$, for each $j \in -v_Q(\mathcal{L}(\infty Q) \setminus \{0\})$. Then

$$T_i + \left(\frac{j - b_i}{-v_Q(X_1 \bmod I)}, 0, \ldots, 0\right)$$

belongs to $B(\prec)$ since the first component is maximum among $L \in \mathbf{N}_0^t$ with $-v_Q(X^L) = j$, so it is minimum with respect to $\prec$ among exponents L such that $-v_Q(X^L \bmod I) = j$. On the other hand, for given $j \in -v_Q(\mathcal{L}(\infty Q) \setminus \{0\})$ there exists exactly one $N \in B(\prec)$ such that $-v_Q(X^N \bmod I) = j$. □

Example 3.9. We compute $B(\prec)$ and $T(\prec)$ for the curve in Example 3.3. Let $\prec_1$ be the monomial order on $\mathbf{F}_4[X_1, X_2, X_3, X_4]$ such that $X_1^{N_1}X_2^{N_2}X_3^{N_3}X_4^{N_4} \succ_1 X_1^{L_1}X_2^{L_2}X_3^{L_3}X_4^{L_4}$ if $4N_1 + 6N_2 + 9N_3 + 11N_4 > 4L_1 + 6L_2 + 9L_3 + 11L_4$, or $4N_1 + 6N_2 + 9N_3 + 11N_4 = 4L_1 + 6L_2 + 9L_3 + 11L_4$ and $N_i < L_i, N_{i-1} = L_{i-1}, \ldots, N_1 = L_1$ for some positive integer i.

Elements in $B(\prec_1)$ are tabulated below. The upper entry in each box represents an element N in $B(\prec_1)$, and the lower entry the corresponding discrete valuation $-v_Q(X^N \bmod I)$.

$(0,0,0,0)$ 0	$(0,0,1,0)$ 9	$(0,1,0,0)$ 6	$(0,0,0,1)$ 11
$(1,0,0,0)$ 4	$(1,0,1,0)$ 13	$(1,1,0,0)$ 10	$(1,0,0,1)$ 15
$(2,0,0,0)$ 8	$(2,0,1,0)$ 17	$(2,1,0,0)$ 14	$(2,0,0,1)$ 19
$\vdots$	$\vdots$	$\vdots$	$\vdots$

$T(\prec_1)$ consists of the elements in the top row. To see $B(\prec_1) = \Delta(I)$, we compute a Gröbner basis for I with respect to $\prec_1$. The reduced Gröbner basis is

$$X_1^3 + X_2 + X_2^2, X_2X_3 + X_1X_4, X_1^2X_3 + X_4 + X_2X_4,$$
$$X_1^3X_2 + X_3 + X_3^2 + X_1X_4, X_1^5 + X_1^2X_2 + X_1^2X_3 + X_3X_4,$$
$$X_1^4 + X_1X_2 + X_1^4X_2 + X_1^2X_4 + X_4^2.$$

Let $\mathrm{NF}(I)$ be the set of polynomials $F \in K[X_1, \ldots, X_t]$ such that the remainder on division of F by a Gröbner basis for I is F itself. An element $f \in \mathcal{L}(\infty Q)$ is represented in a computer by a polynomial $F \in \mathrm{NF}(I)$ such that $F \bmod I = f$. By Propositions 3.6 and 3.8, $\{X^N \mid N \in B(\prec)\}$ is a K-basis of $\mathrm{NF}(I)$. If $X_1^{n_1}X_2^{n_2} \cdots X_t^{n_t}$ is the leading monomial of $F \in \mathrm{NF}(I)$, then

$$v_Q(F \bmod I) = -a_1n_1 - \cdots - a_tn_t,$$

because the lower terms of F with respect to the monomial order $\prec$ have higher discrete valuations at Q by definition of $B(\prec)$. This easy computation method for discrete valuation is essential in Theorem 4.2.

4. Fast Computation of Ideal Quotients

In this section we show how we can efficiently compute various ideal operations in $\mathcal{L}(\infty Q)$. We retain notations from the previous section and define $a := -v_Q(X_1 \bmod I)$. To make computation most efficient, we have to make $a(\neq 0)$ as small as possible.

4.1. Representation of Ideals

Definition 4.1. For a nonzero ideal $J \subset \mathcal{L}(\infty Q)$, we call $G_0, \ldots, G_{a-1} \in \mathrm{NF}(I)$ a minimum pole order basis for J if:

(1) $G_0 \bmod I, \ldots, G_{a-1} \bmod I$ belong to J.
(2) $-v_Q(G_i \bmod I) = \min\{j \in -v_Q(J \setminus \{0\}) \mid j \bmod a = i\}$.

Note that $G_i \bmod I \neq 0$ for $i = 0, \ldots, a-1$ by definition.

This representation is convenient in computing a basis of $\mathcal{L}(D)$.

Theorem 4.2. *Suppose that B is an effective divisor with $v_Q(B) = 0$ and $G_0, \ldots, G_{a-1}$ is a minimum pole order basis for $\mathcal{L}(-B + \infty Q)$. Then a basis of $\mathcal{L}(-B + nQ)$ is*

$$\{X_1^i G_j \bmod I \mid v_Q(X_1^i G_j \bmod I) \geq -n\}.$$

Proof. The assertion immediately follows from Proposition 2.6. □

We next describe how to compute $G_0, \ldots, G_{a-1}$ from given $F_1, \ldots, F_s \in K[X_1, \ldots, X_t]$ where $F_1 \bmod I, \ldots, F_s \bmod I$ generate J. For simplicity we assume that none of $F_i \bmod I$ is zero.

Let $T_0, \ldots, T_{a-1} \in T(\prec)$ satisfy

$$-v_Q(X^{T_i} \bmod I) = \min\{j \in -v_Q(\mathcal{L}(\infty Q) \setminus \{0\}) \mid j \bmod a = i\}.$$

Then $\{X^{T_i} F_j \bmod I \mid 0 \leq i \leq a-1, 1 \leq j \leq s\}$ generates J as a $K[X_1 \bmod I]$-module since $\{X^{T_i} \bmod I\}$ generates $\mathcal{L}(\infty Q)$ as a $K[X_1 \bmod I]$-module by Proposition 3.8. Let $\{H_l\}$ be the set of remainders on division of $X_{T_i} F_j$ by a Gröbner basis for I for $0 \leq i \leq a-1$ and $1 \leq j \leq s$. Then the K-vector space generated by $H_1, \ldots, H_{sa}$ generates J as a $K[X_1 \bmod I]$-module, and by Proposition 2.8 we can find $G_0, \ldots, G_{a-1}$ from the K-vector space generated by $H_1, \ldots, H_{sa}$. $G_0, \ldots, G_{a-1}$ can be obtained by Gaussian elimination as follows. Let $\{B_1, B_2, \ldots\} = \Delta(I)$ be ordered so that

$$v_Q(X^{B_i} \bmod I) > v_Q(X^{B_{i+1}} \bmod I), \tag{4.1}$$

and define the integer μ by the equation

$$-v_Q(X^{B_\mu} \bmod I) = \max\{-v_Q(H_i \bmod I) \mid i = 1, \ldots, sa\}.$$

Write each polynomial H_i as

$$H_i = m_{i1} X^{B_\mu} + m_{i2} X^{B_{\mu-1}} + \cdots + m_{i\mu} X^{B_1},$$

for $i = 1, \ldots, sa$. Note that $X^{B_1} = 1$. Consider the matrix (m_{ij}). By elementary row operations, we can transform the matrix (m_{ij}) into a form such that for any two nonzero rows the columns of their left-most nonzero elements are different. Let (n_{ij}) be a transformed matrix of (m_{ij}), and

$$E_i := \sum_{j=1}^{\mu} n_{ij} X^{B_{\mu+1-j}}.$$

Since the leading monomials of E_k and E_l are different if $k \neq l$, $v_Q(E_k \bmod I) \neq v_Q(E_l \bmod I)$.

Then $\{v_Q(E_i \bmod I) \mid 1 \leq i \leq sa\}$ equals the set of values of v_Q on the vector space spanned by $H_1 \bmod I, \ldots, H_{sa} \bmod I$. Thus we can choose $G_0, \ldots, G_{a-1}$ as $G_i = E_k \notin I$ where

$$-v_Q(E_k \bmod I) = \min\{j \in \{-v_Q(E_1 \bmod I), \ldots, v_Q(E_{sa} \bmod I)\} \mid j \bmod a = i\}.$$

Since (m_{ij}) is a $\mu \times sa$ matrix, the number of arithmetic operations in K required to compute n_{ij} from m_{ij} is $O(\max\{\mu, sa\}^3)$, and

$$\begin{aligned} \mu &\leq \max\{-v_Q(H_i \bmod I) \mid i = 1, \ldots, sa\} \\ &= \max\{-v_Q(F_i \bmod I) \mid i = 1, \ldots, s\} \\ &\quad + \max\{-v_Q(X^{T_i} \bmod I) \mid i = 1, \ldots, a\}. \end{aligned}$$

These $G_0, \ldots, G_{a-1}$ have the following nice property, which is convenient in computing an ideal quotient.

PROPOSITION 4.3. *Let $\mathcal{G}$ be a Gröbner basis for I. Then $\{G_0, \ldots, G_{a-1}\} \cup \mathcal{G}$ is a Gröbner basis for $I + \langle G_0, \ldots, G_{a-1}\rangle$ where $\langle\cdot\rangle$ denotes the ideal generated by $\cdot$.*

PROOF. To prove the assertion, we shall show that a monomial $X^M \in \mathrm{LM}(I + \langle G_0, \ldots, G_{a-1}\rangle)$ is in the ideal generated by the leading monomials of elements in $\{G_0, \ldots, G_{a-1}\} \cup \mathcal{G}$.

Since $I \subset I + \langle G_0, \ldots, G_{a-1}\rangle$,

$$\Delta(I + \langle G_0, \ldots, G_{a-1}\rangle) \subset \Delta(I).$$

If $X^M \in \mathrm{LM}(I)$ then $X^M \in \langle \mathrm{LT}(\mathcal{G})\rangle$. If $M \in \Delta(I)$ and $X^M \in \mathrm{LM}(I + \langle G_0, \ldots, G_{a-1}\rangle)$, then

$$X^M = X^{T_i} X_1^j,$$

where $i = -v_Q(X^M \bmod I) \bmod a$, $T_i \in T(\prec)$ such that $-v_Q(X^{T_i} \bmod I) \bmod a = i$, and $j = (-v_Q(X^M \bmod I) + v_Q(X^{T_i} \bmod I))/a$, by Proposition 3.8. On the other hand,

$$\mathrm{LM}(G_i) = X^{T_i} X_1^k,$$

where $k = (-v_Q(G_i \bmod I) + v_Q(X^{T_i} \bmod I))/a$. Thus

$$X^M = \mathrm{LM}(G_i) X_1^{j-k}. \quad \square$$

If one want to reduce the effort required to implement our algorithm at the cost of efficiency, there is an alternative approach to compute a minimum pole order basis for J.

PROPOSITION 4.4. *Let $\mathcal{G}$ be a Gröbner basis for $I + \langle F_1, \ldots, F_s\rangle$. Then we can find all*

the elements in a minimum pole order basis for J among $\{$the remainders on division of $X^T H \mid T \in T(\prec)$, $H \in \mathcal{G}\}$.

PROOF. By the definition of Gröbner bases and the monomial order $\prec$, we have

$$\begin{aligned} v_Q(J) &= \{v_Q(H \bmod I) \mid H \in \langle \mathcal{G} \rangle\} \\ &= \{v_Q(X^N H \bmod I) \mid H \in \mathcal{G}, N \in \mathbf{N}_0^t\} \\ &= \{v_Q(X^N H \bmod I) \mid H \in \mathcal{G}, N \in \Delta(I)\} \\ &= \{v_Q(X_1^i X^T H \bmod I) \mid H \in \mathcal{G}, T \in T(\prec), 0 \le i\} \\ &= \{-ia + v_Q(X^T H \bmod I) \mid H \in \mathcal{G}, T \in T(\prec)\}. \end{aligned}$$

Since $\{X^T H \bmod I \mid H \in \mathcal{G},\ T \in T(\prec)\}$ generates J and their remainders belong to $\mathrm{NF}(I)$, the assertion follows. □

4.2. IDEAL QUOTIENT

Suppose that a minimum pole order basis for an ideal $J_1 \subset \mathcal{L}(\infty Q)$ is $\{G_0, \ldots, G_{a-1}\}$, and an ideal $J_2 \subset \mathcal{L}(\infty Q)$ is generated by $\{H_1 \bmod I, \ldots, H_b \bmod I\}$, where $H_i \in K[X_1, \ldots, X_t]$ for each i. We would like to compute a minimum pole order basis for

$$J_1 : J_2 = \{z \in \mathcal{L}(\infty Q) \mid zJ_2 \subseteq J_1\}.$$

Obviously $J_1 \subseteq J_1 : J_2$. Let $F_0, \ldots, F_{a-1}$ be a minimum pole order basis for $J_1 : J_2$. Each F_i is determined by the following algorithm. The set $B(\prec)$ is assumed to be indexed as in equation (4.1).

ALGORITHM 4.5. In this algorithm, variables are integers α, γ, a polynomial `element-in-quotient` $\in K[X_1, \ldots, X_t]$, and a polynomial `candidate` $\in K(\beta_1, \ldots, \beta_{\alpha-1})[X_1, \ldots, X_t]$, where β_j is an indeterminate over K for each j.

(1) Let `element-in-quotient` $= G_i$. Find an integer α such that $B_\alpha \in B(\prec)$ and $X_1 X^{B_\alpha} = \mathrm{LM}(G_i)$. If there is no such α, then set $F_i = G_i$ and terminate the algorithm.

(2) Let `candidate` $= X^{B_\alpha} + \beta_{\alpha-1} X^{B_{\alpha-1}} + \cdots + \beta_1$. Let E_j be the remainder on division of $H_j \times$ `candidate` by $I + \langle G_0, \ldots, G_{a-1} \rangle$. We view E_j as a polynomial in variables $X_1, \ldots, X_t$ over the coefficient field $K(\beta_1, \ldots, \beta_{\alpha-1})$. Since the Gröbner basis for $I + \langle G_0, \ldots, G_{a-1} \rangle$ is contained in $K[X_1, \ldots, X_t]$, each coefficient of E_j is a K-linear combination of $1, \beta_1, \ldots, \beta_{\alpha-1}$.
Let $(\delta_1, \ldots, \delta_{\alpha-1}) \in K^{\alpha-1}$. The element in $\mathcal{L}(\infty Q)$ represented by `candidate` with $(\beta_1, \ldots, \beta_{\alpha-1})$ replaced by $(\delta_1, \ldots, \delta_{\alpha-1})$ belongs to $J_1 : J_2$ if and only if E_j with $(\beta_1, \ldots, \beta_{\alpha-1})$ replaced by $(\delta_1, \ldots, \delta_{\alpha-1})$ is zero for $j = 1, \ldots, b$. Thus we consider the linear system of equations in variable $\beta_1, \ldots, \beta_{\alpha-1}$ such that all coefficient of E_j are zero for $j = 1, \ldots, b$. If the linear system of equations has no solution, then `element-in-quotient` has minimum pole order ℓ at Q among elements in $J_1 : J_2$ such that the remainder of ℓ by a is i. Thus $F_i =$ `element-in-quotient`, and the algorithm terminates.
Else update `element-in-quotient` by `candidate` with $\beta_1, \ldots, \beta_{\alpha-1}$ substituted by a solution of the linear system. Find the integer γ as

$$B_\gamma = B_\alpha - (1, 0, \ldots, 0),$$

update $\alpha = \gamma$ and repeat this process. If there is no such γ, then $F_i =$ `element-in-quotient` and the algorithm terminates.

The number of iteration in the algorithm above to compute each F_i is at most

$$\begin{aligned} & a + \#\,\mathrm{LM}(\langle F_0, \ldots, F_{a-1}\rangle + I) \setminus \mathrm{LM}(\langle G_0, \ldots, G_{a-1}\rangle + I) \\ &= a + \#\Delta(\langle G_0, \ldots, G_{a-1}\rangle + I) \setminus \Delta(\langle F_0, \ldots, F_{a-1}\rangle + I) \\ &= a + \dim(J_1 : J_2)/J_1, \end{aligned}$$

where $(J_1 : J_2)/J_1$ is the factor space of $J_1 : J_2$ modulo J_1. If $J_1 = \mathcal{L}(-A + \infty Q)$ and $J_2 = \mathcal{L}(-B + \infty Q)$ with divisors $A \geq B \geq 0$, then

$$\begin{aligned} \dim(J_1 : J_2)/J_1 &= \mathcal{L}(B - A + \infty Q)/\mathcal{L}(-A + \infty Q) \text{ (by Corollary 2.4)} \\ &= \dim \mathcal{L}(\infty Q)/\mathcal{L}(-A + \infty Q) - \dim \mathcal{L}(\infty Q)/\mathcal{L}(B - A + \infty Q) \\ &= \deg A - (\deg A - \deg B) \text{ (by (Eisenbud, 1995, Exercise 11.13))} \\ &= \deg B. \end{aligned}$$

Remark 4.6. When one does not need efficiency, an ideal quotient can be computed in the standard way described in Cox *et al.* (1996).

5. An Example

Since the curve in Example 3.3 is nonsingular, there is 1–1 correspondence between $\mathbf{F}_4$-rational points and rational places in the function field. Let P_1, P_2 be places corresponding to rational points $(0, 1, 0, 0)$, $(0, 0, 1, 0)$, respectively. In this section we demonstrate how we can compute a basis of $\mathcal{L}(9P_1 - 3P_2)$.

We set $x_i := X_i \bmod I$ for $i = 1, \ldots, 4$. Since $\mathcal{L}(-P_1 + \infty Q) = \langle x_1, x_2 - 1, x_3, x_4\rangle$ and $\mathcal{L}(-P_2 + \infty Q) = \langle x_1, x_2, x_3 - 1, x_4\rangle$, by Corollary 2.5

$$\begin{aligned} \mathcal{L}(-9P_1 + \infty Q) &= \langle x_1^9, (x_2 - 1)^9, x_3^9, x_4^9\rangle, \\ \mathcal{L}(-3P_2 + \infty Q) &= \langle x_1^3, x_2^3, (x_3 - 1)^3, x_4^3\rangle. \end{aligned}$$

A minimum pole order basis for $\langle x_1^9\rangle\mathcal{L}(-3P_2 + \infty Q)$ is

$$X_1^{12}, X_1^9(1 + X_3), X_1^{11} + X_1^9 X_4, X_1^9 X_2.$$

A minimum pole order basis for the ideal quotient $\langle x_1^9\rangle\mathcal{L}(-3P_2 + \infty Q) : \mathcal{L}(-9P_1 + \infty Q) = \mathcal{L}(9P_1 - 3P_2 - (x_1^9) + \infty Q)$ is

$$X_1^6 X_2 + X_1^6 X_3 + X_1^4 X_4, X_1^9 + X_1^6 X_2, X_1^8 + X_1^5 X_2 + X_1^8 X_2, X_1^6 X_2 + X_1^7 X_4.$$

The discrete valuations at Q of above elements modulo I are $-33, -36, -38, -39$. Thus a basis of $\mathcal{L}(9P_1 - 3P_2 - (x_1^9))$ is

$$x_1^6 x_2 + x_1^6 x_3 + x_1^4 x_4, x_1^9 + x_1^6 x_2,$$

and that of $\mathcal{L}(9P_1 - 3P_2)$ is

$$\frac{x_1^6 x_2 + x_1^6 x_3 + x_1^4 x_4}{x_1^9}, \frac{x_1^9 + x_1^6 x_2}{x_1^9}.$$

Acknowledgements

The authors would like to thank Dr Arita at NEC C& C Media Laboratory. He realized Proposition 2.2 in e-mail discussion with Mr Arita on his efficient algorithm performing additions in the Jacobian of an algebraic curve (Arita, 1997).

References

Arita, S. (1997). Publickey cryptosystems with C_{ab} curves (1), Technical Report ISEC97-54, Institute of Electronics, Information and Communication Engineers (Japanese).

Berry, T. G. (1998). Construction of linear systems on hyperelliptic curves. *J. Symb. Comput.*, **26**, 315–327.

Brill, V. A., Nöther, M. (1874). Ueber die algebraischen functionen und ihre anwendung in der geometrie. *Math. Ann.*, **7**, 269–310.

Coates, J. (1970). Construction of rational functions on a curve. *Proc. Cambridge Phil. Soc.*, **68**, 105–123.

Cox, D., Little, J., O'Shea, D. (1996). *Ideals, Varieties, and Algorithms*, 2nd edn. Berlin, Springer-Verlag.

Davenport, J. H. (1981). *On the Integration of Algebraic Functions*, LNCS **102**. Berlin, Springer-Verlag.

Eisenbud, D. (1995). *Commutative Algebra with a View Toward Algebraic Geometry*, volume 150 of *Graduate Texts in Mathematics*. Berlin, Springer-Verlag.

Feng, G. L., Rao, T. R. N. (1993). Decoding algebraic geometric codes up to the designed minimum distance. *IEEE Trans. Inf. Theory*, **39**, 36–47.

Ganong, R. (1979). On plane curves with one place at infinity. *J. Reine Angew. Math.*, **307/308**, 173–193.

Garcia, A., Stichtenoth, H. (1995). A tower of Artin–Schreier extensions of function fields, attaining the Drinfeld–Vladut bound. *Invent. Math.*, **121**, 211–222.

Garcia, A., Stichtenoth, H. (1996). On the asymptotic behaviour of some towers of function fields over finite fields. *J. Number Theory*, **61**, 248–273.

Grayson, D. R., Stillman, M. E. (1998). User's manual of Macaulay2 version 0.8.41. `http://www.math.uiuc.edu/Macaulay2`.

Haché, G. (1996). Construction Effective des Codes Géométriques. Ph.D. Thesis, Univ. Paris VI.

Haché, G., Le Brigand, D. (1995). Effective construction of algebraic geometry codes. *IEEE Trans. Inf. Theory*, **41**, 1615–1628.

Høholdt, T., van Lint, J. H., Pellikaan, R. (1998). Algebraic geometry codes. In Pless, V., Huffman, W. C. eds, *Handbook of Coding Theory*, pp. 871–961. Amsterdam, Elsevier.

Huang, M.-D., Ierardi, D. (1994). Efficient algorithms for the Riemann–Roch problem and for addition in the Jacobian of a curve. *J. Symb. Comput.*, **18**, 519–539.

Le Brigand, D., Risler, J. (1988). Algorithme de Brill–Noether et codes de Goppa. *Bull. Soc. Math. France*, **116**, 231–253.

Matsumoto, R. (1998). The C_{ab} curve. `http://tsk-www.ss.titech.ac.jp/~ryutaroh/cab.html`.

Matsumoto, R., Miura, S. (1999). Computing a basis of $\mathcal{L}(D)$ on an affine algebraic curve with one rational place at infinity. In Fossorier, M. *et al.* ed., *Proceedings of AAECC-13*, LNCS **1719**, pp. 271–281. Berlin, Springer-Verlag.

Matsumoto, R., Miura, S. (2000). On the Feng–Rao bound for the $\mathcal{L}$-construction of algebraic geometry codes. To appear in *IEICE Trans. Fundamentals*, Vol E83-A, no. 5. pp. 923–936, May 2000.

Miura, S. (1992). Algebraic geometric codes on certain plane curves. *Trans. IEICE*, **J75-A**, 1735–1745. (Japanese).

Miura, S. (1994). Constructive theory of algebraic curves. In *Proceedings of the 17th Symposium of Information Theory and its Applications*, pp. 461–464. (Japanese).

Miura, S. (1997). On error-correcting codes based on algebraic geometry. Ph.D. Thesis, University of Tokyo, (Japanese).

Miura, S. (1998). Linear codes on affine algebraic curves. *Trans. IEICE*, **J81-A**, 1398–1421.(Japanese).

Pellikaan, R. (1997). On the missing functions of a pyramid of curves. In *Proceedings of the 35th Allerton Conf. on Communication, Control, and Computing*, pp. 33–40. Urbana-Champaign.

Porter, S. C. (1988). Decoding Codes arising from Goppa's Construction on Algebraic Curves. Ph.D. Thesis, Yale University, New Heaven, CT, USA.

Porter, S. C., Shen, B.-Z., Pellikaan, R. (1992). Decoding geometric Goppa codes using an extra place. *IEEE Trans. Inf. Theory*, **38**, 1663–1676.

Saints, K., Heegard, C. (1995). Algebraic-geometric codes and multidimensional cyclic codes: A unified theory and algorithms for decoding using Gröbner bases. *IEEE Trans. Inf. Theory*, **41**, 1733–1751.

Stichtenoth, H. (1993). *Algebraic Function Fields and Codes*. Berlin, Springer-Verlag.

Volcheck, E. J. (1994). Computing in the Jacobian of a plane algebraic curve. In *Proceedings on Algorithmic Number Theory I*, LNCS **877**. pp. 221–233. Berlin, Springer-Verlag.

Volcheck, E. J. (1995). Addition in the Jacobian of a curve over a finite field. `http://acm.org/~volcheck/`.
Voss, C., Høholdt, T. (1997). An explicit construction of a sequence of codes attaining the Tsfasman–Vlăduţ–Zink bound. *IEEE Trans. Inf. Theory*, **43**, 128–135.
Zariski, O., Samuel, P. (1975). *Commutative Algebra*, volumes 28 and 29 of *Graduate Texts in Mathematics*. Berlin, Springer-Verlag.

Originally Received 25 June 1999
Accepted 18 February 2000