Efficient Reduction on the Jacobian Variety of Picard curves

J.-P. Cherdieu , J. Estrada , E. Reinaldo

July 15, 1998

Abstract

In this paper, a system of coordinates for the elements on the Jacobian Variety of Picard curves is presented. These coordinates possess a nice geometric interpretation and provide us with an unifying environment to obtain an explicit structure of abelian variety for the Jacobian, as well as an efficient algorithm for the reduction and addition of divisors. Exploiting the geometry of the Picard curves, a completely effective reduction algorithm is developed, which works for curves defined over any ground field k, with $char(k) = 0$ or $char(k) \neq 3$.

In the generic case, the algorithm works recursively with the system of coordinates representing the divisors, instead of solving for points in their support. Hence, only one factorization is needed (at the end of the algorithm) and the processing of the system of coordinates involves only linear algebra and evaluation of polynomials in the definition field of the divisor D to be reduced. The complexity of this deterministic reduction algorithm is $O(deg(D))$. The addition of divisors may be performed iterating the reduction algorithm.

[0]AMS Subject Classification: 14H45, 14H40, 14H05, 14Q05, 14Q20, 11G10, 11T71.
Key Words: Picard curves, Jacobian Varieties, Addition Law, Discrete logarithm.

1 Introduction

In the present paper we present a fast and completely effective algorithm for the reduction of divisors on the Jacobian Variety of Picard curves. Our algorithm works correctly for any Picard curve $C(k)$ defined over a field k with $char(k) = 0$ or $char(k) \neq 3$. This algorithm is an improvement of an algorithm presented in [5]. The modifications are based on a refinement of the coordinates introduced in [5] (hence, they can also be used to endow the Jacobian Variety of $C(k)$, $J(C)$, with an explicit extructure of abelian variety). The complexity of this new algorithm is, also, linear in the degree of the effective divisor D (i.e. $O(deg(D))$) to be reduced, but the new algorithm possess certain features that permits us to diminish the cost of the computation of of a point as well as obtaining explicit formulas wich in fact are useful to lower down the complexity. We have implemented the algorithm in the symbolic computation language MAPLE V, permiting us to test the algorithm and to show several non-trivial examples.

The Picard Curves are genus *three* plane projective curve which has been intensively studied due to their conection with certain Hilbert's problems (c.f. [7], [8],[9],[10]) as well as to the study of some linear error correcting codes (c.f. [6]).

2 Notations and Terminology

Let k be an arbitrary field and $\overline{k}$ its algebraic closure. Let $X(\overline{k})$ be a k-defined plane projective curve in $\mathbb{P}^2_{\overline{k}}$ (here k-defined means that the polynomial defining $X(k)$ has all its coefficients in k) and $K_{X(\overline{k})}$ be the field of rational functions on $X(\overline{k})$. Let also $X(k)$ be the subset of k-rational points of $X(\overline{k})$ and $K_{X(k)}$ be the subfield of k-rational functions on $X(k)$.

A divisor D on $X(\overline{k})$ is a formal sum

$$D = \sum_{P \in X(\overline{k})} m_P P, \ m_P \in \mathbb{Z},$$

where all but a finite set of the m_P are zero (i.e. D is an element of the free abelian group $Div(X(\overline{k}))$ generated by the elements of $X(\overline{k})$). Given D we associate to it the number $\deg(D) = \sum_{P \in X(\overline{k})} m_P$, the map $deg()$ is an homorphism from $Div(X(\overline{k}))$ onto $\mathbb{Z}$. A divisor D is said to be k-rational iff all its points have coordinates in k (i.e $m_P \neq 0 \Rightarrow P \in X(k)$).

To any element f in $K_{X(\overline{k})}$ we associate the divisors $(f)_0$ and $(f)_\infty$ of zeros and poles of f, respectivelly. Denote also by $(f) = (f)_0 - (f)_\infty$ the divisor of f.

A divisor D is said to be principal iff there exists a rational function f such that $D = (f)$. The fact $\deg((f)) = 0$ joined to $(f \cdot g) = (f) + (g)$ shows that the set $\mathbb{P}(X(\overline{k}))$ of principal divisors forms a subgroup of the group $Div_0(X(\overline{k}))$ of divisor of degree zero. Then, the quotient group

$$J(X(\overline{k})) = Div_0(X(\overline{k}))/\mathbb{P}(X(\overline{k}))$$

is called the Jacobian variety of $X(\overline{k})$. We may consider also the subgroup $J_k(X(\overline{k}))$ of k-rational points of the Jacobian, i.e. the set of classes x having a representant D, with D k-rational.

If k is a finite field it is known that $J_k(X(\overline{k}))$ is a finite abelian group.

3 Some Geometric Facts About Picard Curves

Let k be an arbitrary field of $char(k) \neq 3$, and let $\overline{k}$ denote its algebraic closure.

Definition 3.1 *A Picard curve $C_{p_4}(k)$ is a genus three plane projective curve with model:*

$$C_{p_4}(k) : WY^3 - W^4 p_4(\frac{X}{W}) = 0 \tag{1}$$

where $p_4(x) = x^4 + a_3x + a_2x + a_1x + a_0$ is a polynomial in $k[x]$.

For $char(k) = 0$ or $char(k) > 3$ it is not difficult to prove that $C_{p_4}(k)$ will be non-singular if and only if the discriminant of p_4 is different from *zero* (i.e. p_4 has no multiple roots in $\overline{k}$). Moreover, every curve $C_{p_4}(k)$ is birationally equivalent to a Picard curve $C_{\widehat{p}_4}(k)$, with $\widehat{p}_4(x) = x^4 + \widehat{a}_2x^2 + \widehat{a}_1x + \widehat{a}_0$ (c.f. [4]), hence, without lost of generality, we may suppose in (1) $a_3 = 0$.

If the field k is algebraically closed every Picard curve $C_{p_4}(k)$ has five total ramification points $R_1, \dots, R_5$ with respect to the covering morphism

$$\begin{array}{rccc} \pi_x : & C_{p_4}(k) & \longrightarrow & \mathbb{P}^1_k \\ & (x:y:z) & \longmapsto & x \end{array}$$

The points $R_i = (r_i : 0 : 1)$, $i = 1, \dots, 4$, where r_i are the roots of $p_4(x)$ and $R_5 = P_\infty = (0 : 1 : 0)$, the point at infinity on $C_{p_4}(k)$. Moreover, if ξ represents a primitive cubic root of unity in k (i.e. $\xi^2 + \xi + 1 = 0$) the mapping

$$\begin{array}{rccc} \sigma : & C_{p_4}(k) & \longrightarrow & C_{p_4}(k) \\ & (x:y:z) & \longmapsto & (x:\xi y:z) \end{array} \tag{2}$$

is an automorphism of C satisfying:

$$\pi_x \circ \sigma = id_{\mathbb{P}^1_k} \text{ and } \sigma^3 = id_{C_{p_4}(k)}.$$

Given two points P_1 and P_2 we call them *conjugate* if $P_1 = \sigma(P_2)$ or $P_2 = \sigma(P_1)$ (from here on, we will denote $\sigma(P)$ simply by σP).

Lemma 3.2 *Let $C_{p_4}(k)$ be a non-singular Picard curve. Then the effective divisors of the canonical class K, of $C_{p_4}(k)$, are those which are the intersection of lines with $C_{p_4}(k)$.*

Proof. It is an easy consequence of the fact that:

$$\omega_1 = \frac{1}{y}dx,\ \omega_2 = \frac{x}{y^2}dx,\ \omega_3 = \frac{y}{y^2}dx \tag{3}$$

where

$$x = \frac{X}{W} \qquad y = \frac{Y}{W} \tag{4}$$

constitute a basis of $\Omega(0)$ (c.f. [2]). □

4 Explicit Algebraic Model for the Jacobian Variety of a Picard Curve

¿From here on $C_{p_4}(k)$ will be a fixed Picard curve, hence, we will denote it simply by C.

Definition 4.1 *Given an affine effective divisor D we call it* semireduced *if there exists no P_1 such that $D \succeq P_1 + \sigma P_1 + \sigma^2 P_1$. We set also*

$$Div^{+,i}(C) := \{D \in Div(C) \mid D \text{ } k\text{-rational semireduced of degree } i\}$$

for $i \geq 0$, and

$$\mathcal{D}(r,s) = \bigcup_{i=r}^{s} Div^{+,i}(C)$$

for $0 \leq r < s$.

Given a polynomial $f(x,y) \in k[x,y]$ we define the *order* of $f(x,y)$ at P_∞ as:

$$ord_{P_\infty}(f(x,y)) = -\nu_{P_\infty}(f(x,y)).$$

where, $\nu_{P_\infty}(*)$ denotes the valuation of $*$ at P_∞. We will also call the *leading term* of the polynomial $f(x,y)$ to the term $a_{i_1j_1}x^{i_1}y^{j_1}$ satisfying the equality:

$$\nu_{P_\infty}(v_D(x,y)) = \min_{i,j} \nu_{P_\infty}(a_{ij}x^iy^j) = \nu_{P_\infty}(a_{i_1j_1}x^{i_1}y^{j_1}). \tag{5}$$

Let D be an element of $\mathcal{D}(2,4)$. We will assign to D the conic $v_D(x,y) = a_{20}x^2 + a_{10}x + a_{01}y + a_{11}xy + a_{20}y^2 + a_{00}$ of least *order* at P_∞ satisfying the condition:

$$(v_D(x,y))_0 \succeq D \tag{6}$$

normalized by the additional condition that its *leading term* is monic. Note that in certain cases the conic may degenerate in a line or in the zero polynomial and that $v_D(x,y)$ satisfies

$$ord_{P_\infty}(v_D(x,y)) \leq 8 - (5 - deg(D)). \tag{7}$$

We call v_D the *interpolating conic* of D.

Lemma 4.2 *Let $v(x,y) = a_{20}x^2 + a_{10}x + a_{01}y + a_{11}xy + a_{20}y^2 + a_{00}$. Then the following equivalences hold:*

1. *$ord_{P_\infty}(v(x,y)) = 7 \Leftrightarrow a_{02} = 0$ and $a_{11} \neq 0$.*

2. $ord_{P_\infty}(v(x,y)) = 6 \Leftrightarrow a_{02} = 0,\ a_{11} = 0$ *and* $a_{20} \neq 0$.

3. $ord_{P_\infty}(v(x,y)) = 4 \Leftrightarrow a_{02} = 0,\ a_{11} = 0,\ a_{20} \neq 0$ *and* $a_{01} \neq 0$.

Proof. Consider the local parameter $t = \frac{x}{y}$ at P_∞, and impose the required vanishing conditions on $v_D(x,y)$. □

Definition 4.3 *Given a divisor D of degree ≥ 3 we call D* collinear *if there exist three points P_1, P_2, P_3 in $supp(D)$ and a line r_0 such that $(r_0)_0 \succeq P_1 + P_2 + P_3$. Otherwise, D is called* generic.

Lemma 4.4 *Given a divisor D in $\mathcal{D}(3,4)$, the following propositions are equivalent:*

a) $v_D(x,y)$ is linear *or factorizes in* linear *factors.*

b) $D + P_\infty$ is collinear.

c) $v_D(x,y) = a_{20}x^2 + a_{10}x + a_{01}y + a_{11}xy + a_{00}$ with $a_{11}^2 a_{00} + a_{01}^2 a_{20} - a_{11}a_{01}a_{10} = 0$

Note: recall that after (7) and lemma 4.2 we may assume $a_{02} = 0$.

Proof. *a)* $\Rightarrow$ *c)*. If $v_D(x,y)$ is a line then $a_{11} = a_{20} = 0$. Hence $a_{11}^2 a_{00} + a_{01}^2 a_{20} - a_{11}a_{01}a_{10} = 0$ holds. If $v_D(x,y)$ is of *degree two* then, after lemma 4.2, $a_{02} = 0$. Furthermore, $v_D(x,y)$ factorizes in linear factors if and only if

$$4 \times \det \begin{pmatrix} a_{20} & \frac{a_{11}}{2} & \frac{a_{10}}{2} \\ \frac{a_{11}}{2} & 0 & \frac{a_{01}}{2} \\ \frac{a_{10}}{2} & \frac{a_{01}}{2} & a_{00} \end{pmatrix} = a_{11}^2 a_{00} + a_{01}^2 a_{20} - a_{11}a_{01}a_{10} = 0.$$

c) $\Rightarrow$ *b)*. If $a_{11}^2 a_{00} + a_{01}^2 a_{20} - a_{11}a_{01}a_{10} = 0$ then if $a_{11} = a_{20} = 0$ then obviously holds *b)*. Else, depending on whether $a_{11} = a_{01} = 0$ or not we get either

$$v_D(x,y) = (a_{20}x^2 + a_{10}x + a_{00}) = r_1 r_2$$

or

$$v_D(x,y) = (a_{20}x + a_{11}y + a_{10} - a_{20}a_{01}/a_{11})(x + a_{01}/a_{11}) = r_1 r_2.$$

In any case v_D factorizes as a product of lines. Then, if $D \in Div^{+,4}(C)$, $D + P_\infty$ contains five points and at least three of them belong to r_1 or r_2. If $D \in Div^{+,3}(C)$ then the same reasoning applies to $D + 2P_\infty$.

b) $\Rightarrow$ *a)*. Follows directly from Bezout's theorem. $\square$

Let's denote by Φ the correspondence

$$\Phi : \mathcal{D}(2,4) \longrightarrow k[x] \times k[x,y] \times k[y]$$

which assigns to a divisor D the 3-tuple of polynomials

$$\Phi(D) = (u_D(x), v_D(x,y), w_D(y)), \tag{8}$$

where:

$$\begin{aligned} u_D(x) &= \prod_{P_i \in supp(D)} (x - x_i) && (9)\\ w_D(y) &= \prod_{P_i \in supp(D)} (y - y_i) && (10)\\ v_D(x,y) &= \text{the } \textit{interpolating conic} \text{ at } D, && (11) \end{aligned}$$

where, $P_i = (x_i : y_i : 1)$. The correspondence Φ fails to be injective on $\mathcal{D}(2,4)$: let x_1 and x_2 be elements of k satisfying $p_4(x_1) = p_4(x_2) \neq 0$, and suppose y_0 is a root of $y^3 - p_4(x_1) = 0$, then the divisors

$$\begin{aligned} D_1 &= (x_1 : y_0 : 1) + (x_1 : \xi y_0 : 1) + (x_2 : y_0 : 1) + (x_2 : \xi^2 y_0 : 1),\\ D_2 &= (x_1 : y_0 : 1) + (x_1 : \xi^2 y_0 : 1) + (x_2 : y_0 : 1) + (x_2 : \xi y_0 : 1) \end{aligned}$$

have the same image by Φ. Nevertheless, if we restrict it to the set

$$\mathcal{D}_0(2,4) = \bigcup_{i=2}^{4} Div_0^{+,i},$$

where,

$$Div_0^{+,i}(C) = \{D \in Div^{+,i}(C) \mid D \text{ does not contains two } \textit{conjugate} \text{ points}\},$$

for $i = 2, 3$, and

$$Div_0^{+,4}(C) = \{D \in Div^{+,i}(C) \mid D \neq P_1 + \sigma P_1 + P_2 + \sigma P_2, \}$$

we obtain:

Lemma 4.5 *The correspondence Φ restricted to $\mathcal{D}_0(2,4)$ defines a bijection onto its image $\Phi(\mathcal{D}_0(2,4))$.*

Proof. For D in $Div_0^{+,2}$, $Div_0^{+,3}$ or D in $Div_0^{+,4}$, with $D+P_\infty$ *generic*, after lemma 4.4, we obtain that $v_D(x,y)$ is a conic (or a line) whose coefficient of y is a polynomial in x not vanishing in the x-coordinates of the points in D. Therefore, factoring $u_D(x)$ we can recover the x-coordinates of the points on *supp*(D) and substituting in $v_D(x,y)$ we find the y-coordinates. The remaining cases are:

1. $D = P_1+P_2+P_3+P_4$ with $P_1+P_2+P_3$ *collinear*, $P_4 \neq \sigma^k P_i$, $k=1,2$, $i=1,2,3$. Then $v_D(x,y) = r_1(x,y)\cdot(x-x_4)$, where $(r_1)_0 \succcurlyeq P_1+P_2+P_3$, $r_1 = \alpha x+\beta y+\gamma$, $\beta \neq 0$. Factoring $u_D(x)$ and substituting in r_1 we recover P_1, P_2, P_3. The y-coordinate of P_4 is obtained as the root of the linear polynomial
$$L = \frac{w_D(y)}{(y-y_1)(y-y_2)(y-y_3)}$$

2. D is *generic* but $D+P_\infty$ is *collinear*. Then $D = P_1+P_2+P_3+\sigma P_3$, with $P_1 \neq \sigma^k P_2$, $k=1,2$; and $v_D(x,y) = r_1(x,y)\cdot(x-x_3)$, with $(r_1)_0 \succcurlyeq P_1+P_2$, $r_1 = \alpha x+\beta y+\gamma$, $\beta \neq 0$. Factoring $u_D(x)$ and substituting in r_1 we recover P_1, P_2. We find the y-coordinate of $\sigma^3 P_3$ as the root of the linear polynomial
$$L = \frac{R_x(v_D, C)}{g.c.d(R_x(r_1, C), R_x(v_D, C))}$$

$\square$

Remark 4.6 *If k is algebraically closed then, after lemma 4.5, the mapping Φ defines a bijection from $\mathcal{D}_0(2,4)$ onto the set Γ of 3-uples $(u(x), v(x,y), w(y))$ satisfying:*

1. $2 \leq \deg(u) = \deg(w) \leq 4$, *$u$ and w monic.*

2. $v(x,y) = a_{20}x^2 + a_{10}x + a_{01}y + a_{11}xy + a_{00}$ *is the* minimal normalized *conic which satisfies $u \mid R_y(v,C)$, $w \mid R_x(v,C)$ and $a_{11}x + a_{01} \not\equiv 0$.*

If k is not algebraically closed $\Phi(\mathcal{D}_0(2,4))$ is a proper subset of Γ.

The mapping Φ could be used to introduce an explicit structure of abelian variety in $J(C)$:

Theorem 4.7 *(Explicit structure of abelian variety for $J(C)$.)*
The Jacobian Variety $J(C)$ of a Picard curve contains a subgroup of $3-$torsion points, $\mathcal{T}$ and a Zariski closed subset $\mathcal{Z}$of $J(C)$, such that:

1. *$\mathcal{Z}$ is isomorphic to an affine algebraic variety. Furthermore, $\mathcal{Z}$ is the complete intersection of three polynomial equations in A_k^6, which may be explicitly given.*

2. *$\mathcal{T} \cong (\mathbb{Z}/3\mathbb{Z})^3$ and $J(C) = \cup_{t \in \mathcal{T}}(\mathcal{Z} + t)$*

3. *The family $\mathcal{A} = \{\mathcal{Z} + t \mid t \in \mathcal{T}\}$ is the atlas of a structure of algebraic variety on $J(C)$. Moreover, $\mathcal{A}$ endows $J(C)$ with a structure of abelian variety.*

Proof. For a detailed proof of this theorem we refer the reader to our paper [5] and for the analogous case of hyperelliptic curves to the book of Mumford [13]. □

5 An efficient reduction algorithm in the Jacobian of a Picard curve.

In the present section we will construct an efficient effective reduction algorithm in the Jacobian variety of a Picard curve. This algorithm works correctly in any field k with $char(k) = 0$ or $char(k) \neq 3$, but our main interest (motivated by applications) will be the case when k is a finite field $\mathbb{F}_q$. Let's state, clearly, the problem we will solve:

Reduction problem: Given an effective affine divisor D (by affine we mean $P_\infty \notin supp(D)$) find an effective affine divisor D_f, with $deg(D_f) \leq 3$, such that: $D - deg(D)P_\infty \cong D_f - deg(D_f)P_\infty$.

The reduction algorithm we present in this paper is based on the following geometric idea:

Suppose given an effective affine divisor $D_0 = P_1 + P_2 + P_3 + P_4$ of degree *four*. If the points on the divisor D_0 are collinear, then, by lemma 3.2, D_0 is in the canonical class and $D_0 - 4P_\infty \cong 0$. Otherwise, to find the *reduction* of $D_0 - 4P_\infty$, we take the *interpolating conic* v_0 of the divisor D_0. Then, after the relation (7), v_0 intercepts C, counting multiplicities, in at most *three* more affine points H_1, H_2, H_3. Therefore, we obtain:

$$\begin{aligned} (v_0) &= (D_0 - 4P_\infty) + (D_1 - 3P_\infty) \\ D_0 - 4P_\infty &\cong -(D_1 - 3P_\infty) \end{aligned} \tag{12}$$

where $D_1 = H_1 + H_2 + H_3$. Now, consider the *interpolating conic* v_1 of the divisor D_1; v_1 intercepts C in the additional points M_1, M_2, M_3, then holds:

$$D_1 - 3P_\infty \cong -(D_2 - 3P_\infty) \tag{13}$$

with $D_2 = M_1 + M_2 + M_3$. Combining (12) and (13) , we get:

$$(D_0 - 4P_\infty) \cong (D_2 - 3P_\infty). \tag{14}$$

Therefore, the degree *three* divisor D_2 will be the reduced divisor of D_0.

A possible reduction algorithm for an effective affine divisor D, of arbitrary *degree*, could be the **Algorithm1** in Table 1 (c.f. pag. 23).

Remark 5.1 *¿From the computational point of view,* ***Algorithm1*** *may be very expensive, since in two of its steps it is necessary to factorize polynomials in* $k[x]$.

Our next objective will be to modify algorithm **Algorithm1** constructing a *factorization free* reduction algorithm with computational complexity linear in $deg(D)$. The modified algorithm we will present may be summarized as follows:

1. Suppose that the divisor D is partitioned as $D = D_0 + E_0 + E_1 + \ldots + E_{N-1}$, with E_j affine and effective, for $j = 1, \ldots, N-1$; and the reduction process (in algorithm **Algorithm1**) is performed by constructing a sequence of effective affine divisors

$$D_0, D_1, D_2, D_3, \ldots, D_{3j}, D_{3j+1}, D_{3j+2} \ldots, D_{3N}, D_{3N+1}, D_{3N+2} \tag{15}$$

where

$$D_{3j} = D_{3(j-1)+2} + E_{(j-1)},$$

for $j = 1, \dots, N$ and

$$D_{3j} - 4P_\infty \cong -(D_{3j+1} - deg(D_{3j+1})P_\infty) \cong (D_{3j+2} - deg(D_{3j+2})P_\infty)$$

with, $0 \leq deg(D_{3j+1})$, $deg(D_{3j+2}) \leq 3$, $deg(D_{3j}) = 4$ and $deg(E_{j-1}) = 4 - deg(D_{3j+2})$. Hence,

$$D - deg(D)P_\infty \cong (D_{3N+2} - deg(D_{3N+2})P_\infty)$$

and D_{3N+2} is the reduction of D.

2. If the divisors D_h, $h = 0, \dots, 3N+2$, are in $\mathcal{D}_\infty(2,4)$ we will assign to D_h its coordinates $\overline{D}_h = \Phi(D_h)$. Then we obtain a sequence

$$\overline{D}_0, \overline{D}_1, \overline{D}_2, \overline{D}_3, \dots, \overline{D}_{3j,} \overline{D}_{3j+1}, \overline{D}_{3j+2} \dots, \overline{D}_{3N}, \overline{D}_{3N+1}, \overline{D}_{3N+2}. \quad (16)$$

3. The basic idea is: given $\overline{D}_0$ (resp. D_0), depending on whether $D_0 \in \mathcal{D}_0(2,4)$ or not, we compute $\overline{D}_h$ or D_h, for $h \geq 1$, recursively, from the previous divisors in the sequences (15) and (16). The recursive computation of the D_h and $\overline{D}_h$ will be done, in the worst case, by solving a small (of dimension at most 4×4) k-defined linear system in each step. Finally, known $\overline{D}_{3N+2} = (u_{3N+2}, v_{3N+2}, w_{3N+2})$ we recover the points in $supp(D_{3N+2})$ after Lemma 4.5.

Remark 5.2 *Given $\overline{D}_{3j+1}, \overline{D}_{3j+2}$, we can prove (c.f. [5]) the equalities:*

$$v_{3j+1} = v_{3j+2} \quad (17)$$

and

$$u_{3j+2} = \left(\frac{R_y(v_{3j+1}, C)}{u_{3j+1}}\right)^* \quad (18)$$

$$w_{3j+2} = \left(\frac{R_x(v_{3j+1}, C)}{w_{3j+1}}\right)^* \quad (19)$$

where $(**)^*$ means that the polynomial $**$ is divided by the coefficient of its leading term. Note, also, that if v_{3j+1} does not depends explicitly on x then

$$w_{3j+2} = w_{3j+1}. \quad (20)$$

Lemma 5.3 *Let be $D_{3j} \in Div^{+,4}$, explicitly known, then we can compute:*

1. *$\overline{D}_{3j}$ provided $D_{3j} \in Div_0^{+,4}$.*
2. *$\overline{D}_{3j+1}$ and $\overline{D}_{3j+2}$ provided $D_{3j} \notin Div_0^{+,4}$.*

Proof.

1. We compute u_{3j+1} and w_{3j+1} as in (9) and (10) and v_{3j+1} by solving linear systems of sizes at most 4×4.
2. Necessarily $D_{3j} = P_1 + \sigma P_1 + P_2 + \sigma P_2$, with $P_1 \neq \sigma^k P_2$, $k = 1, 2$. Then $D_{3j+1} = \sigma^2 P_1 + \sigma^2 P_2$, hence we compute u_{3j+1} and w_{3j+1} as in (9) and (10). The *interpolating conic* v_{3j+1} is, clearly, the line joining $\sigma^2 P_1$ with $\sigma^2 P_2$ (in case $P_1 = P_2$, the tangent line to $\sigma^2 P_1$). Known $\overline{D}_{3j+1} = (u_{3j+1}, v_{3j+1}, w_{3j+1})$ we compute $\overline{D}_{3j+2} = (u_{3j+2}, v_{3j+2}, w_{3j+2})$ using remark 5.2. □

Lemma 5.4 *Let $\overline{D}_{3j} = (u_{3j}, v_{3j}, w_{3j})$ be the coordinates of a divisor D_{3j} in $Div_0^{+,4}(C)$, then, one of the following possibilities holds:*

1. *we can compute*
   $\overline{D}_{3j+1} = (u_{3j+1}, v_{3j+1}, w_{3j+1})$ and $\overline{D}_{3j+2} = (u_{3j+2}, v_{3j+2}, w_{3j+2})$,
   with v_{3j+1} (and therefore v_{3j+2}) dependent on y.
2. *we can compute D_{3j+2} explicitly.*

(it is not necessary to know D_{3j} explicitly.)

Proof. It is necessary to consider the cases:

1. Case $v_{3j}(x, y)$ is linear. Then the points in *supp*(D_{3j}) are collinear and $D_{3j} - 4P_\infty \cong 0$, hence $D_{3j+2} = 0$.
2. Case $v_{3j}(x, y)$ is a conic not factorizing in linear factors (i.e. $v_{3j}(x, y) = a_{20}x^2 + a_{10}x + a_{01}y + a_{11}xy + a_{00}$ with $a_{11}^2 a_{00} + a_{01}^2 a_{20} - a_{11}a_{01}a_{10} \neq 0$). We begin computing u_{3j+1} and w_{3j+1} using (18) and (19). To recover $v_{3j+1}(x, y) = b_{20}x^2 + b_{10}x + b_{00} + b_{01}y$, we solve the 4×4 linear system

   $$R_y(v_{3j}, v_{3j+1}) = \lambda u_{3j+1} \text{ where } \lambda \text{ is a constant} \neq 0. \tag{21}$$

   This system has determinant $a_{11}^2 a_{00} + a_{01}^2 a_{20} - a_{11}a_{01}a_{10} \neq 0$, hence, it has a unique solution. Selecting λ conveniently we normalize v_{3j+1}.

3. Case $v_{3j}(x,y)$ is a conic that factorizes in linear factors (i.e. $v_{3j}(x,y) = r_1(x,y)(x+a_{01}/a_{11})$ with $r_1(x,y) = (a_{20}x + a_{11}y + a_{10} - a_{20}a_{01}/a_{11}))$

   (a) If $(x+a_{01}/a_{11})^2 \mid u_{3j}$, then $D_{3j} = P_1+P_2+P_3+\sigma P_3$ with P_1, P_2, P_3 unknown. In this case, as in case 2, we will try to compute $\overline{D}_{3j+1}$. First we compute u_{3j+1} and w_{3j+1}. Clearly, we can not use the system (21) to recover v_{3j+1}. Next, we find $\sigma^2 P_3$: $x_3 = -a_{01}/a_{11}$ and $\xi^2 y_3$ is the root of the linear polynomial

   $$L = \frac{w_{3j+1}}{g.c.d(R_x(r_1, C), w_{3j+1})}$$

   if $g.c.d(R_x(r_1, C), w_{3j+1})$ is a polynomial of *degree* 2. If it is not the case that means $\sigma^2 P_3$ is a root of r_1 and substituting x_3 in r_1 we recover $\xi^2 y_3$. Once we have $\sigma^2 P_3$, we must consider the cases:

      i. If P_3 (resp. σP_3) anulates $r_1(x,y)$ then the underlying divisor D_{3j} is collinear and as the polynomial $u_{3j+1}/(x+a_{01}/a_{11})^2$ is linear we may recover the other interception point, M, of $r_1(x,y)$ with C. Clearly, $D_{3j+2} = \sigma M + \sigma^2 M + P_3$ (resp. $D_{3j+2} = \sigma M + \sigma^2 M + \sigma P_3$)

      ii. we try to find v_{3j+1} as the solution of the 4×4 linear system

      $$\begin{array}{c} v_{3j+1}(\sigma^2 P_3) = 0 \\ R_y(v_{3j+1}, r_1) = \lambda(u_{3j+1}/(x+a_{01}/a_{11})) \end{array} \tag{22}$$

      This system has determinant $(a_{11})^2 \cdot r_1(\sigma^2 P_3)$ which if different from zero iff $r_1(\sigma^2 P_3) \neq 0$. If this is the case, we can recover v_{3j+1} and $\overline{D}_{3j+1}$. Otherwise, $(r_1(x,y))_0 \succeq P_1 + P_2 + \sigma^2 P_3 + M$ and we can recover M: x_M is the root of the linear polynomial

      $$L = \frac{u_{3j+1}}{(x+a_{01}/a_{11})^2},$$

      and evaluating x_M in r_1 recover the y_M. Now, $D_{3j+1} = 2 \cdot \sigma^2 P_3 + M$. and we may find v_{3j+1} from one of the systems:

      $$\begin{array}{l} v_{3j+1}(\sigma^2 P_3) = 0 \quad \text{of order two} \\ v_{3j+1}(M) = 0 \end{array} \tag{23}$$

if $\sigma^2 P_3 \neq M$ (with determinant $-3\xi y_3^2 (x_3 - x_M)^2 \neq 0$) or

$$v_{3j+1}(\sigma^2 P_3) = 0 \quad \text{of order three} \tag{24}$$

if $\sigma^2 P_3 = M$ (with determinant $-54\xi^2 y_3^7 \neq 0$)

(b) If $(x + a_{01}/a_{11})^2 \nmid u_{3j}$ the unknown D_{3j} is necessarily equal to $D_{3j} = P_1 + P_2 + P_3 + P_4$ with, let's say, P_1, P_2, P_3 collinear (i.e. $(r_1(x,y))_0 \succeq P_1 + P_2 + P_3$), then,

$$\begin{aligned} D_{3j} - 4P_\infty &\cong -(\sigma P_4 + \sigma^2 P_4 + M - 3P_\infty) \\ &\cong (\sigma M + \sigma^2 M + P_4 - 3P_\infty) \end{aligned}$$

where M is the fourth point in which $r_1(x,y)$ intersects C. To find P_4 and M we proceed as follows: $x_4 = -a_{01}/a_{11}$, x_M is the root of the linear polynomial

$$L_M = \frac{R_y(r_1, C)(x + a_{01}/a_{11})}{u_{3j}},$$

if r_1 depends on x, then y_M is obtained evaluating r_1 in x_M and y_4 is the root of the lineal polynomial

$$L_1 = \frac{w_{3j}(y - y_M)}{R_x(r_1, C)},$$

otherwise, y_M is the solution (in y) of $r_1 = 0$ and y_4 is the root of the linear polynomial

$$L_1 = \frac{w_{3j}}{(y - y_M)^3},$$

Hence we may recover $D_{3j+2} = \sigma M + \sigma^2 M + P_4$ explicitly.

In those cases where we have computed $\overline{D}_{3j+1}$ then using remark 5.2, we may compute $\overline{D}_{3j+2}$. □

Lemma 5.5 *Given $\overline{D}_{3j+1} = (u_{3j+1}, v_{3j+1}, w_{3j+1})$ and $\overline{D}_{3j+2} = (u_{3j+2}, v_{3j+2}, w_{3j+2})$ and known the divisor E_{j-1} then, exactly one of the following cases holds:*

1. *we can compute $\overline{D}_{3(j+1)} = (u_{3(j+1)}, v_{3(j+1)}, w_{3(j+1)})$ explicitly.*

2. *we can compute* $\overline{D}_{3(j+1)+1}$ *and* $\overline{D}_{3(j+1)+2}$ *explicitly.*

3. *we can compute the* $D_{3(j+1)+2}$ *explicitly and it is* k*-rational.*

Proof. The strategy will be try to compute $\overline{D}_{3(j+1)}$ if possible, if it is not possible then we are in the other cases. First, we compute $u_{3(j+1)}$ and $w_{3(j+1)}$ as

$$
\begin{aligned}
u_{3(j+1)} &= u_{3j+2} \prod_{P_i \in supp(E_{j-1})} (x - x_i), && (25) \\
w_{3(j+1)} &= w_{3j+2} \prod_{P_i \in supp(E_{j-1})} (y - y_i), && (26)
\end{aligned}
$$

then, we try to find $v_{3(j+1)}$ from the linear system

$$
\begin{cases} v_{3(j+1)}(P_i) = 0 & \text{with } P_i \in supp(E_{j-1}) \\ R_y(v_{3j+2}, v_{3(j+1)}) = \lambda u_{3j+2} & \lambda \text{ a non-zero contant.} \end{cases} \qquad (27)
$$

We must consider the following cases:

1. Case v_{3j+2} linear (i.e. $v_{3j+2} = b_{10}x + b_{00} + y$). Then $E_{j-1} = P_{01} + P_{02}$ and the system (27) has determinant equal to

$$
\begin{array}{ll} -3y_{01}^2 \cdot v_{3j+2}(P_{01})^2 & \text{if } P_{01} = P_{02} \\ (x_{01} - x_{02}) \cdot v_{3j+2}(P_{01}) \cdot v_{3j+2}(P_{02}) & \text{if } P_{01} \neq P_{02} \end{array}
$$

   then, we have to consider the excluding cases:

   (a) Case $u_{3j+2}(P_{01})$ or $u_{3j+2}(P_{02}) = 0$. Then as u_{3j+2} is of degree 2 we can recover D_{3j+2} without making factorizations, then holds $D_{3(j+1)} = D_{3j+2} + P_{01} + P_{02}$ and we may apply lemma 5.3.

   (b) Case $v_{3j+2}(P_{01}) = 0$ and $u_{3j+1}(P_{01}) = 0$ (resp. $v_{3j+2}(P_{02}) = 0$ and $u_{3j+1}(P_{02}) = 0$), then the divisor $D_{3(j+1)}$ is a collinear divisor and we can compute the other point M in which v_{3j+2} intercepts C. Then $D_{3j+2} = \sigma M + \sigma^2 M + P_{02}$ (resp. $D_{3j+2} = \sigma M + \sigma^2 M + P_{01}$).

   (c) Case $P_{01} = \sigma P_{02}$, then set $v_{3(j+1)} = (x - x_{01}) \cdot v_{3j+2}$

   (d) Otherwise, the system (27) is solvable.

2. Case v_{3j+2} is a conic (i.e. $v_{3j+2} = b_{20}x^2 + b_{10}x + b_{00} + y$, $b_{20} \neq 0$) and $E_{j-1} = P_{01}$. Then, we begin computing $u_{3(j+1)}$, $w_{3(j+1)}$ as in (25) and (26), respectively. Now, the system (27) has determinant $b_{20} \cdot v_{3j+2}(P_{01})$ and we have the cases:

   (a) if $v_{3j+2}(P_{01}) \neq 0$ we recover $w_{3(j+1)}$ from (27).

   (b) if $v_{3j+2}(P_{01}) = 0$ and $u_{3j+1}(P_{01}) = 0$, clearly $v_{3(j+1)} = v_{3j+2}$.

   (c) if $v_{3j+2}(P_{01}) = 0$ and $u_{3j+2}(P_{01}) = 0$ we look for $w_{3(j+1)}$ in the system

$$\begin{cases} v_{3(j+1)}(P_{01}) = 0 \text{ of order two.} \\ R_y(v_{3j+2}, v_{3(j+1)})/(x - x_{01}) = \lambda\left(u_{3j+2}/(x - x_{01})\right), \ \lambda \neq 0 \end{cases} \tag{28}$$

      i. In case P_{01} is not a ramification point, the previous system has determinant

$$b_{20}(6y_{01}^2 x_{01} b_{20} + 3y_{01}^2 b_{10} + p_4^I(x_{01})), \tag{29}$$

      this expression is equal to zero if and only if v_{3j+2} has a zero of order *two* in P_{01}. If it is the case, then, as u_{3j+2} is of degree *three*, $u_{3j+2}/(x-x_{01})^2$ is linear in x and we can recover (without factorizing) the other point P_2 in D_{3j+2}, and we apply lemma 5.3 to $D_{3(j+1)} = 3P_{01} + P_2$. Otherwise we solve (28) to find $v_{3(j+1)}$.

      ii. In case P_{01} is a ramification point, the determinant of (28) is b_{20}, hence, we can solve for $v_{3(j+1)}$. □

Combining lemmas (5.3,5.4,5.5) we can construct the algorithm **Algorithm2** (see Table 2 in pag. 24) which is the announced efficient modification to algorithm **Algorithm1** (see Table 1).

Proposition 5.6 *Given the divisor D, the **Algorithm 2** computes the reduced divisor of D making $O(deg(D))$ operations in k and only one factorization of a polynomial, of degree at most 3 in $k[x]$. Morover, if the ground field k is $\mathbb{F}_q$, the constant c that realizes $O(deg(D))$ satisfies:*

$$c \leq 2(4\log_2(q))^3. \tag{30}$$

Proof. The fact that the algorithm in Table 2 makes the reduction of D is an inmediate consequence of lemmas (5.3,5.4,5.5). The complexity in every iteration of algorithm is $O(1)$ operations in k, hence, the total cost is $O(deg(D))$. Moreover, in the worst case, in lemmas (5.3,5.4,5.5) the most expensive computations are done solving linear systems of order (at most) 4×4. Hence, in each iteration of the algorithm we have to solve (at most) 2 linear systems of sizes (at most) 4×4, which give the estimate of (30). $\square$

Let's illustrate with an example the application of **Algorithm 2**.

Example 5.7 *Let $p = 37$, $k = \mathbb{F}_p$ and $p_4(x) = x^4 + 2x$. The $\mathcal{L}$-polynomial of C_{p_4} is*

$$\mathcal{L}(t) = 50653t^6 + 24642t^5 + 6660t^4 + 1225t^3 + 180t^2 + 18t + 1$$

and the cardinal of the group of k-rational points of the Jacobian, $J_p(C_{p_4})$, of C_{p_4} is

$$\# \left| J_p(C_{p_4}) \right| = \mathcal{L}(1) = 3 \cdot 27793.$$

The group $J_p(C_{p_4})$ is cyclic: the curve C_{p_4} has only one k-rational affine ramification point $R_1 = (0 : 0 : 1)$ and the calss $[P_1 - P_\infty]$, where P_1 is any other affine point, generates $J_p(C_{p_4})$. Let $P_1 = (5 : 29 : 1)$ then the explicit computation of the reduction of $7 \cdot [P_1 - P_\infty]$ is shown in Table 3 . Now, after lemma 4.5, (applied to $\overline{D}_{11}$) we recover the reduced divisor

$$D_f = P_{1f} + P_{2f} + P_{3f}$$

where

$$\begin{aligned}
P_{1f} &= (33\beta^2 + 6\beta + 10 : 5\beta^2 + 17\beta + 1 : 1), \\
P_{2f} &= (34\beta^2 + 8\beta + 10 : 13\beta^2 + 35\beta + 1 : 1), \\
P_{3f} &= (7\beta^2 + 23\beta + 10 : 19\beta^2 + 22\beta + 1 : 1),
\end{aligned}$$

and $k(\beta)$ is an algebraic extention of k defined by the k-irreducible polynomial $z^3 + 2$.

6 Further Remarks.

6.1 Improving the Complexity

In fact the complexity estimate given in (30) is an overestimate of the real complexity by the following reasons:

1. We can make an exhaustive analysis of all the possible linear systems of equations and give explicit formulas connecting the divisors with their coordinates and the successive coordinates. This translates the problem of solving linear systems to the evaluation of some rational formulas. Moreover, since the *interpolating conics* v_i (and the u_i, w_i) are unique up constant non-zero factors then, the above mentioned formulas could be rewriten in such a way that they are polymonials in k, hence, they do not involve divisions in k. Therefore, we need only to use the arithmetic of k as ring, not as a field, and this reduces the complexity of the algorithm.

2. In several steps of the **Algorithm 2** it jumps from $\overline{D}_0$ to $\overline{D}_2$ (resp. to D_5) by solving one linear system (resp. performing only elemetary polynomial operations). Clearly, this reduces the complexity of the computations. Computer experiments show that this cases are not infrequent (specially in the case when the divisor to reduce is a multiple of a point).

3. In the special case when $D = N \cdot P_1$ it is possible to design especial strategies: suppose that in some intermediate step of the algorithm we obtain a divisor D_2 (resp. a D_5) explicitly, i.e. D_2 (resp. D_5) is the reduction of $N_1 \cdot P_1$, for certain $N_1 < N$. Then, it is possible to substitute the original problem (i.e. to find the reduction of $D = NP_1$) by the new one of finding the reduction of $a_1 \cdot D_2 + b_1 \cdot P_1$ (resp. $a_1 \cdot D_5 + b_1 \cdot P_1$) , where $N = a_1 \cdot N_1 + b_1$. If N_1 is sufficiently big then, since $\deg(D_2) \leq 3$ (resp. $\deg(D_5) \leq 3$) the original problem is considerablely reduced. Proceeding recursively the complexity of computing the reduction of a large multiple of a point could be dramaticaly reduced.

The next example illustrates the discution in 3:

Example 6.1 *(With the same notation of example 5.7) Let's compute the reduction of* $D = 27793 \cdot P_1$, $P_1 = (5:29:1)$. *First we obtain:* $35 \cdot (P_1 - P_\infty) \cong (P_{11} + P_{12}) - 2 \cdot P_\infty$, *where* $P_{11} = (5:31:1)$ *and* $P_{12} = (19:2:1)$, *then*

$$D = 27793 \cdot (P_1 - P_\infty) \cong 794 \cdot (P_{11} + P_{12}) + 3 \cdot P_1 - 797 \cdot P_\infty.$$

We find that $35 \cdot (P_{11} - P_\infty) \cong (P_{111} + P_{112}) - 2 \cdot P_\infty$ *and* $35 \cdot (P_{12} - P_\infty) \cong (P_{121} + P_{122}) - 2 \cdot P_\infty$, *where* $P_{111} = (19:20:1)$, $P_{112} = (5:14:1)$, $P_{121} = (19:20:1)$ *and* $P_{122} = (13:18:1)$, *then*

$$\begin{aligned} 794(P_{11} + P_{12} - P_\infty) \cong & \quad 22(P_{111} + P_{112} + P_{121} + P_{122}) \\ & + \quad 24(P_{11} + P_{12}) - 136P_\infty, \end{aligned}$$

and the computation of the reduction of $D = 27793 \cdot P_1$ *is simplified to the computation of the reduction of the divisor*

$$D_1 = 22 \cdot (P_{111} + P_{112} + P_{121} + P_{122}) + 24 \cdot (P_{11} + P_{12}) + 3 \cdot P_1,$$

which is of degree 139. Finally, the reduction of D_1 *is* $D_f = (0:0:1)$. *Then, as the class* $[D_f - P_\infty]$ *is a 3-torsion on* $J_p(C_{p4})$, *the class* $[P_1 - P_\infty]$ *is a generator of* $J_p(C_{p4})$ *and* $J_p(C_{p4})$ *is a cyclic group.*

6.2 Comparison with Cantor's Algorithm for Hyperelliptic Curves

Suppose given an hyperelliptic curve (of genus *three*) and a Picard curve over the same ground field k. When computing the reduction of small divisors D both algorithms have similar complexities. The more important differences appears in the computation of the reduction of a large divisor D (in particular in the computation of a large multiples of a point).

1. Our algorithm has less memory requirements: Cantor's algorithm (c.f. [1], [12]) associates polynomials coordinates to D, if $D = M \cdot P_1$ with M big, it has to operate (at least in the inicial steps) with large poynomials; in our algorithm it is only necessary to store the point P_1 and the value M.

2. When computing large multiples of a point our algorithm could be faster than Cantor's algorithm: applying the tecniques mentioned in 1 and 3 of 6.1 we can lower significantly the complexity of computing large multiples of a point. No such tecnique, is known by the authors for Cantor's algorithm in the hyperelliptic case.

In summary, we can expect that good implementation of our algorithm could be as fast as Cantor's algorithm. Additionally it has the advantage of requiring less memory storage.

6.3 Comparison with the General Algorithm of Huang and Ierardi

It is more difficult to compare our algorithm with the fairly general algorithm of Huang and Ierardi (c.f. [11]). The reasons are several:

1. The approach they follow is different: they solve the effective Riemann-Roch problem and then, apply this to solve the problem of the addition (reduction).

2. It is difficult (at least for us) from the paper [11] to estimate the real complexity of the algorithms they present when applied to Picard curves, for intance, it is difficult to estimate how big is the constant involved in their $O(deg(D))$ complexity estimate.

3. We don't know any references to effective implementation of this algorithm.

In spite of this difficulties we can quote the following:

1. Our algorithm (as Cantor's algorithm) is completelly deterministic: it does not requiere to make probabilistic searches, hence, it has no limitations on the cardinality of ground field k.

2. Our algorithm is specific for Picard curves. Consequently, it uses (and reflects) special geometric features of this curves that permit us to diminish the complexity: our algorithm handles very efficiently cases in which appears collinearity of divisors, we obtained also efficient techniques to compute multiples of a point, etc.

By the above reasons one may expect that our algorithm is faster and better in the Picard curves case.

Acknowledgements

We wish to thank R.-P. Holzapfel, for his valuable comments, discussions and encouragements. Also, to G. Frey and U. Krieger for their valuable comments. This work was partially supported by a DFG grant.

Last but not least, the first and second authors want to thank the third author for his warm hospitality during their stay at U.A.G, Guadeloupe.

References

[1] Cantor, D., "*Computing in the Jacobian of a hyperelliptic curve,*" Math. of Computation, 48 (1987), 95-101.

[2] Estrada Sarlabous. J, "*Higher differentials on Cyclic Curves,*". Math. Nachr. 135 (1988), 311-317.

[3] Estrada Sarlabous. J, "*On the Jacobian Varieties of Picard Curves Defined over Fields of Characteristic p,*". Math. Nachr. 152 (1991), 329-340.

[4] Estrada Sarlabous. J., "*A finiteness theorem for Picard curves with good reduction,*". Appendix I of *Ball models and some Hilbert Problems* by R.-P. Holzapfel. Lectures in Mathematics. Birkhäuser-Verlag, (1995).

[5] Estrada Sarlabous. J, Reinaldo Barreiro. E, Piñeiro Barceló. J.A.,. "*On the Jacobian Varieties of Picard curves: explicit Addition Law and Algebraic Structure,*" (to appear in Math. Nachr.), Preprint Nr. 95-5 Humbold Univ. zu Berlin, 1995.

[6] Estrada Sarlabous. J., Piñeiro Barceló. J.A., "*Decoding of codes in Picard curves,*". submitted to Math. Nachricten 1997.Preprint Nr. 96-30 Humbold Univ. zu Berlin, 1996.

[7] Holzapfel, R.-P., "*Geometry and arithmetic around Euler partial differential equations,*". Dt. Ver. d. wiss., Berlin/Reidel Publ. Comp., Dordrecht (1986).

[8] Holzapfel, R.-P., "*On the algebraic value of the Picard modular function,*". Proc. Special. Diff .Equations, Arkata (1991).

[9] Holzapfel, R.-P., "*Transcendental Ball Points of Algebraic Picard Integrals,*". Math. Nachr. 162 (1993).

[10] Holzapfel, R.-P., *Ball models and some Hilbert problems.* Lectures in Mathematics. Birkhäuser-Verlag (1995).

[11] Huang, M.-D and Ierardi, D.J., "*Efficient algorithms for the effective Riemann-Roch problem and for addition in the Jacobian of a curve,*". Proc. of the twenty-first ACM Symp. on the fundations of Computer Science, (May 1991).

[12] Koblitz, N., *Hyperelliptic cryptosystems*, Journal of cryptology 1, pp. 139-150.

[13] Mumford, D., *Tata Lectures on Theta II. Jacobian theta functions and differential equations.* Progress in Math, Vol.42, Birkhäuser Verlag (1984).

Ernesto Reinaldo Barreiro
Jorge Estrada Sarlabous
Department of Geometry and Combinatorics.
CEMAFIT/ICIMAF, Calle E No. 309, esquina 15,
Vedado, La Habana, Cuba

Jean-Pierre Cherdieu
Département de Mathématiques et Informatique
Université des Antilles et de la Guyane
Campus de Fouillole, F97159 Pointe-à-Pitre

e-mails:
alejo@cidet.icmf.inf.cu
matdis@cidet.icmf.inf.cu
Jean-Pierre.cherdieu@univ-ag.fr

Algorithm1 (receives D and returns D_f)

1-**If** $deg(D) \leq 3$ **then** D is already reduced, set $D_f := D$ and go to **End**.
else take $D_0 \preceq D$, $deg(D_0) = 4$ and set $D = D - D_0$.

2-Compute the *interpolating conic* v_0 of D_0.

3-Factorize $R_y(v_0, C)$ (resultant with respect to y) to obtain the x-coordinates of the points on $supp(D_1)$, using v_0 compute their y-coordinates.

4-Known D_1 compute the conic v_1 interpolating C at $D_1 + 2P_\infty$.

5-**If** $deg(D) < 4 - deg(D_2)$ **then** set $D_f = D_2 + D$ and go to **End**. **else** take $E_0 \preceq D$, $deg(E_0) = 4 - deg(D_2)$, set $D_3 := D_2 + E_0$, $D_0 := D_3$ and go to 2.

End Return(D_f)

Table 1: **Algorithm1**: the naive one

Algorithm2 (receives D and returns D_f)

1-**if** $deg(D) < 4$ **then** set $D_f = D$ and go to **End.**

2- Set $D_0 = P_1 + P_2 + P_3 + P_4$.

3- **if** $D_0 \in Div_0^{+,4}$ **then** compute $\overline{D}_0$.

4- **else** compute $\overline{D}_1$, $\overline{D}_2$ and go to SubAlg1.

5- Given $\overline{D}_0$ apply lemma 5.4 to obtain:

5.a- D_2 explicitly. if $deg(D) + D_2 < 4$ **then** set $D_f = D + D_2$ and go to **End**. else set $D_0 = D_2 + E_0$, $D = D \setminus E_0$ and go to 3.

5.b- $(\overline{D}_1, \overline{D}_2)$ explicitly **then** go to SubAlg1.

SubAlg1 (given $\overline{D}_1$ and $\overline{D}_2$))

S1 **if** $deg(D) + deg(v_2) < 4$ call SubFactor$(D, \overline{D}_2)$

S2 **else** select E_0, $deg(E_0) + deg(v_2) = 4$, $E_0 \preceq D_0$, set $D = D \setminus E_0$ and apply lemma 5.5. We have the following possibilities:

a) we obtain $\overline{D}_3$. **then** set $\overline{D}_0 = \overline{D}_3$ go to 5.

b) we obtain $\overline{D}_4$ and $\overline{D}_5$. **then** put $\overline{D}_1 = \overline{D}_4$, $\overline{D}_1 = \overline{D}_4$ and go to S1.

c) we obtain D_5 explicitly. if $deg(D) + D_5 < 4$ **then** set $D_f = D + D_5$ and go to **End**. **else** set $D_0 = D_5 + E_0$, $D = D \setminus E_0$ and go to 3.

EndSubAlg1

SubFactor$(D, \overline{D}_2)$

Using lemma 4.5 recover D_2, **then** set $D_f = D + D_2$ and go to **End**.

EndSubAlg1

End Return(D_f)

Table 2: **Algorithm2**: the efficient one

D_i	$\overline{D}_i$	E_j
$D_0{=}4{\cdot}P_1$	$\overline{D}_0{=}(x^4{+}17x^3{+}2x^2{+}18x{+}33,x^2{+}14x{+}2y{+}xy{+}35,y^4{+}32y^3{+}14y^2{+}13y{+}26)$	—
$D_1{=}?$	$\overline{D}_1{=}(x^3{+}27x^2{+}2,x^2{+}9x{+}21y{+}17,y^3{+}15y^2{+}30y{+}20)$	—
$D_2{=}?$	$\overline{D}_2{=}(x^3{+}9x{+}33,x^2{+}9x{+}21y{+}17,y^3{+}28y^2{+}14y{+}26)$	$E_0{=}P_1$
$D_3{=}?$	$\overline{D}_3{=}(x^4{+}32x^3{+}9x^2{+}25x{+}20,27x^2{+}14x{+}3y{+}xy{+}22,y^4{+}36y^3{+}16y^2{+}27y{+}23)$	—
$D_4{=}?$	$\overline{D}_4{=}(x^3{+}13x^2{+}28x{+}7,x^2{+}29x{+}24y{+}18,y^3{+}19y^2{+}4y{+}36)$	—
$D_5{=}?$	$\overline{D}_5{=}(x^3{+}19x{+}35,x^2{+}29x{+}24y{+}18,y^3{+}13y^2{+}18y{+}1)$	$E_0{=}P_1$
$D_6{=}?$	$\overline{D}_6{=}(x^4{+}32x^3{+}19x^2{+}14x{+}10,18x^2{+}9x{+}33y{+}xy{+}31,y^4{+}21y^3{+}11y^2{+}34y{+}8)$	—
$D_7{=}?$	$\overline{D}_7{=}(x^3{+}16x^2{+}14x{+}8,x^2{+}22x{+}33y{+}29,y^3{+}31y{+}8)$	—
$D_8{=}?$	$\overline{D}_8{=}(x^3{+}13x^2{+}32x{+}10,x^2{+}22x{+}33y{+}29,y^3{+}5y^2{+}12y{+}31)$	$E_0{=}P_1$
$D_9{=}?$	$\overline{D}_9{=}(x^4{+}8x^3{+}4x^2{+}35x{+}24,32x^2{+}5x{+}11y{+}xy{+}6,y^4{+}13y^3{+}15y^2{+}16y{+}26)$	—
$D_{10}{=}?$	$\overline{D}_{10}{=}(x^3{+}11x^2{+}17x{+}9,x^2{+}6x{+}21y{+}19,y^3{+}9y^2{+}26y{+}15)$	—
$D_{11}{=}?$	$\overline{D}_{11}{=}(x^3{+}7x^2{+}8x{+}18,x^2{+}6x{+}21y{+}19,y^3{+}34y^2{+}32y{+}9)$	$E_0{=}\emptyset$

Table 3: Reduction of the divisor $7 \cdot P_1$, $P_1 = (5 : 29 : 1)$