TWMS J. Pure Appl. Math. V.4, N.1, 2013, pp.69-77

C_{ab} CURVES: A QUICK SHORT-CUT

A. BASIRI[1], S. RAHMANY[1]

Abstract. The objective of this paper is to state and prove some useful theorems for realizing the group law in the Jacobians of C_{ab} curves, which provide an efficient and easy-to-implement algorithm for computations within the group. The idea is a generalization of a method previously presented in 2005, which gave an algorithm to realizing the group law on the superelliptic curves of genus 3 or 4. As an example of our approach, we will show how this method can be used to formulate a reasonably fast arithmetic in the Jacobian of C_{35} curve.

Keywords: C_{ab} curves, Jacobian group, Arita algorithm.

AMS Subject Classification: 68W30, 14H40, 14H45.

1. Introduction

Our interest in the subject of this paper is inspired by the idea presented in [3], where the authors use the FGLM algorithm for realizing the group law in the Jacobian group of superelliptic curves of genus 3 or 4. Similar to the hyper-elliptic curves, the addition in the Jacobian of a C_{ab} curve proceeds in two steps. In the first step, the two reduced divisors are simply added yielding a divisor of degree up to $2g$ (g is the genus of curve). In the second step, this divisor is reduced to the representative of minimal degree in its class.

Several efficient algorithms exist for Jacobian arithmetic of super-elliptic and C_{ab} curves, [1, 9, 10]. These algorithms use the representation of Jacobian elements by polynomials and rely on rather heavy techniques of symbolic computations like LLL, Hermite normal form and Gröbner basis computations. As explained in [3], the core of these algorithms consists of the reduction process, namely transforming any group element into its equivalent reduced representative. These algorithms generally admit a unifying description as follows:

Algorithm 1 (Reduction).
Input: ideal $\mathfrak{a}$ of $K[C]$
Output: reduced ideal RED($\mathfrak{a}$) equivalent to $\mathfrak{a}$

(1) Choose an integral ideal $\mathfrak{b}$ in the class of $\mathfrak{a}^{-1}$, such that $\mathfrak{b} = u\mathfrak{a}^{-1}$ for some $u \in \mathfrak{a}$
(2) Let $e \neq 0$ be the minimum of $\mathfrak{b}$ w.r.t the C_{ab} order
(3) Put $\text{RED}(\mathfrak{a}) = e\mathfrak{b}^{-1} = \frac{e}{u}\mathfrak{a}$

In [1], the ideals of $K[C]$ are represented by their Gröbner bases w.r.t C_{ab} order, and u is chosen as the C_{ab} minimum of $\mathfrak{a}$. The approach relies on Buchberger's algorithm. Whilst, in both [9] and [10], the ideals are represented by their Hermite normal forms as $K[X]$-modules, or equivalently, by their Gröbner bases w.r.t the lexicographic order. The natural choice for u is, then, the minimum w.r.t this order. However, the minimum for the C_{ab} order can be computed via a variant of LLL algorithm for function fields according to Paulus [12].

[1]School of Mathematics and Computer Science, Damghan University, Damghan, Iran,
e-mail: basiri@du.ac.ir
Manuscript received May 2012.

Moreover, some new algorithms were described in [3] for realizing the arithmetic in the Jacobians of super-elliptic curves of genus 3 or 4. They consider a special class of ideals allowing a simplified polynomial representation called "typical ideals". These special ideals occur with a probability near one. This approach follows the framework of Algorithm 1. Having represented ideals by their lexicographic Gröbner bases, one uses the FGLM algorithm ([8]) to find the C_{ab} minimum.

Our purpose is to generalize the above idea to C_{ab} curves. The paper is organized as follows. In Section 2, some basic definitions of Jacobians of C_{ab} curves are introduced. In Section 3 our main results are stated and proved. Also, as an application of the presented method, we will provide explicit formulae for realizing the group law in the Jacobians of C_{35} curves in Section 4.

2. Basic definitions

In this section, some basic algebraic structures of C_{ab} curves will be reviewed. Also some definitions which will be used throughout this paper, are introduced.

Let K be a field with characteristic different from a and $\overline{K}$ be its algebraic closure. The following definition introduces C_{ab} curves ([11]).

Definition 2.1. *For co-prime positive integers a and b, which are also co-prime to the characteristic of the ground field, a C_{ab} curve is defined by a non-singular affine equation of the form*

$$C = Y^a + \sum_{ia+jb<ab} c_{ij} X^i Y^j + X^b. \tag{1}$$

The *coordinate ring* of C is defined by $K[C] = K[X,Y]/(C)$, its *function field* by $K(C)$, which is the field of fractions of $K[C]$. A *rational prime divisor* of C is given by an orbit of points on C with coordinates in $\overline{K}$ under the action of $Gal(\overline{K}/K)$, and its degree is the number of points in the orbit. The group of K-rational divisors is the free abelian group over the prime divisors, with the degree function extended naturally, and of special interest is its degree zero part D^0. Associating to a function in $K(C)$, its divisors of zeroes and poles with the appropriate multiplicities, one defines the subgroup of principal divisors P_K. Finally the residue group of D^0 by P_K is called *Jacobian group* of C.

Since C is non-singular on affine plane, $K[C]$ is a Dedekind domain and hence the Jacobian group of C is naturally isomorphic to the ideal class group of $K[C]$. So, every divisor in the Jacobian group of C corresponds to an ideal in the ideal class group of $K[C]$ and therefore, we may focus only onto the arithmetic on the ideals.

For the computations of the Gröbner basis of these ideals, we need the following definition:

Definition 2.2. *For $\alpha = (\alpha_1, \alpha_2)$ and $\beta = (\beta_1, \beta_2) \in \mathbb{Z}^2_{\geq 0}$, the order $\prec_{C_{ab}}$ which is defined as: $\alpha \prec_{C_{ab}} \beta$ if and only if $a\cdot\alpha_1 + b\cdot\alpha_2 < a\cdot\beta_1 + b\cdot\beta_2$ or $a\cdot\alpha_1 + b\cdot\alpha_2 = a\cdot\beta_1 + b\cdot\beta_2$ and $\beta_1 < \alpha_1$, is called a C_{ab} order.*

In the step 2 of Algorithm 1, we have to use the C_{ab} order to find the minimum of the given ideal. But as explained in Section 1, it is better to consider a special class of ideals allowing a simplified polynomial representation w.r.t the lexicographical order, which is defined as follows:

Definition 2.3. *Let C be a C_{ab} curve and g be its genus. An ideal $\mathfrak{a}$ (resp. a divisor D) of $K[C]$ (resp. of C) is called typical iff $\mathfrak{a} = \mathrm{id}(u, Y - v)$ (resp. $D = \mathrm{Div}(u, Y - v)$) where u and v are some polynomials in $K[X]$ such that: $\deg(v) < \deg(u) \leq g$ and $u | C(X, v)$.*

Remark 2.1. *It is known that the genus of a C_{ab} curve is equal to $\frac{(a-1)(b-1)}{2}$.*

3. Main theorems

The product of two ideal classes, represented by ideals $\mathfrak{a}_i = (u_i, Y - v_i)$, $\deg u_i = g$, $\deg v_i = g - 1$, $i \in \{1, 2\}$, is obtained in two steps as explained in Section 1. The *composition* (or the first step) corresponds simply to the ideals multiplication and yields $\mathfrak{a} = (u, Y - v) = \mathfrak{a}_1\mathfrak{a}_2$ [3, 4].

In this section we compute the the second step which takes an ideal $\mathfrak{a} = (u, Y - v)$ as input with u of degree at most $2g$ and v of degree at most $2g - 1$, yielding a generator set for the equivalent ideal $\mathfrak{a}' = (u', Y - v')$, where u'(resp. v') is a polynomial of degree at most g(resp. $g - 1$), which, by [3], is the reduced representative of its class.

In this section we use the following notations and remarks:

(1) $\phi(s)$ the remainder of division s by u where $s \in k[X, Y]$ and $u \in k[X]$
(2) $\delta(s)$ the quotient of division s by u
(3) $m_{ab}(S)$ the minimum polynomial of the set S, w.r.t the C_{ab} order
(4) u and v some polynomials in $K[X]$
(5) $\mathfrak{a} := \mathrm{id}(u, Y - v)$ the ideal generated by u and $Y - v$ in $K[X, Y]$
(6) C a C_{ab}. curve

Remark 3.1. *We always assume that* $C \in \mathfrak{a}$

(7) $\mathfrak{b} := \mathrm{denom}(\mathfrak{a})\mathfrak{a}^{-1}$
(8) $[s_1, \cdots, s_m]_{K[X]}$ the $K[X]$-submodule of $K[X, Y]$, generated by $s_1, \cdots, s_m \in K[X, Y]$
(9) $q := \frac{C(X,Y)-C(X,v)}{Y-v}$.

Remark 3.2. *Note that* $Y - v$ *divides* $C(X, Y) - C(X, v)$ *(Lemma 2 of* [5]*).*

In [5] the step 1 of Algorithm 1 is run as follows

$$\begin{aligned}
\mathfrak{b} &= \mathrm{denom}(\mathfrak{a})\mathfrak{a}^{-1} = (\mathrm{id}(u, C) : \mathfrak{a}) = \\
&= \mathrm{id}(C) + [u, uY, ..., uY^{a-2}, q]_{K[X]} = \\
&= \{\lambda C + \sum_{i=0}^{a-2} \gamma_i u Y^i + \gamma_{a-1} q | \lambda \in K[X, Y] \text{ and } \gamma_i \in K[X] \text{ for } i = 0..a - 1\}.
\end{aligned}$$

We are now in a position to state the theorem which gives a minimal element of the ideal $\mathfrak{b}$ w.r.t C_{ab} order and hence runs the step 2 of the Algorithm 1.

Theorem 3.1. *Let* $\mathfrak{b}_1 = [u, uY, ..., uY^{a-2}, q]_{K[X]}$. *Then*

$$m_{ab}(\mathfrak{b}_1) = m_{ab}(\{u\} \cup \{\phi(\alpha q) | \alpha \in K[X]\}).$$

Proof. There are polynomials $q_i \in K[X]$ such that $q = \sum_{i=0}^{a-1} q_i Y^i$. The $\deg_{C_{ab}}(g)$ and $m_{ab}(\{u\} \cup$ $\cup \{\phi(\alpha q) | \alpha \in K[X]\})$ are replaced by $\Gamma(g)$ and m_{ab}.

For $0 \neq \gamma \in \mathfrak{b}_1$, there are polynomials $\gamma_0, \gamma_1, \ldots \gamma_{a-1} \in K[X]$ such that

$$\begin{aligned}
\gamma &= \sum_{i=0}^{a-2} \gamma_i u Y^i + \gamma_{a-1} q = \\
&= \sum_{i=0}^{a-2} \gamma_i u Y^i + \phi(\gamma_{a-1} q) + \delta(\gamma_{a-1} q) u \sum_{i=0}^{a-2} \phi(\gamma_{a-1} q_i Y^i) \phi(\gamma_{a-1} q) = \\
&= (u\delta(\gamma_{a-1} q_{a-1}) + \phi(\gamma_{a-1} q_{a-1}))Y^{a-1} + \sum_{i=0}^{a-2} (\phi(\gamma_{a-1} q_i) + u(\gamma_i + \delta(\gamma_{a-1} q_i)))Y^i.
\end{aligned}$$

We have $\deg(\phi(\gamma_{a-1}q_i)) < \deg(u)$, put $d_{a-1} = \Gamma(u\delta(\gamma_{a-1}q_{a-1}))$ and for $i = 0, 1, \ldots, a-2$, $d_i = \Gamma(u(\gamma_i + \delta(\gamma_{a-1}q_i))Y^i)$. Thus if $\delta(\gamma_{a-1}q_{a-1}) \neq 0$ or if there is an $0 \leq i \leq a-2$ such that $\gamma_i + \delta(\gamma_{a-1}q_i) \neq 0$ then

$$\Gamma(\gamma) \geq \max\{d_i |\ 0 \leq i \leq a-1\} \geq \Gamma(u)$$

consequently $\gamma \geq_{C_{ab}} u \geq_{C_{ab}} m_{ab}$. On the other hand, $\delta(\gamma_{a-1}q_{a-1}) = 0$ and for all $0 \leq i \leq$ $\leq a-2 \gamma_i + \delta(\gamma_{a-1}q_i) = 0$, thus

$$\gamma = \phi(\gamma_{a-1}q_{a-1})Y^{a-1} + \sum_{i=0}^{a-2} \phi(\gamma_{a-1}q_i)Y^i = \phi(\gamma_{a-1}q) \geq_{C_{ab}} m_{ab}.$$

Hence, $m_{ab}(\mathfrak{b}_1) \geq_{C_{ab}} m_{ab}$ and clearly $m_{ab}(\mathfrak{b}_1) \leq_{C_{ab}} m_{ab}$ and consequently $m_{ab}(\mathfrak{b}_1) = m_{ab}$. □

Here, we are at the end of the step 2 of the Algorithm 1. The following theorem computes a generator set for the ideal $\mathrm{RED}(\mathfrak{a})$ (step 3 of the Algorithm 1).

Theorem 3.2. *Let $\mathfrak{b}_1 = [u, uY, ..., uY^{a-2}, q]_{K[X]}$ and there exist $w \in K[X]$ such that $C(X, v) = = uw$. Then the following hold:*
i) If $m_{ab}(\mathfrak{b}_1) = \phi(\alpha q)$, for some $\alpha \in K[X]$ then

$$\mathrm{RED}(\mathfrak{a}) = \mathrm{id}(C, \phi(\alpha q), \alpha w + \delta(\alpha q)(Y - v)).$$

ii) If $m_{ab}(\mathfrak{b}_1) = \phi(q)$ then $\mathrm{RED}(\mathfrak{a}) = \mathrm{id}(\phi(q), w + \delta(q)(Y - v))$, in particular if $m_{ab}(\mathfrak{b}_1) = q$ then $\mathrm{RED}(\mathfrak{a}) = \mathrm{id}(q, w)$.
iii) If $m_{ab}(\mathfrak{b}_1) = u$ then $\mathrm{RED}(\mathfrak{a}) = \mathfrak{a}$.

Proof.
i) By algorithm 1, $\mathrm{RED}(\mathfrak{a}) = \mathrm{id}(C, (u\phi(\alpha q))/u, ((Y - v)\phi(\alpha q))/u)$ but by Lemma 2 of [5], $q(Y - - v) = C - wu$ thus $(Y - v)\phi(\alpha q) = (Y - v)(\alpha q - \delta(\alpha q)u) = \alpha(C - wu) - \delta(\alpha q)u(Y - v)$ and hence the proof of i) will be fulfilled.
ii) We have

$$\begin{aligned} C &= q(Y - v) + wu = \\ &= \phi(q)(Y - v) + (w + \delta(q)(Y - v))u \in \\ &\in \mathrm{id}(\phi(q), w + \delta(q)(Y - v)), \end{aligned}$$

hence

$$\mathrm{RED}(\mathfrak{a}) = \mathrm{id}(\phi(q), w + \delta(q)(Y - v)).$$

iii)

$$\mathrm{RED}(\mathfrak{a}) = \mathrm{id}(C, (u^2)/u, (u(Y - v))/u) = \mathrm{id}(C, u, Y - v) = \mathrm{id}(u, Y - v) = \mathfrak{a}.$$

□

Corollary 3.1. *We have presented the above formulas to compute the form of a minimal element of ideal $\mathfrak{b}$ w.r.t. C_{ab} order (it is either u or $\phi(\alpha q)$ for a $\alpha \in K[X]$, Theorem 3.1). We have also presented a generator set for ideal $\mathrm{RED}(\mathfrak{a})$ (Theorem 3.2).*

4. Example: Arithmetic in the Jacobians of C_{35} curves

In this section, we provide explicit formulae for realising the group law in the Jacobians of C_{35} curves. To do so, we compute a Gröbner basis for the reduced ideal associated with ideal $\mathfrak{a}$ in $K[X,Y]/\mathrm{id}(C)$ where C is a C_{35} curve.

We use a well-known tricks to speed up the computations. By using two linear changes of variables, we can assume that $C := Y^3 + C_1Y + C_0$ where C_1 and C_0 are some polynomials in $K[X]$ of degree 3 and 5, respectively, and the coefficient of X^4 in C_0 is zero.

Also, we denote the coefficient of a polynomial in front of X^i by a subscript i and keep the following notations:

- K is a field of characteristic different from 3 and $\overline{K}$ its algebraic closure.
- C_1 and C_0 are some polynomials of degree 3 and 5 in $K[X]$, where $C_0 := C_{00} + + C_{01}X + C_{02}X^2 + C_{03}X^3 + X^5$, and $C := Y^3 + C_1Y + C_0$.
- v is a polynomial of degree 7 and u a monic polynomial of degree 8 in $K[X]$ and $v^3 + + C_1v + C_0 = wu$.
- $q = Y^2 + vY + v^2 + C_1$.
- $\mathfrak{b} := [\mathrm{id}(u, C) : \mathfrak{a}] = \mathrm{id}(C, u, q) = \mathrm{id}(C) + [u, uY, q]_{K[X]}$.

Remark 4.1. *We consider the general case, where* $\deg(u) = 8$ *and* $\deg(v) = 7$*, the other cases are easier.*

Theorem 4.1. *If* $\mathfrak{a} = \mathrm{id}(u(X), Y - v(X))$ *then the reduced ideal of* $\mathfrak{a}$ *is*

$$\mathrm{RED}(\mathfrak{a}) = \mathrm{id}(C, \phi(\alpha q), \alpha w + (\delta(\alpha v)Y + \delta(\alpha v^2 + C_1))(Y - v)),$$

where α *is a polynomial in* $k[X]$ *such that* $\phi(\alpha q) = \min_{C_{35}}(\mathfrak{b})$.

Proof. Note that the set

$$B := \{X^iY^j | 0 \le i \le 7 \ \& \ 0 \le j \le 1\}$$

is a generator for the vector space $K[C]/\mathfrak{b}$ and $|B| = 16$ thus $\dim_K(K[C]/\mathfrak{b}) \le 16$ (we mean by $X^iY^j + \mathfrak{b}$ by X^iY^j). This ensures that there is a linear relation between the set of the first seventeen monomials of $K[C]/\mathfrak{b}$ w.r.t C_{35} order, *i.e.*, $B' := \{X^iY^j | 3i + 5j \le 20, \ j \le 2\}$. There for $\deg_{C_{35}}(\min_{C_{35}}(b)) \le \deg_{C_{35}}(X^5Y) = 20$ but since $\deg_{C_{35}}(u) = 24$, we deduce from Theorem 3.1 that there is a $\alpha \in K[X]$ (with $\deg(\alpha) \le 3$) such that $\min_{C_{35}}(\mathfrak{b}) = \phi(\alpha q)$.

Since $\deg_{C_{35}}(\phi(q)) = 26$, there is an $\alpha \in K[X]$ with $1 \le \deg(\alpha) \le 3$ such that $\min_{C_{35}}(\mathfrak{b}) = = \phi(\alpha q)$. Especially in the general case, α is a polynomial of degree 3 and is derived in such a way that $\varphi := \phi(\alpha v) = \alpha v \bmod u$ be of degree 5, and $\psi := \phi(\alpha v^2 + \alpha C_1) = \phi(\varphi v) + \alpha C_1$ of degree 6. In this case

$$e \ := \ \min_{C_{35}}(\mathfrak{b}) = \phi(\alpha q) = \alpha Y^2 + \varphi Y + \psi. \tag{2}$$

Then, the reduced ideal $\mathrm{RED}(\mathfrak{a}) = \frac{e}{u}\mathfrak{a}$ is computed as follows (by Theorem 3.2):

$$\mathrm{RED}(\mathfrak{a}) = \mathrm{id}(C, \phi(\alpha q), \alpha w + (\delta(\alpha v)Y + \delta(\alpha v^2))(Y - v)),$$

but $\delta(\alpha v^2) = \delta(\varphi v) + \delta(\alpha v)v$ hence:

$$\mathrm{RED}(\mathfrak{a}) = \mathrm{id}(C, \phi(\alpha q), \alpha w + (\delta(\alpha v)(Y + v) + \delta(\varphi v))(Y - v)).$$

□

Now we compute a Gröbner basis for RED($\mathfrak{a}$) w.r.t $\prec_{Lex}$ order in the general case (where there is no division by zero). Let α be a polynomial of $K[X]$ such that $\min_{C_{35}}(\mathfrak{b}) = \phi(\alpha q) = e$. We denote by

$$e_1(Y) = Y^3 + C_1Y + C_0,$$
$$e_2(Y) = \alpha w + (\delta(\alpha v)(Y + v) + \delta(\varphi v))(Y - v),$$
$$e(Y) = \alpha Y^2 + \varphi Y + \psi,$$

the elements of a generator set for RED($\mathfrak{a}$) which is obtained in Theorem 4.1.

Lemma 4.1. *In the general case, α divides the* Resultant(e_2, e, Y) *and*

$$\begin{aligned}\frac{\text{Resultant}(e_2, e, Y)}{\alpha} &= 3\delta(\alpha v)^2\alpha w v u + \delta(\alpha v)^2\alpha v^2 C_1 - 3\delta(\alpha v)^2\alpha v C_0 + \\ &+2\delta(\alpha v)^3 u C_0 + 3\alpha v^2\delta(\varphi v)^2 + \delta(\alpha v)^2\alpha C_1^2 - \\ &-\delta(\varphi v)^3 u + \alpha C_1\delta(\varphi v)^2 + \alpha^3 w^2 - 3\alpha^2 w\delta(\alpha v)v^2 - \\ &-3\alpha^2 w v\delta(\varphi v) - 2\alpha^2 w\delta(\alpha v)C_1 + 6\alpha w\delta(\alpha v)\delta(\varphi v)u - \\ &-2\alpha v\delta(\varphi v)\delta(\alpha v)C_1 - 3\delta(\alpha v)\alpha\delta(\varphi v)C_0 - \delta(\alpha v)^3 u^2 w - \\ &-3\delta(\alpha v)^2 v^2\delta(\varphi v)u - 3v\delta(\varphi v)^2\delta(\alpha v)u - \delta(\alpha v)^2 C_1\delta(\varphi v)u\end{aligned}$$

is an element of the ideal id(e_1, e_2, e).

Proof. By Proposition 9, Section 3.5 of [7], we have

$$\text{Resultant}(e_2, e, Y) = \lambda_2(\alpha)e_2 + \lambda_3(\alpha)e,$$

where

$$\lambda_2(\alpha) = \det(M_1)Y + \det(M_2), \quad \lambda_3(\alpha) = \det(M_3)Y + \det(M_4)$$

and

$$M_1 = \begin{pmatrix} 0 & 0 & b_0 & 0 \\ 0 & a_0 & b_1 & b_0 \\ 0 & a_1 & b_2 & b_1 \\ 1 & a_2 & 0 & b_2 \end{pmatrix}, M_2 = \begin{pmatrix} a_0 & 0 & b_0 & 0 \\ a_1 & 0 & b_1 & b_0 \\ a_2 & 0 & b_2 & b_1 \\ 0 & 1 & 0 & b_2 \end{pmatrix},$$

$$M_3 = \begin{pmatrix} a_0 & 0 & 0 & 0 \\ a_1 & a_0 & 0 & b_0 \\ a_2 & a_1 & 0 & b_1 \\ 0 & a_2 & 1 & b_2 \end{pmatrix}, M_4 = \begin{pmatrix} a_0 & 0 & b_0 & 0 \\ a_1 & a_0 & b_1 & 0 \\ a_2 & a_1 & b_2 & 0 \\ 0 & a_2 & 0 & 1 \end{pmatrix}$$

and for $i = 0, 1, 2$:

$$a_i = \text{coeff}(e_2, Y^{2-i}), \ b_i = \text{coeff}(e, Y^{2-i}).$$

But

$$\begin{aligned}\lambda_2(\alpha) &= \alpha^3 w + ((\delta(\alpha v)v - \delta(\varphi v))Y - \delta(\alpha v)C_1 - \delta(\alpha v)v^2 - 2v\delta(\varphi v))\alpha^2 + \\ &+(-v\delta(\alpha v)^2 u + 2\delta(\alpha v)\delta(\varphi v)u - Y\delta(\alpha v)^2 u)\alpha + \delta(\alpha v)^3 u^2\end{aligned}$$

and

$$\begin{aligned}\lambda_3(\alpha) &= -\delta(\alpha v)\alpha^2 w + (\delta(\alpha v)(\delta(\varphi v) - \delta(\alpha v)v)Y + \delta(\alpha v)^2 C_1 + 2\delta(\alpha v)^2 v^2 + \\ &+\delta(\varphi v)^2)\alpha + \delta(\alpha v)^3 u Y - v\delta(\alpha v)^3 u,\end{aligned}$$

hence

$$\lambda_2(0) = \delta(\alpha v)^3 u^2$$

and

$$\lambda_3(0) = u\delta(\alpha v)^3(Y - v).$$

After simplification we have

$$\lambda_2(0)e_2 + \lambda_3(0)e = \alpha u C\delta(\alpha v)^3,$$

hence

$$\text{Resultant}(e_2, e, Y) = (\lambda_2(\alpha) - \lambda_2(0))e_2 + (\lambda_3(\alpha) - \lambda_3(0))e + \lambda_2(0)e_2 + \lambda_3(0)e$$

which implies that $\alpha \mid \text{Resultant}(e_2, e, Y)$ and

$$\begin{aligned}
\frac{\text{Resultant}(e_2, e, Y)}{\alpha} &= \frac{\lambda_2(\alpha) - \lambda_2(0)}{\alpha}e_2 + \frac{\lambda_3(\alpha) - \lambda_3(0)}{\alpha}e + uC\delta(\alpha v)^3 = \\
&= 3\delta(\alpha v)^2\alpha w v u + \delta(\alpha v)^2\alpha v^2 C_1 - 3\delta(\alpha v)^2\alpha v C_0 + \\
&\quad +2\delta(\alpha v)^3 u C_0 + 3\alpha v^2\delta(\varphi v)^2 + \delta(\alpha v)^2\alpha C_1^2 - \\
&\quad -\delta(\varphi v)^3 u + \alpha C_1\delta(\varphi v)^2 + \alpha^3 w^2 - 3\alpha^2 w\delta(\alpha v)v^2 - \\
&\quad -3\alpha^2 w v\delta(\varphi v) - 2\alpha^2 w\delta(\alpha v)C_1 + 6\alpha w\delta(\alpha v)\delta(\varphi v) - u - \\
&\quad -2\alpha v\delta(\varphi v)\delta(\alpha v)C_1 - 3\delta(\alpha v)\alpha\delta(\varphi v)C_0 - \delta(\alpha v)^3 u^2 w - \\
&\quad -3\delta(\alpha v)^2 v^2\delta(\varphi v)u - 3v\delta(\varphi v)^2\delta(\alpha v)u - \delta(\alpha v)^2 C_1\delta(\varphi v)u.
\end{aligned}$$

□

The next corollary gives us a bound for the degree of $\frac{\text{Resultant}(e_2,e,Y)}{\alpha}$.

Corollary 4.1. *In the general case,*

$$u^2 \mid ((\alpha C_0^2 + C_1(C_1\psi - C_0\varphi))\alpha + \psi(3C_0\varphi - 2C_1\psi))\alpha + \varphi^2(C_1\psi - C_0\varphi) + \psi^3$$

and $\frac{\text{Resultant}(e_2,e,Y)}{\alpha}$ *is equal to*

$$\frac{((\alpha C_0^2 + C_1(C_1\psi - C_0\varphi))\alpha + \psi(3C_0\varphi - 2C_1\psi))\alpha + \varphi^2(C_1\psi - C_0\varphi) + \psi^3}{u^2}$$

which is a polynomial of degree at most 4.

Proof. The result is done by substitution

$$\delta(\alpha v) = \frac{\alpha v - \varphi}{u}, \delta(\varphi v) = \frac{\varphi v + \alpha C_1 - \psi}{u} \text{ and } w = \frac{v^3 + C_1 v + C_0}{u} \tag{3}$$

for the formula obtained in Lemma 4.1.

□

Now, to compute a Gröbner basis for RED($\mathfrak{a}$), put

$$u' = \text{monic}(\frac{((\alpha C_0^2 + C_1(C_1\psi - C_0\varphi))\alpha + \psi(3C_0\varphi - 2C_1\psi))\alpha + \varphi^2(C_1\psi - C_0\varphi) + \psi^3}{u^2}) \tag{4}$$

and

$$S(Y) = \alpha e_2 - \delta(\alpha v)e.$$

Then

$$\begin{aligned}
S &= (\alpha\delta(\varphi v) - \delta(\alpha v)(\alpha v - \delta(\alpha v)u))\, Y + \\
&\quad +\alpha(w\alpha - v(\delta(\alpha v)v + \delta(\varphi v))) - \delta(\alpha v)(v(\alpha v - \delta(\alpha v)u) - \delta(\varphi v)u + \alpha C_1).
\end{aligned}$$

Here we substitute w, $\delta(\alpha v)$ and $\delta(\varphi v)$ for the equations 3, so

$$S = \frac{\alpha(\alpha C_1 - \psi) + \varphi^2}{u}Y + \frac{\alpha^2 C_0 + \varphi\psi}{u}.$$

Put

$$\begin{aligned} \lambda &:= \frac{\alpha^2 C_0 + \varphi\psi}{u}, \\ \mu &:= \frac{\alpha(\alpha C_1 - \psi) + \varphi^2}{u}, \\ v' &:= -\mu^{-1}\lambda \bmod u'. \end{aligned} \tag{5}$$

Here, all divisions by u are exact, that is with remainder zero.

Theorem 4.2. *$\{u', Y - v'\}$ is a Gröbner basis for* $\mathrm{RED}(\mathfrak{a}) = \mathfrak{a}' = \frac{e}{u}\mathfrak{a}$.

Proof. By Lemma 4.1, we have $u' \in \mathrm{RED}(\mathfrak{a})$, and it is clear that $S \in \mathrm{RED}(\mathfrak{a})$, hence $Y - v' \in \in \mathrm{RED}(\mathfrak{a})$, consequently $\mathrm{id}(u', Y - v') \subset \mathrm{RED}(\mathfrak{a})$. For the inverse case, inclusion in other sens, we use the equations 3 and replacing Y by v' in $e_1(Y)$, $e_2(Y)$ and $e(Y)$, one of this element becomes a multiplication of u'. We deduce that $\mathrm{RED}(\mathfrak{a}) \subset \mathrm{id}(u', Y - v')$ which completes the proof. □

Therefor, we are able to use the method presented in this paper to obtain explicit formula for realizing the group law in the Jacobian of a C_{ab} curve. For example, in [6] it is shown that the computational cost for addition in the Jacobian of a C_{35} curve is less than 400 multiplications.

5. Concluding remarks

A method based on Arita algorithm has been presented to find the explicit formula for realizing the group law in the Jacobian of a C_{ab} curve. These formula can be used to speed up the computations. The number of multiplications and inversions can be also counted to add two distinct elements in the Jacobian of the curve for given a and b, as for $a = 3$, $b = 5$ in [6]. The fact that the same method still goes for the case of Jacobian of C_A curves [2] is another advantage of the presented method.

Acknowledgments

The authors would like to express their gratitude to J.-C. Faugère, A. Enge, N. Ghal-Eh and N. Gürel for their helpful discussions, as well as the anonymous reviewers for their valuable comments.

References

[1] Arita, S., (1999), Algorithms for computations in Jacobian group of C_{ab} curve and their application to discrete-log based public key cryptosystems, IEICE Transactions J82-A, 8, pp.1291–1299, English translation in the proceedings of the Conference on The Mathematics of Public Key Cryptography, Toronto 1999 (in Japanese).

[2] Arita, S., Miura, S., Sekiguchi, T., (2004), An addition algorithm on the Jacobian varieties of curves, Journal of the Ramanujan Mathematical Society, 19(4), pp.235–251.

[3] Basiri, A., Enge, A., Faugère, J.-C., Gürel, N., (2005), The arithmetic of Jacobian groups of superelliptic cubics, Mathematics of Computation, 74, pp.389–410.

[4] Basiri, A., Enge, A., Faugère, J.-C., Gürel, N., (2004), Implementing the arithmetic of $c_{3,4}$ curves, in: Proceedings of ANTS-VI, Lecture Notes in Computer Science, Springer-Verlag, pp.87–101.

[5] Basiri, A., (2008), New method for computing the inverse ideal in a coordinate ring, International Journal of Mathematical, Physical and Engineering Sciences, 2(1), pp.38–40.

[6] Basiri, A., Rahmany, S., (2012), Implementing the arithmetic of $c_{3,5}$ curves (submitted).

[7] Cox, D., Little, J., O'Shea, D., (1992), Ideals, Varieties, and Algorithms, Undergraduate Texts in Mathematics, Springer-Verlag.

[8] Faugère, J.C., Gianni, P., Lazard, D., Mora, T., (1993), Efficient computation of zero-dimensional Gröbner bases by change of ordering, Journal of Symbolic Computation, 16, pp.329–344.
[9] Galbraith, S.D., Paulus, S., Smart, N.P., (2002), Arithmetic on superelliptic curves, Mathematics of Computation, 71(237), pp.393–405.
[10] Harasawa, R., Suzuki, J., (2000), Fast Jacobian group arithmetic on C_{ab} curves, in: W. Bosma (Ed.), Algorithmic Number Theory — ANTS-IV, 1838 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, pp.359–376.
[11] Miura, S., (1998), Linear codes on affine algebraic curves, IEICE Transactions J81-A 1398–1421, English summary by Ryutaroh Matsumoto available at *http://www.rmatsumoto.org/cab.html* (in Japanese).
[12] Paulus, S., (1998), Lattice basis reduction in function fields, in: J. P. Buhler (Ed.), Algorithmic Number Theory — ANTS-III, 1423 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, pp.567–575.

Abdolali Basiri received his Ph.D. degree on Informatics from "Laboratoire d'informatiqe de Paris 6, France" in 2003. Presently he is an assistant professor at Damghan University in Iran.

Sajjad Rahmany received his Ph.D. degree on Informatics from "Laboratoire d'informatiqe de Paris 6, France" in 2003. Presently he is an assistant professor at Damghan University in Iran.