Computing in the Jacobian of a C_{34} curve

Soondug Kim, Yasuo Morita *

1 Introduction

In recent years, certain algebraic curves, for example elliptic curves and hyperelliptic curves, are drawing attention in applications to cryptography. To use algebraic curves in cryptography, we require a fast algorithm on addition in the Jacobian. In elliptic curve cryptosystems, a point of the Jacobian can be uniquely represented by a point of the curve. In hyperelliptic curve cryptosystems, a point of the Jacobian can be uniquely represented by Mumford's form, and the known algorithms on computing in the Jacobian use Mumford's form. S. Miura found a family of algebraic curves named C_{ab} curves, which include elliptic curves and hyperelliptic curves, and S. Arita provided an algorithm on addition in the Jacobian of a C_{ab} curve.

Algebraic curves of large genus suffer efficient attacks such as function sieves and their variants. The genus of a C_{34} curve is 3, and it is the smallest genus of a non-elliptic, non-hyperelliptic C_{ab} curve. For this reason, we study C_{34} curves. Especially, we study the addition in the Jacobian of a C_{34} curve.

In this paper, for a C_{34} curve defined over a perfect field, we give a unique representation on the points of the Jacobian by normal divisors. Further, we express a normal divisor by the reduced Groebner basis with respect to the C_{ab} order for the corresponding ideal of $K[X, Y]$. Such an ideal is called a normal ideal. We give a condition of a polynomial subset to be a reduced Groebner basis for a normal ideal, and we give an explicit expression of the reduced Groebner basis for a given normal ideal. We give the reduced Groebner basis for the normal ideal corresponding to the normal divisor which is linearly equivalent to $-D$ for a given normal divisor D. Finally, we study the sum of normal divisors.

Throughout this paper, K denotes a perfect field and $\overline{K}$ denotes the algebraic closure of K.

*Yasuo Morita: Mathematical Institute, Tohoku University

2 Preliminaries

In this section, we review the Jacobian of an algebraic curve and C_{ab} curves.

2.1 Jacobian of an algebraic curve

Let C be a plane curve defined over K and let $K(C)$ denote the function field of C. Then the divisor group $\mathrm{Div}(C)$ of C is defined to be the free abelian group generated by the points of C. Thus a divisor $D \in \mathrm{Div}(C)$ is a formal sum $D = \sum_{P \in C} n_P P$ with $n_P \in \mathbf{Z}$ and $n_P = 0$ for all but a finite number of $P \in C$. The degree of a divisor $D = \sum_{P \in C} n_P P$ is defined by $\deg D = \sum_{P \in C} n_P$. The divisors of degree 0 form a subgroup $\mathrm{Div}^0(C) = \{D \in \mathrm{Div}(C) \mid \deg D = 0\}$ of $\mathrm{Div}(C)$. Let the Galois group $G_{\overline{K}/K}$ act on $\mathrm{Div}(C)$ as $D^\sigma = \sum_{P \in C} n_P P^\sigma$. Then D is defined over K if and only if $D^\sigma = D$ for all $\sigma \in G_{\overline{K}/K}$. We denote by $\mathrm{Div}_K(C)$ the group of divisors defined over K and put $\mathrm{Div}_K^0(C) = \mathrm{Div}^0(C) \cap \mathrm{Div}_K(C)$. A divisor $D \in \mathrm{Div}(C)$ is principal if it has the form $D = (f) = \sum_{P \in C} \mathrm{ord}_P(f) P$ for some $f \in \overline{K}(C)^*$, where $\mathrm{ord}_P(f)$ denotes the order of f at P. The set of principal divisors of C forms a subgroup of $\mathrm{Div}^0(C)$. Two divisors D_1 and D_2 are linearly equivalent if $D_1 - D_2$ is principal, and it is denoted as $D_1 \sim D_2$. The Jacobian group of C, denoted $J(C)$, is the quotient group of $\mathrm{Div}^0(C)$ by the subgroup of principal divisors. The invariant subgroup $J_K(C)$ of $J(C)$ under the action of $G_{\overline{K}/K}$ is called the Jacobian group of C defined over K.

A divisor $D = \sum_{P \in C} n_P P$ is said to be effective if each $n_P \geq 0$. We write $\sum_{P \in C} n_P P \geq \sum_{P \in C} m_P P$ if $n_P \geq m_P$ holds for any P. For a divisor $D = \sum_{P \in C} n_P P$, $D^+ = \sum_{n_P > 0} n_P P$ and $D^- = \sum_{n_P < 0} (-n_P) P$ are the zero divisor and the pole divisor of D, respectively. For a divisor D defined over K, we set

$$L(D) := \{f \in K(C)^* \mid (f) \geq -D\} \cup \{0\},$$

and we denote the dimension $\dim_K L(D)$ by $l(D)$.

2.2 C_{ab} curves

In this subsection, we review the C_{ab} curves.

Definition 2.1 *Let a and b be relatively prime positive integers. Then a C_{ab} curve defined over K is a nonsingular curve defined by $F(X,Y) = 0$, where $F(X,Y)$ has the form*

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

for nonzero $\alpha_{0,a}, \alpha_{b,0} \in K$.

Since $\gcd(a,b)=1$, we have $m,n \in \mathbf{Z}$ such that $am+bn=1$. Then, multiplying $F(X,Y)$ by $\alpha_{0,a}^{(a-1)bn}\alpha_{b,0}^{-am}$ and replacing X and Y by $\alpha_{0,a}^{-(a-1)n}\alpha_{b,0}^{-n}X$ and $\alpha_{0,a}^{-(m+bn)}\alpha_{b,0}^{m}Y$, respectively, we have a simplified equation $F_1(X,Y)=0$, where

$$F_1(X,Y) := Y^a + X^b + \sum_{ai+bj<ab} \beta_{i,j}X^iY^j \in K[X,Y].$$

Throughout this subsection, let C be a C_{ab} curve defined by $F(X,Y)=0$ with a polynomial $F(X,Y) \in K[X,Y]$. Let $R_K(C)$ denote the coordinate ring of C. Then
(a) C is an absolutely irreducible algebraic curve;
(b) There exists exactly one K-rational place ∞ at infinity, which implies that the degree of ∞ is 1. Furthermore, the pole divisors of X and Y are $a\cdot\infty$ and $b\cdot\infty$, respectively;
(c) For $m \in \mathbf{Z}_{\geq 0}$, $\{X^iY^j \bmod F(X,Y) \mid 0 \leq i, 0 \leq j \leq a-1, ai+bj \leq m\}$ is a basis of a vector space $L(m\cdot\infty)$ over K.

For a fixed monomial order on $K[X,Y]$, the multidegree $\mathrm{MD}(f)$ of a polynomial $f = \sum_\alpha a_\alpha X^{\alpha_1}Y^{\alpha_2}$ is $\max\{\alpha = (\alpha_1,\alpha_2) \in \mathbf{Z}_{\geq 0}^2 \mid a_\alpha \neq 0\}$, where the maximum is taken with respect to the monomial order. For a polynomial f, we let $\mathrm{LC}(f), \mathrm{LM}(f)$ and $\mathrm{LT}(f)$ denote the leading coefficient, the leading monomial and the leading term of f, respectively. For a nonempty subset G of $K[X,Y]$, we let $\mathrm{LT}(G)$ and $\mathrm{LM}(G)$ denote the set of leading terms and the set of leading monomials of elements of G, respectively.

Now, we recall the definition of Groebner bases.

Definition 2.2 *Fix a monomial order. A finite subset $G=\{g_1,\ldots,g_t\}$ of an ideal I in $K[X,Y]$ is called a Groebner basis if $\langle \mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_t)\rangle = \langle \mathrm{LT}(I)\rangle$. In particular, a Groebner basis satisfying*
(i) $\mathrm{LC}(g)=1$ *for all* $g \in G$,
(ii) *For $g \in G$, any term of g is not in $\langle \mathrm{LT}(G-\{g\})\rangle$*
is called a reduced Groebner basis.

Fix a monomial order on $K[X,Y]$ and let $I \neq \{0\}$ be an ideal in $K[X,Y]$. Then I has a unique reduced Groebner basis. Furthermore, any Groebner basis for I generates I. On division by a Groebner basis G, the remainder is uniquely determined no matter how the elements of G are listed.

We introduce the monomial order named C_{ab} order, which is of great significance in C_{ab} curves.

Definition 2.3 (**C_{ab} order**) *Let a and b be relatively prime positive integers with $a<b$. For $\alpha=(\alpha_1,\alpha_2), \beta=(\beta_1,\beta_2) \in \mathbf{Z}_{\geq 0}^2$, we write $\alpha > \beta$ if*

$$a\alpha_1 + b\alpha_2 > a\beta_1 + b\beta_2, \quad \text{or} \quad a\alpha_1 + b\alpha_2 = a\beta_1 + b\beta_2 \text{ and } \alpha_1 < \beta_1.$$

It is easily known that this monomial order corresponds to pole degrees of functions in $R_K(C)$. We use only this monomial order in this paper.

We consider representations of $J_K(C)$. Let $g(C)$ denote the genus of C.

Definition 2.4 *A divisor $D = E - n \cdot \infty \in \mathrm{Div}^0_K(C)$ with an effective divisor E prime to ∞ and $0 \leq n \leq g(C)$ is called a semi-normal divisor. In particular, a semi-normal divisor $D = E - n \cdot \infty$ such that $n = \min\{n' \mid E' - n' \cdot \infty \sim D, E' \geq 0\}$ is called a normal divisor.*

It is possible that a semi-normal divisor may be linearly equivalent to another semi-normal divisor. But, every divisor $D \in \mathrm{Div}^0_K(C)$ has a unique normal divisor D_n such that $D_n \sim D$. In fact, $D_n = D + (f)$ for a nonzero function $f \in L(D + m \cdot \infty)$ with the smallest integer m such that $l(D + m \cdot \infty) = 1$. In particular, for a divisor $D = D^+ - n \cdot \infty \in \mathrm{Div}^0_K(C)$, the normal divisor D' such that $D' \sim -D$ is $-D + (f)$ for a nonzero function $f \in L(-D + m \cdot \infty)$ with the smallest integer m such that $l(-D + m \cdot \infty) = 1$. It implies that $D' = -D + (f)$ for a nonzero function $f \in R_K(C)$ with the smallest pole degree such that $(f)^+ \geq D^+$.

The Jacobian group $J_K(C)$ is isomorphic to the ideal class group $H(R_K(C))$ of $R_K(C)$ by the isomorphism

$$\begin{array}{rccl} \Phi : & J_K(C) & \longrightarrow & H(R_K(C)) \\ & [E - \deg E \cdot \infty] & \longmapsto & [L(\infty \cdot \infty - E)], \end{array}$$

where, for any class $[D]$ in $J_K(C)$, we choose an effective divisor E which satisfies that $D \sim E - \deg E \cdot \infty$. For a divisor $D \in \mathrm{Div}^0_K(C)$ with the pole points only at infinity, we denote by I_D the ideal $L(\infty \cdot \infty - D^+)$ of $R_K(C)$.

Next,we consider the homomorphism

$$\begin{array}{rccl} \varphi : & K[X,Y] & \longrightarrow & R_K(C) \\ & f(X,Y) & \longmapsto & f(X,Y) \bmod F(X,Y). \end{array}$$

It is well-known that every ideal I of $R_K(C)$ is one-to-one correspondent to an ideal $\varphi^{-1}(I)$ of $K[X,Y]$ containing $\ker \varphi = \langle F(X,Y) \rangle$. For a normal divisor $D \in \mathrm{Div}^0_K(C)$, we call the ideal $\varphi^{-1}(I_D)$ of $K[X,Y]$ a normal ideal of C.

For an ideal I of $K[X,Y]$, we define $\Delta(I)$ as $\{X^iY^j \in K[X,Y] \mid X^iY^j \notin \mathrm{LM}(I)\}$ and we let $\delta(I)$ denote the number of elements in $\Delta(I)$. For a subset $G = \{g_1, \ldots, g_m\}$ of $K[X,Y]$, we define $\Delta(G)$ as $\{X^iY^j \mid (i,j) \in \mathbf{Z}^2_{\geq 0} - \cup_{i=1}^m (\mathrm{MD}(g_i) + \mathbf{Z}^2_{\geq 0})\}$ and we let $\delta(G)$ denote the number of elements in $\Delta(G)$. Then, for a subset $G = \{g_1, \ldots, g_t\}$ of an ideal I satisfying $\delta(I) < \infty$, G is a Groebner basis for I if and only if $\delta(I) = \delta(G)$.

Now, we quote the following, which plays an important role in this paper:

Proposition 2.5 *For a divisor $D = E - n \cdot \infty \in \mathrm{Div}_K^0(C)$ with an effective divisor E prime to ∞, we have*

$$\deg E = \delta(I),$$

where I is the ideal $\varphi^{-1}(I_D)$ of $K[X,Y]$.

3 C_{34} curves

In this section, we consider C_{34} curves. Throughout this section, let C be a C_{34} curve defined by

$$F(X,Y) := Y^3 + \gamma_2(X)Y + \gamma_3(X) = 0$$

with $\gamma_2(X) = s_2X^2 + s_1X + s_0, \gamma_3(X) = X^4 + t_3X^3 + t_2X^2 + t_1X + t_0 \in K[X]$. Then the genus of C is equal to 3.

3.1 Normal divisors

In this subsection, we give a condition for a semi-normal divisor to be a normal divisor of C. The pole divisors of X and Y in $R_K(C)$ are $3 \cdot \infty$ and $4 \cdot \infty$, respectively. It follows that:

Lemma 3.1 *Let a, b, c be elements of K. Then the principal divisor $(X+a)$ can be written as $(X+a) = P_1+P_2+P_3-3\cdot\infty$ with $P_1, P_2, P_3 \in C$, and the principal divisor $(Y+bX+c)$ can be written as $(Y + bX + c) = Q_1 + Q_2 + Q_3 + Q_4 - 4 \cdot \infty$ with $Q_1, Q_2, Q_3, Q_4 \in C$.*

The following proposition gives a condition for a semi-normal divisor $D \in \mathrm{Div}_K^0(C)$ to be a normal divisor.

Proposition 3.2 *Let $D \in \mathrm{Div}_K^0(C)$ be a semi-normal divisor and let $n = \deg D^+$. Then D is a normal divisor if and only if either*
(i) $0 \leq n \leq 2$, *or*
(ii) $n = 3$ *and I_D contains no function of the form $X + a$ or $Y + bX + c$ for $a, b, c \in K$.*

Proof. The semi-normal divisor D is a normal divisor if and only if D is not linearly equivalent to any semi-normal divisor with a pole degree which is smaller than n.

If $n = 0$, then $D = 0$ is a normal divisor.

If $n = 1$ and D is not a normal divisor, then $D \sim 0$. It follows that $D = (f)$ for some $f \in K(C)^*$. Then f is in $L(1 \cdot \infty) - L(0 \cdot \infty)$. But it is a contradition because $L(1 \cdot \infty) - L(0 \cdot \infty) = \emptyset$.

If $n = 2$ and D is not a normal divisor, then $D \sim 0$ or $D \sim P - \infty$ for a point $P \in C$. First, it is impossible that $D \sim 0$, since $L(2 \cdot \infty) - L(1 \cdot \infty) = \emptyset$. Second, suppose that

$D \sim P - \infty$ for $P = (x, y) \in C$. Then $D - P + \infty = (f)$ for some $f \in K(C)^*$. Since $(f)+(X-x) = D^+ + P_2 + P_3 - 4\cdot\infty$ for $P_2, P_3 \in C$ such that $(X-x) = P+P_2+P_3-3\cdot\infty$. It follows that the function $f\cdot(X-x) \in L(4\cdot\infty)-L(3\cdot\infty)$. This implies that $(f\cdot(X-x)) = (Y + bX + c)$ for $b, c \in K$. Thus we have $Y + bX + c, X - x \in L(\infty\cdot\infty - (P_2 + P_3))$. It is a contradiction because there is only one line through with P_1 and P_2, which is the tangent line if $P_1 = P_2$.

If $n = 3$ and D is not a normal divisor, then $D \sim 0$, $D \sim P-\infty$, or $D \sim Q_1+Q_2-2\cdot\infty$ for $P, Q_1, Q_2 \in C$. First, suppose that $D \sim 0$. Then $D = (f)$ for some $f \in K(C)^*$. It follows that $f \in L(3\cdot\infty) - L(2\cdot\infty)$. This implies that $(f) = (X + a)$, i.e. $X + a \in I_D$, for $a \in K$. Second, suppose that $D \sim P - \infty$. Then $D - P + \infty = (f)$ for some $f \in K(C)^*$. For $P = (x, y) \in C$, $(f) + (X - x) = D^+ + P_2 + P_3 - 5\cdot\infty$ for $P_2, P_3 \in C$ such that $(X-x) = P+P_2+P_3-3\cdot\infty$. It follows that $f\cdot(X-x) \in L(5\cdot\infty)-L(4\cdot\infty) = \emptyset$, which is a contradiction. Last, suppose that $D \sim Q_1+Q_2-2\cdot\infty$. Then $D-Q_1-Q_2+2\cdot\infty = (f)$ for some $f \in K(C)^*$. Let g be the defining equation of the line through with Q_1 and Q_2, which is the tangent line if $Q_1 = Q_2$. Then either $g = X+a$ for $a \in K$ or $g = Y+bX+c$ for $b, c \in K$. For $g = Y+bX+c$, we can write $(g) = Q_1+Q_2+Q_3+Q_4-4\cdot\infty$ for $Q_3, Q_4 \in C$. Then $(fg) = D^+ + Q_3 + Q_4 - 5\cdot\infty$, which is a contradiction since $L(5\cdot\infty) - L(4\cdot\infty) = \emptyset$. Thus $g = X+a$. Let $(g) = Q_1+Q_2+Q_5-3\cdot\infty$ for $Q_5 \in C$. Then $(fg) = D^+ + Q_5 - 4\cdot\infty$. It follows that $fg \in L(4\cdot\infty)-L(3\cdot\infty)$. Thus $(fg) = (Y+b'X+c')$, i.e. $Y+b'X+c' \in I_D$, for $b', c' \in K$. Therefore, we proved that if D is not a normal divisor, there is a function $f \in I_D$ of the form $X + a$ or $Y + bX + c$ for $a, b, c \in K$.

Conversely, if $n = 3$ and there is a function $f = X + a \in I_D$ for $a \in K$. Then we have $(f)^+ = D^+$, since $(f)^+ \geq D^+$ with $\deg(f)^+ = \deg D^+$. It implies that $(f) = D$, and $D \sim 0$. Thus D is not a normal divisor. If $n = 3$ and there is a function $f = Y + bX + c \in I_D$ for $b, c \in K$, then $(f) = D^+ + P - 4\cdot\infty$ for $P = (x, y) \in C$. It follows that $D-(f)+(X-x) = P_2+P_3-2\cdot\infty$ for $P_2, P_3 \in C$ such that $(X-x) = P+P_2+P_3-3\cdot\infty$. It implies that $D \sim P_1 + P_2 - 2\cdot\infty$. Thus D is not a normal divisor. □

3.2 A Groebner basis for a normal ideal

In this subsection, we give a condition of an ideal of $K[X, Y]$ to be a normal ideal of C, and a condition of a polynomial subset of $K[X, Y]$ to be a reduced Groebner basis for a normal ideal of C. Furthermore, we give an expression of the reduced Groebner basis for a normal divisor $D = \sum P_i - n\cdot\infty \in \mathrm{Div}_K^0(C)$.

The following lemma, which is followed from Proposition 3.2, states a condition of a polynomial ideal to be a normal ideal of C, i.e. $\varphi^{-1}(L(\infty\cdot\infty - D^+))$ for a normal divisor $D \in \mathrm{Div}_K^0(C)$.

Lemma 3.3 *Let $I \neq \{0\}$ be an ideal in $K[X, Y]$ and let G be the reduced Groebner basis for I. Then I is a normal ideal of C if and only if G satisfies the following two conditions:*

(a) *The remainder* $\overline{F}^G$ *of* $F(X,Y)$ *on division by* G *is* 0*;*
(b) *Either* $0 \le \delta(G) \le 2$*, or* $\delta(G) = 3$ *and* $\mathrm{LM}(G) = \{X^2, XY, Y^2\}$.

It follows that a polynomial subset $G \neq \{0\}$ of $K[X,Y]$ is the reduced Groebner basis for a normal ideal of C if and only if G is the reduced Groebner basis satisfying the conditions (a), (b) of Lemma 3.3. Thus we have:

Proposition 3.4 *Let* $G \neq \{0\}$ *be a polynomial subset of* $K[X,Y]$*. Let* a_i, b_i, c_i *be elements of* K*. Then* G *is a reduced Groebner basis for a normal ideal of* C *if and only if* G *is one of the following:*
(a) $G = \{1\}$;
(b) $G = \{g_1(X,Y) = X + c_1, g_2(X,Y) = Y + c_2\}$ *and satisfies* $F(-c_1, -c_2) = 0$*;*
(c) $G = \{g_1(X,Y) = X + c_1, g_2(X,Y) = Y^2 + a_2Y + c_2\}$ *and satisfies* $g_2(X,Y) \mid F(-c_1, Y)$*;*
(d) $G = \{g_1(X,Y) = Y + b_1X + c_1, g_2(X,Y) = X^2 + b_2X + c_2\}$ *and satisfies* $g_2(X,Y) \mid F(X, -b_1X - c_1)$*;*
(e) $G = \{g_1(X,Y), g_2(X,Y), g_3(X,Y)\}$ *for*

$$\begin{aligned} g_1(X,Y) &= X^2 + a_1Y + b_1X + c_1, \\ g_2(X,Y) &= XY + a_2Y + b_2X + c_2, \\ g_3(X,Y) &= Y^2 + a_3Y + b_3X + c_3, \end{aligned}$$

satisfying

$$\begin{aligned} c_1 &= -a_2^2 + a_2b_1 - a_1b_2 + a_1a_3, \\ c_2 &= a_2b_2 - a_1b_3, \\ c_3 &= -a_2b_3 - b_2^2 + a_3b_2 + b_1b_3, \end{aligned}$$

and

$$\begin{aligned} a_1 \neq 0 &\Rightarrow g_2(X, f(X)) \mid F(X, f(X)), \\ b_3 \neq 0 &\Rightarrow g_2(g(Y), Y) \mid F(g(Y), Y), \\ a_1 = b_3 = 0 &\Rightarrow g_1(X,Y) \mid F(X, -b_2),\ g_3(X,Y) \mid F(-a_2, Y), \end{aligned}$$

where $f(X) = -a_1^{-1}(X^2 + b_1X + c_1)$ *and* $g(Y) = -b_3^{-1}(Y^2 + a_3Y + c_3)$.

Proof. Let $\overline{F}^G$ denote the remainder of $F(X,Y)$ on division by G. Then it is enough to find a reduced Groebner basis G such that $\overline{F}^G$ is equal to 0, and $\mathrm{LM}(G)$ is $\{1\}$, $\{X,Y\}$, $\{X,Y^2\}$, $\{Y,X^2\}$, or $\{X^2,XY,Y^2\}$ by Lemma 3.3. We wish to find a condition that $\overline{F}^G = 0$ is satisfied by a reduced Groebner basis G with a set of leading monomials of the above form.

(a) If G is a reduced Groebner basis with $\mathrm{LM}(G) = \{1\}$, then $G = \{1\}$.

(b) If G is a reduced Groebner basis with $\mathrm{LM}(G) = \{X,Y\}$, then the elements of G are $g_1(X,Y) = X + c_1, g_2(X,Y) = Y + c_2$ for $c_1, c_2 \in K$. For the remainder $\overline{F}^G = r_0 \in K$, we can write

$$F(X,Y) = q_1(X,Y)g_1(X,Y) + q_2(X,Y)g_2(X,Y) + r_0,$$

with $q_1(X,Y), q_2(X,Y) \in K[X,Y]$. Thus $\overline{F}^G = 0$ if and only if $F(-c_1,-c_2) = 0$.

(c) If G is a reduced Groebner basis with $\mathrm{LM}(G) = \{X, Y^2\}$, then the elements of G are $g_1(X,Y) = X + c_1, g_2(X,Y) = Y^2 + a_2Y + c_2$ for $a_2, c_1, c_2 \in K$. For the remainder $\overline{F}^G = r_1Y + r_0$, we can write

$$F(X,Y) = q_1(X,Y)g_1(X,Y) + q_2(X,Y)g_2(X,Y) + r_1Y + r_0$$

with $q_1(X,Y), q_2(X,Y) \in K[X,Y]$. Since

$$F(-c_1,Y) = q_2(-c_1,Y)g_2(-c_1,Y) + r_1Y + r_0,$$

the remainder of $F(-c_1,Y)$ on division by $g_2(-c_1,Y)$ is $r_1Y + r_0$. Thus $\overline{F}^G = 0$ if and only if $F(-c_1,Y)$ is divisible by $g_2(-c_1,Y) = g_2(X,Y)$.

(d) If G is a reduced Groebner basis with $\mathrm{LM}(G) = \{Y, X^2\}$, then the elements of G are $g_1(X,Y) = Y + b_1X + c_1, g_2(X,Y) = X^2 + b_2X + c_2$ for $b_1, b_2, c_1, c_2 \in K$. For the remainder $\overline{F}^G = r_1X + r_0$, we can write

$$F(X,Y) = q_1(X,Y)g_1(X,,Y) + q_2(X,Y)g_2(X,Y) + r_1X + r_0$$

with $q_1(X,Y), q_2(X,Y) \in K[X,Y]$. Since

$$F(X,-b_1X-c_1) = q_2(X,-b_1X-c_1)g_2(X,-b_1X-c_1) + r_1X + r_0,$$

the remainder of $F(X,-b_1X-c_1)$ on division by $g_2(X,-b_1X-c_1)$ is $r_1X + r_0$. Thus $\overline{F}^G = 0$ if and only if $F(X,-b_1X-c_1)$ is divisible by $g_2(X,-b_1X-c_1) = g_2(X,Y)$.

(e) If G is a reduced Groebner basis with $\mathrm{LM}(G) = \{X^2, XY, Y^2\}$, then G has the elements

$$\begin{aligned} g_1(X,Y) &= X^2 \quad +a_1Y + b_1X + c_1, \\ g_2(X,Y) &= XY \quad +a_2Y + b_2X + c_2, \\ g_3(X,Y) &= Y^2 \quad +a_3Y + b_3X + c_3, \end{aligned}$$

with $a_i, b_i, c_i \in K$ for $i = 1,2,3$ satisfying that the remainder of S-polynomial

$$S(g_j(X,Y), g_k(X,Y)) = \mathrm{lcm}(\mathrm{LM}(g_j), \mathrm{LM}(g_k)) \left(\frac{g_j(X,Y)}{\mathrm{LT}(g_j(X,Y))} - \frac{g_k(X,Y)}{\mathrm{LT}(g_k(X,Y))} \right),$$

on division by G is equal to 0 for all $1 \le j \ne k \le 3$, where $\mathrm{lcm}(\mathrm{LM}(g_j), \mathrm{LM}(g_k))$ denotes the least common multiple of $\mathrm{LM}(g_j(X,Y))$ and $\mathrm{LM}(g_k(X,Y))$. It follows that

$$\begin{aligned} c_1 &= -a_2^2 + a_2b_1 - a_1b_2 + a_1a_3, \\ c_2 &= a_2b_2 - a_1b_3, \\ c_3 &= -a_2b_3 - b_2^2 + a_3b_2 + b_1b_3. \end{aligned} \tag{2.1}$$

For the remainder $\overline{F}^G = r_2Y + r_1X + r_0$, we can write

$$\begin{aligned} F(X,Y) = \; & q_1(X,Y)g_1(X,Y) + q_2(X,Y)g_2(X,Y) + q_3(X,Y)g_3(X,Y) \\ & +r_2Y + r_1X + r_0 \end{aligned} \tag{2.2}$$

with $q_1(X,Y), q_2(X,Y), q_3(X,Y) \in K[X,Y]$.

If $a_1 \neq 0$, (2.2) can be written as

$$F(X,Y) = q_1'(X,Y)g_1(X,Y) + q_2'(X,Y)g_2(X,Y) + r_2Y + r_1X + r_0$$

for $q_1'(X,Y), q_2'(X,Y) \in K[X,Y]$, since $g_3(X,Y) = a_1^{-1}(Y+b_2)g_1(X,Y) - a_1^{-1}(X - a_2 + b_1)g_2(X,Y)$. If we substitute $f(X) = -a_1^{-1}(X^2 + b_1X + c_1)$ for Y, then

$$F(X, f(X)) = q_2'(X, f(X))g_2(X, f(X)) + r_2f(X) + r_1X + r_0.$$

It follows that the remainder of $F(X, f(X))$ on division by $g_2(X, f(X))$ is $r_2f(X)+r_1X+r_0$. Thus $\overline{F}^G = 0$ if and only if $F(X, f(X))$ is divisible by $g_2(X, f(X))$.

If $b_3 \neq 0$, (2.2) can be written as

$$F(X,Y) = q_2''(X,Y)g_2(X,Y) + q_3''(X,Y)g_3(X,Y) + r_2Y + r_1X + r_0$$

for $q_2''(X,Y), q_3''(X,Y) \in K[X,Y]$, since $g_1(X,Y) = -b_3^{-1}(Y - b_2 + a_3)g_2(X,Y) + b_3^{-1}(X + a_2)g_3(X,Y)$. If we substitute $g(Y) = -b_3^{-1}(Y^2 + a_3Y + c_3)$ for X, then

$$F(g(Y), Y) = q_2''(g(Y), Y)g_2(g(Y), Y) + r_2Y + r_1g(Y) + r_0.$$

It follows that the remainder of $F(g(Y), Y)$ on division by $g_2(g(Y), Y)$ is $r_2Y+r_1g(Y)+r_0$. Thus $\overline{F}^G = 0$ if and only if $F(g(Y), Y)$ is divisible by $g_2(g(Y), Y)$.

If $a_1 = b_3 = 0$, then

$$\begin{aligned} g_1(X,Y) &= (X+a_2)(X-a_2+b_1), \\ g_2(X,Y) &= (X+a_2)(Y+b_2), \\ g_3(X,Y) &= (Y+b_2)(Y-b_2+a_3) \end{aligned}$$

by (2.1). Applying them in (2.2), we have

$$F(-a_2, Y) = q_3(-a_2, Y)g_3(-a_2, Y) + r_2Y - a_2r_1 + r_0$$

and

$$F(X, -b_2) = q_1(X, -b_2)g_1(X, -b_2) + r_1X - b_2r_2 + r_0.$$

Thus $\overline{F}^G = 0$ if and only if $g_3(X,Y) \mid F(-a_2, Y)$ and $g_1(X,Y) \mid F(X, -b_2)$. □

The following is on the reduced Groebner basis for a given normal divisor.

Theorem 3.5 *Let $D = \sum_{i=1}^n P_i - n \cdot \infty \in \mathrm{Div}_K^0(C)$ be a normal divisor, where $P_i = (x_i, y_i) \in C$ for $i = 1, \ldots, n$. Let*

$$l(X,Y) = \begin{cases} (x_2 - x_1)(Y - y_1) - (y_2 - y_1)(X - x_1) & \text{if } P_1 \neq P_2; \\ F_Y(x,y)(Y-y) + F_X(x,y)(X-x) & \text{if } P_1 = P_2 = (x,y), \end{cases}$$

where F_X (resp. F_Y) denotes the partial derivative of $F(X,Y)$ with respect to X (resp. Y). Let I be the normal ideal $\varphi^{-1}(I_D)$ and let G be the reduced Groebner basis for I. Then G satisfies the following:
(a) *If $D=0$, then $G=\{1\}$;*
(b) *If $D=P_1-\infty$, then $G=\{X-x_1, Y-y_1\}$;*
(c) *If $D=P_1+P_2-2\cdot\infty$, then*
(i) $\mathrm{LM}(l(X,Y))=X$*: $G=\{l_m(X,Y),(Y-y_1)(Y-y_2)\}$;*
(ii) $\mathrm{LM}(l(X,Y))=Y$*: $G=\{l_m(X,Y),(X-x_1)(X-x_2)\}$,*
where $l_m(X,Y)=\mathrm{LC}(l(X,Y))^{-1}l(X,Y)$.
(d) *If $D=P_1+P_2+P_3-3\cdot\infty$, then $G=\{g_1(X,Y),g_2(X,Y),g_3(X,Y)\}$ with*

$$
\begin{aligned}
g_1(X,Y) &= (X-x_1)(X-x_2)+k_1 l(X,Y),\\
g_2(X,Y) &= (X-x_1)(Y-y_2)+k_2 l(X,Y),\\
g_3(X,Y) &= (Y-y_1)(Y-y_2)+k_3 l(X,Y),
\end{aligned}
$$

for
(i) *if $\sharp\{P_1,P_2,P_3\}=2$ or 3, then we can assume that $P_3\neq P_1,P_2$ and we have*

$$
\begin{aligned}
k_1 &= -l(x_3,y_3)^{-1}(x_3-x_1)(x_3-x_2),\\
k_2 &= -l(x_3,y_3)^{-1}(x_3-x_1)(y_3-y_2),\\
k_3 &= -l(x_3,y_3)^{-1}(y_3-y_1)(y_3-y_2);
\end{aligned}
$$

(ii) *if $\sharp\{P_1,P_2,P_3\}=1$, then*

$$
\begin{aligned}
k_1 &= (S_0^2T_2+3yT_1^2-S_0S_1T_1)^{-1}S_0^2,\\
k_2 &= -(S_0^2T_2+3yT_1^2-S_0S_1T_1)^{-1}S_0T_1,\\
k_3 &= (S_0^2T_2+3yT_1^2-S_0S_1T_1)^{-1}T_1^2,
\end{aligned}
$$

for

$$
\begin{aligned}
S_0 &= 3y^2+s_2x^2+s_1x+s_0,\\
S_1 &= 2s_2x+s_1,\\
T_1 &= 2s_2xy+s_1y+4x^3+3t_3x^2+2t_2x+t_1,\\
T_2 &= s_2y+6x^2+3t_3x+t_2,
\end{aligned}
$$

where $\sharp\{P_1,P_2,P_3\}$ denotes the number of elements in $\{P_1,P_2,P_3\}$.

Proof. For the reduced Groebner basis G for I, we have $\delta(G)=\delta(I)=n$.
(a) If $D=0$, then $\delta(G)=0$. It follows that $\mathrm{LM}(G)=\{1\}$. Thus $G=\{1\}$.
(b) If $D=P_1-\infty$, then $\delta(G)=1$. Thus $\mathrm{LM}(G)=\{X,Y\}$ and

$$G=\{g_1(X,Y)=X+c_1, g_2(X,Y)=Y+c_2\}$$

for $c_1,c_2\in K$. Since $(g_1)^+,(g_2)^+\geq P_1$, we have $c_1=-x_1$, $c_2=-y_1$.

(c) If $D = P_1 + P_2 - 2 \cdot \infty$, then $\delta(G) = 2$. Thus $\mathrm{LM}(G) = \{X, Y^2\}$ or $\{Y, X^2\}$. For the linear polynomial $l(X,Y)$, we have $l(X,Y) \in I$ and $(X - x_1)(X - x_2), (Y - y_1)(Y - y_2) \in I$. The reduced Groebner basis G are obtained from a Groebner basis $\{l(X,Y), (X - x_1)(X - x_2), (Y - y_1)(Y - y_2)\}$ for I.

(d) If $P_1 + P_2 + P_3 - 3 \cdot \infty$, then $\delta(G) = 3$. Thus the elements of G are

$$\begin{aligned} g_1(X,Y) &= X^2 + a_1 Y + b_1 X + c_1, \\ g_2(X,Y) &= XY + a_2 Y + b_2 X + c_2, \\ g_3(X,Y) &= Y^2 + a_3 Y + b_3 X + c_3 \end{aligned}$$

for $a_i, b_i, c_i \in K$ $(i = 1, 2, 3)$ by Proposition 3.4. For the linear polynomial $l(X,Y)$, every polynomial of the form $aY + bX + c$ in $\varphi^{-1}(L(\infty \cdot \infty - (P_1 + P_2)))$ is $kl(X,Y)$ for $k \in K$.

(i) Since $(g_1)^+ \geq P_1 + P_2$, we have $g_1(X,Y) - (X - x_1)(X - x_2) \in \varphi^{-1}(L(\infty \cdot \infty - (P_1 + P_2)))$ with a leading monomial $\leq Y$. It follows that $g_1(X,Y) = (X - x_1)(X - x_2) + k_1 l(X,Y)$ for $k_1 \in K$. Further, $g_1(x_3, y_3) = 0$. Since D is a normal divisor, $l(x_3, y_3) \neq 0$ by Proposition 3.2. Thus $k_1 = -l(x_3, y_3)^{-1}(x_3 - x_1)(x_3 - x_2)$. Further, $g_2(X,Y)$ and $g_3(X,Y)$ are obtained from $(X - x_1)(Y - y_2), (Y - y_1)(Y - y_2) \in \varphi^{-1}(L(\infty \cdot \infty - (P_1 + P_2)))$.

(ii) Since $P_1 = P_2$, we have $l(X,Y) = F_Y(x,y)(Y - y) + F_X(x,y)(X - x)$.

If $F_Y(x,y) = S_0 = 0$, then $(l)^+ = (X - x)^+ \geq 2P$. It follows that $g_1(X,Y) = (X - x)^2$ and $g_2(X,Y) = (X - x)(Y - y)$. For a polynomial $(Y - y)^3 - F(X,Y) \in I$, the remainder $r(X,Y) = 3y(Y - y)^2 + X - x$ on division by $\{g_1(X,Y), g_2(X,Y)\}$ is also in I. Since D is a normal divisor, we have $y \neq 0$ by Proposition 3.2. Thus $\mathrm{LM}(r(X,Y)) = Y^2$. It follows that $g_3(X,Y) = (Y - y)^2 + (3y)^{-1}(X - x)$.

If $F_Y(x,y) = S_0 \neq 0$, then $(l)^+ \geq 2P$ with $\mathrm{LM}(l(X,Y)) = Y$. It follows that $l(X,Y)(X - x), l(X,Y)(Y - y) \in I$ with the leading monomials XY and Y^2. For a polynomial $F(X,Y) - F_Y(x,y)^{-1} l(X,Y)(Y - y)Y \in I$, the remainder $r(X,Y) = S_0^{-2}(S_0^2 T_2 + 3yT_1^2 - S_0 S_1 T_1)(X - x)^2 + l(X,Y)$ on division by $\{l(X,Y)(X - x), l(X,Y)(Y - y)\}$ is also in I. Since D is a normal divisor, we have $S_0^2 T_2 + 3yT_1^2 - S_0 S_1 T_1 \neq 0$ by Proposition 3.2. Thus $\mathrm{LM}(r(X,Y)) = X^2$. It implies that $g_1(X,Y) = (X - x)^2 + (S_0^2 T_2 + 3yT_1^2 - S_0 S_1 T_1)^{-1} S_0^2 l(X,Y)$. Further, $g_2(X,Y)$ and $g_3(X,Y)$ are obtained from a Groebner basis $\{g_1(X,Y), l(X,Y)(X - x), l(X,Y)(Y - y)\}$. □

3.3 Inverse of a normal divisor

In this subsection, we give the inverse of normal divisors of C. Let $D = E - n \cdot \infty \in \mathrm{Div}_K^0(C)$ be a divisor with $E = D^+$ and let G be the reduced Groebner basis for $\varphi^{-1}(I_D)$. Let $D' = E' - n' \cdot \infty$ be the normal divisor such that $D' \sim -D$ and let G' be the reduced Groebner basis for $\varphi^{-1}(I_{D'})$. Then $D' = -D + (g_1)$ for the element $g_1(X,Y)$ with the smallest leading monomial but Y^3 in G, where (g_1) denotes the divisor $(\varphi(g_1(X,Y)))$.

Since $E' = (g_1)^+ - E$, $\varphi^{-1}(I_{D'})$ is

$$\{h(X,Y) \mid h(X,Y)g_i(X,Y) \in \langle g_1(X,Y), F(X,Y)\rangle \text{ for all } g_i(X,Y) \in G\}.$$

In particular, if D is a normal divisor, then $n' = \deg(g_1)^+ - n$ and $g_1(X,Y)$ is also the element with the smallest leading monomial in G'.

For example, let $D = E - 3\cdot\infty$ be a normal divisor with

$$G = \{g_1(X,Y), g_2(X,Y), g_3(X,Y)\}$$

such that $\mathrm{LM}(g_1(X,Y)) = X^2$. Then $D' = -D + (g_1)$ and $\deg E' = 3$. Thus

$$G' = \{h_1(X,Y) = g_1(X,Y), h_2(X,Y), h_3(X,Y)\}$$

with $h_2(X,Y) = XY + A_2Y + B_2X + C_2$, $h_3(X,Y) = Y^2 + A_3Y + B_3X + C_3$ for $A_i, B_i, C_i \in K$ $(i = 2,3)$ such that $h_j(X,Y)g_k(X,Y) \in \langle g_1(X,Y), F(X,Y)\rangle$ for all $j,k = 2,3$.

For a normal divisor D, we have the following on a normal divisor D' such that $D' \sim -D$:

Theorem 3.6 *Let $D \in \mathrm{Div}_K^0(C)$ be a normal divisor, and let G be the reduced Groebner basis for the normal ideal $\varphi^{-1}(I_D)$. Let D' be the normal divisor such that $D' \sim -D$. Then the reduced Groebner basis G' for the normal ideal $\varphi^{-1}(I_{D'})$ is as follows:*
(a) *If $G = \{1\}$, then $G' = \{1\}$;*
(b) *If $G = \{g_1(X,Y) = X + c_1, g_2(X,Y) = Y + c_2\}$, then*
$G' = \{h_1(X,Y) = X + c_1, h_2(X,Y) = Y^2 - c_2Y + {c_2}^2 + s_2c_1^2 - s_1c_1 + s_0\}$;
(c) *If $G = \{g_1(X,Y) = X + c_1, g_2(X,Y) = Y^2 + a_2Y + c_2\}$, then*
$G' = \{h_1(X,Y) = X + c_1, h_2(X,Y) = Y - a_2\}$;
(d) *If $G = \{g_1(X,Y) = Y + b_1X + c_1, g_2(X,Y) = X^2 + b_2X + c_2\}$, then*
$G' = \{h_1(X,Y), h_2(X,Y)\}$ *for*

$$\begin{aligned} h_1(X,Y) &= Y + b_1X + c_1, \\ h_2(X,Y) &= X^2 + (-b_1^3 - b_2 + t_3 - b_1s_2)X \\ &\quad +b_1^3b_2 + b_2^2 - 3b_1^2c_1 - c_2 + t_2 - b_2t_3 - b_1s_1 + b_1b_2s_2 - c_1s_2; \end{aligned}$$

(e) *If $G = \{g_1(X,Y), g_2(X,Y), g_3(X,Y)\}$ for*

$$\begin{aligned} g_1(X,Y) &= X^2 + a_1Y + b_1X + c_1, \\ g_2(X,Y) &= XY + a_2Y + b_2X + c_2, \\ g_3(X,Y) &= Y^2 + a_3Y + b_3X + c_3, \end{aligned}$$

then $G' = \{h_1(X,Y), h_2(X,Y), h_3(X,Y)\}$ *for*

$$\begin{aligned}
h_1(X,Y) &= X^2 + a_1Y + b_1X + c_1, \\
h_2(X,Y) &= XY + (-a_2 + b_1)Y + (a_1^2 - a_3 - a_1s_2)X \\
&\quad -a_1^2a_2 + a_2a_3 - a_1^2b_1 - a_3b_1 + a_1b_3 - a_1s_1 + a_1a_2s_2 + a_1^2t_3, \\
h_3(X,Y) &= Y^2 + (a_1^2 - b_2 - a_1s_2)Y + (2a_1b_1 - b_3 + s_1 - b_1s_2 - a_1t_3)X \\
&\quad -2a_1a_2^2 + 2a_1^2a_3 + 2a_1a_2b_1 - a_1b_1^2 - 3a_1^2b_2 + b_2^2 + a_2b_3 - b_1b_3 + s_0 + a_2^2s_2 \\
&\quad -a_1a_3s_2 - a_2b_1s_2 + 2a_1b_2s_2 - a_1t_2 + a_1b_1t_3.
\end{aligned}$$

3.4 Addition of normal divisors

In this subsection, we consider the addition of normal divisors in C. Let $D_1 = E_1 - n_1 \cdot \infty$ and $D_2 = E_2 - n_2 \cdot \infty$ be normal divisors of C with $E_1 = D_1^+$ and $E_2 = D_2^+$. Let $D' = E' - n' \cdot \infty$ be a normal divisor such that $D' \sim -(D_1 + D_2)$ and $D = E - n \cdot \infty$ be a normal divisor such that $D \sim D_1 + D_2$. In this subsection, we use the following notation:

$$\begin{aligned}
I' &: \text{a normal ideal } \varphi^{-1}(L(\infty \cdot \infty - E')), \\
I &: \text{a normal ideal } \varphi^{-1}(L(\infty \cdot \infty - E)), \\
G_1 &: \text{ a reduced Groebner basis for } \varphi^{-1}(L(\infty \cdot \infty - E_1)), \\
G_2 &: \text{ a reduced Groebner basis for } \varphi^{-1}(L(\infty \cdot \infty - E_2)), \\
G_g &: \text{ a set } \{f_i(X,Y)g_j(X,Y), F(X,Y) \mid f_i(X,Y) \in G_1, g_j(X,Y) \in G_2\}, \\
G &: \text{ a reduced Groebner basis for } I, \\
H &: \text{ a reduced Groebner basis for } \varphi^{-1}(L(\infty \cdot \infty - (E_1 + E_2))), \\
h_1(X,Y) &: \text{ a polynomial with the smallest leading monomial in } H, \\
v_1(X,Y) &: \text{ a monic polynomial with the smallest leading monomial in } I', \\
f &: \text{ a function } \varphi(f(X,Y)) \text{ for a polynomial } f(X,Y).
\end{aligned}$$

The final purpose of this subsection is to find G for the given G_1 and G_2.

Since G_g generates $\varphi^{-1}(L(\infty \cdot \infty - (E_1 + E_2)))$, H is obtained by the algorithm due to Buchberger for computing a Groebner basis using S-polynomials. H satisfies that $\Delta(H) \subset \Delta(G_g)$ with $\delta(H) = n_1 + n_2$. Since $h_1 \in L(m \cdot \infty - (D_1 + D_2))$ with the smallest integer m such that $l(m \cdot \infty - (D_1 + D_2)) = 1$, we have $n_1 + n_2 \le \deg{(h_1)^+} = n_1 + n_2 + m \le n_1 + n_2 + 3$. For the polynomial $h_1(X,Y)$, we have $D' = -(D_1 + D_2) + (h_1)$ and

$$I' = \{v(X,Y) \mid v(X,Y)h_i(X,Y) \in \langle h_1(X,Y), F(X,Y)\rangle \text{ for all } h_i(X,Y) \in H\}.$$

If $\mathrm{LM}(H)$ is obtained, $\mathrm{LM}(v_1(X,Y))$ is determined by $n' = \deg{(h_1)^+} - (n_1 + n_2)$ and $\mathrm{LM}(v_1(X,Y)h_i(X,Y)) \in \mathrm{LM}(\langle h_1(X,Y), F(X,Y)\rangle)$ for all $h_i(X,Y) \in H$. Further, $\mathrm{LM}(G)$ is determined with $\mathrm{LM}(v_1(X,Y))$ and n' by Theorem 3.6. Thus, $\mathrm{LM}(G)$ is determined by $\mathrm{LM}(H)$ when G_1 and G_2 are given. As a result, we have the following on the relation between $\mathrm{LM}(H)$ and $\mathrm{LM}(G)$ for the given G_1 and G_2:

no.	LM(G_1)	LM(G_2)	LM(H)	LM(G)
I	$\{X, Y\}$	$\{X, Y\}$	(i) $\{X, Y^2\}$	$\{X, Y^2\}$
			(ii) $\{Y, X^2\}$	$\{Y, X^2\}$
II	$\{X, Y\}$	$\{X, Y^2\}$	(i) $\{X, Y^3\}$	$\{1\}$
			(ii) $\{X^2, XY, Y^2\}$	$\{X^2, XY, Y^2\}$
III	$\{X, Y\}$	$\{Y, X^2\}$	(i) $\{Y, X^3\}$	$\{X, Y^2\}$
			(ii) $\{X^2, XY, Y^2\}$	$\{X^2, XY, Y^2\}$
IV	$\{X, Y\}$	$\{X^2, XY, Y^2\}$	(i) $\{X^2, XY, Y^3\}$	$\{X, Y\}$
			(ii) $\{X^2, Y^2\}$	$\{Y, X^2\}$
			(iii) $\{XY, Y^2, X^3\}$	$\{X^2, XY, Y^2\}$
V	$\{X, Y^2\}$	$\{X, Y^2\}$	(i) $\{X^2, XY, Y^3\}$	$\{X, Y\}$
			(ii) $\{X^2, Y^2\}$	$\{Y, X^2\}$
VI	$\{X, Y^2\}$	$\{Y, X^2\}$	(i) $\{X^2, XY, Y^3\}$	$\{X, Y\}$
			(ii) $\{XY, Y^2, X^3\}$	$\{X^2, XY, Y^2\}$
VII	$\{Y, X^2\}$	$\{Y, X^2\}$	(i) $\{Y, X^4\}$	$\{1\}$
			(ii) $\{X^2, Y^2\}$	$\{Y, X^2\}$
			(iii) $\{XY, Y^2, X^3\}$	$\{X^2, XY, Y^2\}$
VIII	$\{X, Y^2\}$	$\{X^2, XY, Y^2\}$	(i) $\{X^2, XY^2, Y^3\}$	$\{X, Y^2\}$
			(ii) $\{XY, X^3, Y^3\}$	$\{Y, X^2\}$
			(iii) $\{Y^2, X^3, X^2Y\}$	$\{X^2, XY, Y^2\}$
IX	$\{Y, X^2\}$	$\{X^2, XY, Y^2\}$	(i) $\{X^2, XY^2, Y^3\}$	$\{X, Y^2\}$
			(ii) $\{XY, Y^2, X^4\}$	$\{X, Y\}$
			(iii) $\{XY, X^3, Y^3\}$	$\{Y, X^2\}$
			(iv) $\{Y^2, X^3, X^2Y\}$	$\{X^2, XY, Y^2\}$
X	$\{X^2, XY, Y^2\}$	$\{X^2, XY, Y^2\}$	(i) $\{X^2, Y^3\}$	$\{1\}$
			(ii) $\{XY, X^4, Y^3\}$	$\{X, Y^2\}$
			(iii) $\{Y^2, X^3\}$	$\{X, Y\}$
			(iv) $\{Y^2, X^2Y, X^4\}$	$\{Y, X^2\}$
			(v) $\{X^3, X^2Y, XY^2, Y^3\}$	$\{X^2, XY, Y^2\}$

Since $v_1(X,Y)h_i(X,Y) \in \langle h_1(X,Y), F(X,Y)\rangle$, we can write

$$v_1(X,Y)h_i(X,Y) = q_{1,i}(X,Y)h_1(X,Y) + q_{2,i}(X,Y)F(X,Y)$$

with $q_{1,i}(X,Y), q_{2,i}(X,Y) \in K[X,Y]$. It follows that $(v_1) + (h_i) = (q_{1,i}) + (h_1)$. Thus $(q_{1,i})^+ = (v_1)^+ + (h_i)^+ - (h_1)^+$. Since $(h_i)^+ \geq E_1 + E_2$, we have $q_{1,i} \in L(\infty \cdot \infty - E)$. Thus $q_{1,i}(X,Y) \in I$. Conversely, if $f(X,Y) \in I$, then $(f)^+ \geq E$. For $H =$

$\{h_1(X,Y),\ldots,h_t(X,Y)\}$, it follows that

$$\begin{aligned}(f)^+ &\geq E_1+E_2-(h_1)^+ + (v_1)^+\\ &= \min\{(q_{1,i})^+ \mid i=1,\cdots,t\}.\end{aligned}$$

It implies that the function $\varphi(f(X,Y)) \in \langle q_{1,1},\cdots,q_{1,t}\rangle$. Thus

$$f(X,Y)\in\langle q_{1,1}(X,Y),\cdots,q_{1,t}(X,Y),F(X,Y)\rangle.$$

As a result,

$$I=\langle q_{1,1}(X,Y),\cdots,q_{1,t}(X,Y),F(X,Y)\rangle.$$

References

[1] L. M. Adleman, J. DeMarrais, and M. D. Huang, *A subexponential Algorithm for Discrete Logarithms over the Rational Subgroup of the Jacobians of Large Genus Hyperelliptic Curves over Finite Fields,* Algorithmic Number Theory, Lect. Notes Comp. Sci., 877, Springer-Verlag, pp. 28–40.

[2] S. Arita, *Algorithms for computation in Jacobian group of C_{ab} curve and their application to discrete-log-based public key cryptosystems,* The mathematics of public key cryptography, Fields Institute A. Odlyzko et al (eds.), 1999.

[3] D. G. Cantor, *Computing in the Jacobian of a hyperelliptic curve,* Math. Comp., 48(177), pp. 95–101 (1987).

[4] D. Cox, J. Little, D. O'shea, *Ideals, Varieties, and Algorithms,* Springer-Verlag, Berlin, 1997.

[5] W. Fulton, *Algebraic Curves,* Benjamin, New York, 1969.

[6] S. D. Galbraith, S. M. Paulus, and N. P. Smart, *Arithmetic on Superelliptic Curves,* Math. Comp. vol. 71, no. 237, pp. 393–405, 2000.

[7] V. D. Goppa, *Geometry and Codes,* Kluwer Academic Publishers, 1988.

[8] R. Matsumoto, *The Cab curve - a generalization of the Weierstrass form to arbitrary plane curves,* http://www.rmatsumoto.org/cab/html.

[9] S. Miura, *Algebraic geometric codes on certain plane curves,* Trans. IEICE **J75-A** (1992), no. 11, pp. 1735–1745 (Japanese).

[10] S. Miura, *Linear codes on affine algebraic curves,* Trans. IEICE **J81-A** (1998), no. 10, pp. 1398–1421, (Japanese).

[11] R. Pellikaan, *On the existence of order functions,* J. Statistical Planning and Inference, no. 94, pp. 287–301, 2001.

[12] J. H. Silverman, *The Arithmetic of Elliptic Curves,* Springer-Verlag.