# Reduced Mumford divisors of a genus 2 curve through its jacobian function field

Eduardo Ruíz Duarte

Johann Bernoulli Institute, University of Groningen, P.O. Box 407 9700 AK,
Groningen, The Netherlands
e.ruiz.duarte@rug.nl
http://www.math.rug.nl

**Abstract.** We explore the function field of the jacobian $\mathbb{J}_{\mathcal{H}}$ of a hyperelliptic curve $\mathcal{H}$ of genus 2 in order to find reduced coordinates to represent points of $\mathbb{J}_{\mathcal{H}}$ and do arithmetic.
We show how this relates to the usual Mumford representation of points of $\mathbb{J}_{\mathcal{H}}$. Moreover we identify the open subsets of $\mathbb{J}_{\mathcal{H}}$ where our reduced coordinates are defined, characterizing the elements which can be reduced and we discuss the group operation with them.

**Keywords:** hyperelliptic curves, Mumford representation, jacobian coordinates

## 1 Introduction

Reducing the representation of elements in a group for cryptography is an important task. Mumford representation of divisors consists of a pair of polynomials that save the information of points in the support of the divisor of a genus $g$ curve $\mathcal{H}$ and its multiplicities in a handy way in order to do arithmetic in the jacobian $\mathbb{J}_{\mathcal{H}}$ of $\mathcal{H}$. The main goal of this paper is to reduce the information needed to represent a divisor class in $\mathbb{J}_{\mathcal{H}}$. The divisor classes in $\mathbb{J}_{\mathcal{H}}$ are represented by $\langle u(x), v(x)\rangle$ where $deg(u) \leq g$, $deg(v) \leq g-1$ and $u$ is monic.

We will restrict to the case $g = 2$, and the information that defines the divisors in this form is given by the coefficients of the polynomials $u$ and $v$. We will prove that we only need one coefficient of $v$ to do arithmetic using the function field of the jacobian $\mathbb{K}(\mathbb{J}_{\mathcal{H}})$.

Let $\mathcal{H}$ be a hyperelliptic curve of genus 2 over a perfect field $\mathbb{K}$ where $char(\mathbb{K}) \neq 2$ given by the model $y^2 = x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$. We will construct an affine variety $\mathbb{J}_{\mathcal{H}}^{Aff} \subset \mathbb{A}^4_{\mathbb{K}}$ which is birational to $\mathbb{J}_{\mathcal{H}}$ to simplify computations in $\mathbb{K}(\mathbb{J}_{\mathcal{H}})$. It is well known that the jacobian $\mathbb{J}_{\mathcal{H}}$ of $\mathcal{H}$ is birational to $Sym^2(\mathcal{H}) = (\mathcal{H} \times \mathcal{H})/\sigma$ where we define $\sigma \in Aut_{\mathbb{K}}(\mathcal{H} \times \mathcal{H})$ as the automorphism that interchanges $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ where $(P, Q) \in \mathcal{H} \times \mathcal{H}$, this means that it acts on the coordinates of the points by $x_1 \leftrightarrow x_2$ and $y_1 \leftrightarrow y_2$.

Working with $\mathbb{K}(Sym^2(\mathcal{H}))$ is relatively easy since $Sym^2(\mathcal{H})$ can be regarded as the set of unordered pairs of points $\{P, Q\}$ on $\mathcal{H}$ where $P = Q$ is allowed.

The variety $\mathbb{J}_{\mathcal{H}}^{Aff}$ will be obtained by describing generators of $\mathbb{K}(Sym^2(\mathcal{H}))$. We want to reduce the space needed to store the Mumford representation of divisor classes and characterize in which cases it is practical. Further, we will analyze $\mathbb{K}(\mathcal{H} \times \mathcal{H})$ as a vector space over $\mathbb{K}(\mathbb{J}_{\mathcal{H}}^{Aff})$.

## 2 Description of $\mathbb{J}_{\mathcal{H}}^{Aff}$

Consider a divisor class $\mathcal{D} \in \mathbb{J}_{\mathcal{H}}$ of the form $\mathcal{D} = [P_1 + P_2 - 2\infty]$, where the affine points on $\mathcal{H}$ are given by $P_i := (x_i, y_i)$ for $i = 1, 2$ and $\mathcal{D}$ is not the zero divisor. Following [Can87,Mum84] we can save the information of a divisor class $\mathcal{D}$ in a unique and handy way, as follows. Write $\mathcal{D} = \langle u(x), v(x) \rangle$, where $u(x)$ is the monic quadratic polynomial with $u(x_1) = u(x_2) = 0$ and $v(x)$ is a polynomial with $\deg(v) \leq 1$ such that $v(x_1) = y_1$ and $v(x_2) = y_2$. This means that $u$ has as roots the $x$ coordinates of the points in the support of $\mathcal{D}$ and $v$ is the line through $P_1$ and $P_2$ which in the case that $P_1 = P_2$, $v$ will be tangent to $\mathcal{H}$ at $P_1$. Clearly $P_1, P_2$ determine $u, v$ and vice versa. Moreover, a field automorphism fixes $\{P_1, P_2\}$ precisely when it fixes the polynomials $u, v$. Explicitly we have that $\mathcal{D} = [P_1 + P_2 - 2\infty]$ corresponds in this representation to:

$$\mathcal{D} = \langle x^2 + Ax + B, Cx + D \rangle.$$

We will be concerned now with the equations that relate $A, B, C, D$, the notation for the function field of $\mathbb{J}_{\mathcal{H}}$ will be $\mathbb{K}(\mathbb{J}_{\mathcal{H}})$.

**Definition 1** *Let $\mathbb{J}_{\mathcal{H}}$ be the jacobian of a hyperelliptic curve $\mathcal{H}$ of genus 2 over $\mathbb{K}$ and consider the following embedding of $\mathcal{H}$ into $\mathbb{J}_{\mathcal{H}}$:*

$$\begin{aligned} \Theta : \mathcal{H} &\to \mathbb{J}_{\mathcal{H}} \\ P &\mapsto [P - \infty] \end{aligned} \tag{1}$$

*We define $\mathbb{J}_{\mathcal{H}}^{Aff} := \mathbb{J}_{\mathcal{H}} \setminus Im(\Theta)$*

As $Im(\Theta)$ is a Zariski closed subset of $\mathbb{J}_{\mathcal{H}}$, its complement in $\mathbb{J}_{\mathcal{H}}$ is the open subset $\mathbb{J}_{\mathcal{H}}^{Aff}$ which is important because it implies that $\mathbb{K}(\mathbb{J}_{\mathcal{H}}^{Aff}) \cong \mathbb{K}(\mathbb{J}_{\mathcal{H}})$.

The object $\mathbb{J}_{\mathcal{H}}^{Aff}$ misses divisor classes of the form $[(x_1, y_1) - \infty]$ which correspond in Mumford representation to $\langle x - x_1, y_1 \rangle$, that is why we will work with points $(A, B, C, D) \in \mathbb{J}_{\mathcal{H}}^{Aff}$ which are defined for divisors classes of the form $[P + Q - 2\infty]$ for $P, Q \neq \infty$.

**Remark:** We are not going to deal with the divisors in $Im(\Theta)$ as they are not part of our affine model and they don't need reduced representation, also following [Lan05], [HC14], divisors in $Im(\Theta)$ have a very small probability of being encountered in the scalar multiplication routine for cryptographic applications.

The coefficients $A, B, C, D$ of a divisor class represented by $\langle u, v \rangle$ are invariant under the action of $\sigma \in Aut_{\mathbb{K}}(\mathcal{H} \times \mathcal{H})$ because we have this symmetry in the jacobian. The points $(A, B, C, D)$ from the open subset $\mathbb{J}_{\mathcal{H}}^{Aff} \subset Sym^2(\mathcal{H})$ which corresponds to a quasi-affine variety $\mathbb{J}_{\mathcal{H}}^{Aff} \subsetneq \mathbb{J}_{\mathcal{H}}$ will be described by the following lemma.

**Lemma 1** *Let $\mathcal{H}$ be a genus 2 curve defined by $y^2 = f(x)$ as before, with $deg(f) = 5$ and $(x_1, y_1), (x_2, y_2) \in \mathcal{H}$ affine points. Assume the divisor class $\mathcal{D} = [(x_1, y_1) + (x_2, y_2) - 2\infty]$ is represented by $\mathcal{D} = \langle u, v\rangle$ then $u \mid f - v^2$ where $deg(v) < deg(u) = 2$ with $u$ monic*

*Proof.* We want to prove that $u \mid f - v^2$, we have that $f(x) = y^2 = v(x)^2$ and then $f(x) - v(x)^2$ has degree 5 and its roots include the $x$-coordinate of the intersection of the line $y - v(x)$ with the curve $\mathcal{H}(x, y) = y^2 - f(x)$, that is $x_1, x_2$. As $u(x)$ has roots $x_1$ and $x_2$ by construction it must divide $f(x) - v(x)^2$, equivalently $f(x) \equiv v(x) \bmod u(x)$. □

With this we have that if $\mathcal{D} = \langle u, v\rangle \in \mathbb{J}_{\mathcal{H}}$ then $f(x) \equiv v(x)^2 \bmod u(x)$ defines the points $(A, B, C, D) \in \mathbb{J}_{\mathcal{H}}^{Aff}$. We now solve this congruence to get the equations of $\mathbb{J}_{\mathcal{H}}^{Aff}$

Using a different function from the Riemann space $\mathcal{L}(2\infty)$ we can eliminate the degree 4 term in $f(x)$ in the model of $\mathcal{H}$ when $char(\mathbb{K}) \neq 2, 5$ and write our hyperelliptic curve of genus 2 as:

$$y^2 = x^5 + a_3x^3 + a_2x^2 + a_1x + a_0 =: f(x) \tag{2}$$

The condition $f - v^2 = 0$ in $\mathbb{K}[x]/(u)$ proven in Lemma 1 that give us the points in $(A, B, C, D) \in \mathbb{J}_{\mathcal{H}}^{Aff}$ means explicitly:

$$x^5 + a_3x^3 + (a_2 - C^2)x^2 + (a_1 - 2CD)x + a_0 - D^2 \equiv 0 \mod x^2 + Ax + B \tag{3}$$

Solving (3) leave us with two hypersurfaces, the intersection of these two are the points $(A, B, C, D) \in \mathbb{J}_{\mathcal{H}}^{Aff}$:

$$\begin{aligned} B^2 + A^4 + a_3A^2 - 3A^2B - a_2A + AC^2 - a_3B - 2DC + a_1 = 0 \\ D^2 - A^3B - a_3AB + 2AB^2 - BC^2 + a_3B - a_0 = 0 \end{aligned} \tag{4}$$

These equations will be useful to define the addition of two points in these coordinates. An interesting modification of these formulæ will be given in the next sections showing that $D$ in $(A, B, C, D)$ can be generated by some rational function $\eta(A, B, C) \in \mathbb{K}(\mathbb{J}_{\mathcal{H}}^{Aff})$ for *most* of the elements of $\mathbb{J}_{\mathcal{H}}^{Aff}$. We will characterize the elements that need additional information to keep the reduction. This rational function $\eta$ will be described in the following sections and will be used to reduce the representation of the points which is one of the main purposes of this paper.

Now, explicitly if we let $\{(x_1, y_1), (x_2, y_2)\} \in Sym^2(\mathcal{H})$ and $x_1 \neq x_2$, the divisor defined by these points is:

$$\mathcal{D} = \langle x^2 - (x_1 + x_2)x + x_1x_2, \frac{y_2 - y_1}{x_2 - x_1}x + \frac{x_2y_1 - x_1y_2}{x_2 - x_1}\rangle$$

So we have that the points in $\mathbb{J}_{\mathcal{H}}^{Aff}$ are:

$$(A, B, C, D) := (-(x_1 + x_2), x_1x_2, \frac{y_2 - y_1}{x_2 - x_1}, \frac{x_2y_1 - x_1y_2}{x_2 - x_1}) \in \mathbb{J}_{\mathcal{H}}^{Aff}.$$

Obviously each coordinate is invariant under the action of $\sigma$.

The following step is to have a birational map between $Sym^2(\mathcal{H})$ and $\mathbb{J}_{\mathcal{H}}^{Aff}$. Let $\{(x_1, y_1), (x_2, y_2)\} \in Sym^2(\mathcal{H})$ and consider the following map:

$$\psi : Sym^2(\mathcal{H}) \dashrightarrow \mathbb{J}_{\mathcal{H}}^{Aff}$$
$$\{(x_1, y_1), (x_2, y_2)\} \mapsto (-(x_1 + x_2), x_1x_2, \frac{y_1 - y_2}{x_1 - x_2}, \frac{x_1y_2 - x_2y_1}{x_1 - x_2})$$

We will prove that $\psi$ is birational, i.e. $\mathbb{K}(Sym^2(\mathcal{H})) \cong \mathbb{K}(A, B, C, D) = \mathbb{K}(\mathbb{J}_{\mathcal{H}})$. The proof involves inclusions of function fields which will be useful in the next sections.

**Proposition 2** *The map $\psi$ is birational.*

*Proof.* We are going to prove $\mathbb{K}(A, B, C, D) = \mathbb{K}(\mathcal{H} \times \mathcal{H})^{\sigma^*}$. We already know that $\mathbb{K}(\mathcal{H} \times \mathcal{H}) = \mathbb{K}(x_1, x_2, y_1, y_2)$ where $y_i^2 = f(x_i)$ and further we have $\mathbb{K}(Sym^2(\mathcal{H})) = \mathbb{K}(\mathcal{H} \times \mathcal{H})^{\sigma^*}$ where $\sigma^* \in Aut(\mathbb{K}(\mathcal{H} \times \mathcal{H}))$ is the interchange of functions $x_1 \leftrightarrow x_2$ and $y_1 \leftrightarrow y_2$.

Let $A = x_1 + x_2, B = x_1x_2, C = \frac{y_2 - y_1}{x_2 - x_1}, D = \frac{x_2y_1 - x_1y_2}{x_2 - x_1}$ which are symmetric and then invariant under $\sigma^*$ justifying the existence of the $\psi^*$ inclusion in the following diagram where the arrows represent inclusions and the numbers the degrees as field extensions.

$$\begin{tikzcd}
\mathbb{K}(\mathcal{H} \times \mathcal{H})^{\sigma^*} \arrow[r, "2"] & \mathbb{K}(\mathcal{H} \times \mathcal{H}) & \mathbb{K}(x_1, x_2) \arrow[l, "4"'] \\
\mathbb{K}(A, B, C, D) \arrow[u, "\psi^*"'] \arrow[r] & \mathbb{K}(A, B, C, D)(x_1 - x_2) \arrow[u] & \\
 & & \mathbb{K}(A, B) \arrow[uu, "2"'] \arrow[uul, "8"] \arrow[ull, "\tau^*"]
\end{tikzcd}$$

Note that $\sigma^*$ restricts to an involution of $\mathbb{K}(x_1, x_2)$, and the fixed field is $\mathbb{K}(x_1, x_2)^{\sigma^*} = \mathbb{K}(A, B)$.

The birationality of $\psi$ means precisely that $\mathbb{K}(A, B, C, D) = \mathbb{K}(\mathcal{H} \times \mathcal{H})^{\sigma^*}$, this will be immediate after showing $[\mathbb{K}(A, B, C, D) : \mathbb{K}(A, B)] = 4$ which is the degree of the field extension induced by $\tau^*$ because the four paths in the diagram from $\mathbb{K}(A, B)$ to $\mathbb{K}(\mathcal{H} \times \mathcal{H})$ must multiply to 8 in their degree extensions given in each arrow.

We are interested in path:

$$\mathbb{K}(A, B) \to \mathbb{K}(A, B, C, D) \to \mathbb{K}(\mathcal{H} \times \mathcal{H})^{\sigma^*} \to \mathbb{K}(\mathcal{H} \times \mathcal{H})$$

If $\tau^*$ induces a degree 4 extension, this path will force $\mathbb{K}(\mathcal{H} \times \mathcal{H})^{\sigma *} = \mathbb{K}(\mathbb{J}_{\mathcal{H}}^{Aff})$, i.e. $\psi$ birational.To prove that $\tau^*$ induces a degree 4 field extension we will prove that $[\mathbb{K}(\mathcal{H}\times\mathcal{H}) : \mathbb{K}(A,B,C,D)] = 2$ using an extension of $\mathbb{K}(A,B,C,D)$ given by $\mathbb{K}(A,B,C,D)(x_1-x_2)$.

It is not difficult to see that $[\mathbb{K}(A,B,C,D)(x_1-x_2) : \mathbb{K}(A,B,C,D)] = 2$. In fact $x_1-x_2$ is a zero of $T^2-(A^2+4B)\in\mathbb{K}(A,B,C,D)[T]$ and since it is not fixed by $\sigma^*$, $x_1-x_2\notin\mathbb{K}(A,B,C,D)$.

We claim that $\mathbb{K}(A,B,C,D)(x_1-x_2)=\mathbb{K}(\mathcal{H}\times\mathcal{H})$. Namely, it is trivial that $\mathbb{K}(A,B,C,D)(x_1-x_2)\subseteq\mathbb{K}(x_1,x_2,y_1,y_2)$, and as $char(\mathbb{K})\neq 2$:

$$x_1=\frac{A+(x_1-x_2)}{2}$$
$$x_2=\frac{A-(x_1-x_2)}{2}$$

shows that $x_1,x_2\in\mathbb{K}(A,B,C,D)(x_1-x_2)$. Then

$$y_1=D+x_1C$$
$$y_2=D+x_2C$$

proves that $\mathbb{K}(\mathcal{H}\times\mathcal{H})=\mathbb{K}(x_1,x_2,y_1,y_2)\subseteq\mathbb{K}(A,B,C,D)(x_1-x_2)$ and then they are equal, forcing $\tau^*$ to induce a degree 4 extension i.e. the $\psi$ is birational. □

With this we have that $\mathbb{K}(\mathbb{J}_{\mathcal{H}}^{Aff})\cong\mathbb{K}(x_1+x_2,x_1x_2,\frac{y_2-y_1}{x_2-x_1},\frac{x_2y_1-x_1y_2}{x_2-x_1})$ with 4 generators.

## 3 Representation of $\mathbb{K}(\mathbb{J}_{\mathcal{H}})$ with 3 generators

For now we have that $\mathbb{K}(\mathbb{J}_{\mathcal{H}})\cong\mathbb{K}(\mathbb{J}_{\mathcal{H}}^{Aff})$ is in terms of 4 generators $A,B,C,D$. We want to reduce this to 3 generators. Recall that the previous diagram implies that

$$[\mathbb{K}(\mathcal{H}\times\mathcal{H}) : \mathbb{K}(\mathbb{J}_{\mathcal{H}})] = 2,$$

because $\mathbb{K}(\mathbb{J}_{\mathcal{H}})=\mathbb{K}(\mathcal{H}\times\mathcal{H})^{\sigma^*}$ by Proposition 2, where $\sigma^*\in Aut(\mathbb{K}(\mathcal{H}\times\mathcal{H})$ is the involution induced by $\sigma\in Aut_{\mathbb{K}}(\mathcal{H}\times\mathcal{H})$. We also consider the map $\xi^*$ of function fields induced by:

$$\begin{aligned}\xi:\mathcal{H}\times\mathcal{H} &\dashrightarrow Sym^2(\mathcal{H})\\ (x_1,y_1,x_2,y_2) &\mapsto (-(x_1+x_2),x_1x_2,\frac{y_1-y_2}{x_1-x_2},\frac{x_1y_2-x_2y_1}{x_1-x_2})\end{aligned}$$

We have the following induced map of function fields due to the birationality of $Sym^2(\mathcal{H})$ and $\mathbb{J}_{\mathcal{H}}$.

$$\begin{aligned}\xi^*:\mathbb{K}(\mathbb{J}_{\mathcal{H}}) &\hookrightarrow \mathbb{K}(\mathcal{H}\times\mathcal{H})\\ f &\mapsto f\circ\xi\end{aligned}$$

So $[\mathbb{K}(\mathcal{H}\times\mathcal{H}) : \xi^*\mathbb{K}(\mathcal{H}\times\mathcal{H})] = [\mathbb{K}(\mathcal{H}\times\mathcal{H}) : \mathbb{K}(\mathbb{J}_{\mathcal{H}})] = 2$.

Now we proceed to reduce the generators of $\mathbb{K}(\mathbb{J}_{\mathcal{H}})$, let $\delta = x_1y_2 + x_2y_1$, we claim

$$\mathbb{K}(A, B, \delta) = \mathbb{K}(A, B, C, D) \cong \mathbb{K}(\mathbb{J}_{\mathcal{H}}). \tag{5}$$

It is clear that the function $\delta$ is invariant under $\sigma$. To have $\mathbb{K}(\mathbb{J}_{\mathcal{H}})$ represented with three generators is enough to prove the following:

$$[\mathbb{K}(A, B, \delta) : \mathbb{K}(A, B)] = [\mathbb{K}(x_1 + x_2, x_1x_2, x_1y_2 + x_2y_1) : \mathbb{K}(x_1 + x_2, x_1x_2)] = 4.$$

Proving this will suffice to prove (5) because if we let $A = x_1 + x_2, B = x_1x_2$, $C = \frac{y_1-y_2}{x_1-x_2}, D = \frac{x_1y_2-x_2y_1}{x_1-x_2}$ and we consider the following diagram where the "?" symbol in the arrows indicates what we claim but we don't know yet:

$$\begin{tikzcd}
\mathbb{K}(A,B,C,D) \arrow[r, "2"] & \mathbb{K}(\mathcal{H}\times\mathcal{H}) \\
\mathbb{K}(A,B,\delta) \arrow[u, "?="] & \\
\mathbb{K}(A,B) \arrow[u, "?4"] \arrow[uu, bend left=60, "4"] \arrow[r, "2"] & \mathbb{K}(x_1,x_2) \arrow[uu, "4", "\mu^*"']
\end{tikzcd}$$

By Proposition 2 we know that the curved arrow has degree 4. If we can prove that $[\mathbb{K}(A, B, \delta) : \mathbb{K}(A, B)] = 4$, we get $\mathbb{K}(A, B, C, D) = \mathbb{K}(A, B, \delta)$. The $\mu^*$ map with degree 4 extension in the diagram is justified by:

$$[\mathbb{K}(\mathcal{H}) : \mathbb{K}(x_1)] = 2 \Rightarrow [\mathbb{K}(\mathcal{H}) \otimes_{\mathbb{K}} \mathbb{K}(\mathcal{H}) : \mathbb{K}(x_1) \otimes_{\mathbb{K}} \mathbb{K}(x_2)] = 4.$$

**Proposition 3** *The minimal polynomial of $\delta = x_1y_2 + x_2y_1 \in \mathbb{K}(x_1, x_2)(y_1, y_2)$ over $\mathbb{K}(x_1, x_2)$ with $y^2 = x^5 + a_3x^3 + a_2x^2 + a_1x + a_0 =: f(x)$, has degree 4, i.e. $\mathbb{K}(A, B)(\delta) = \mathbb{K}(\mathbb{J}_{\mathcal{H}})$*

*Proof.* Let $\mathcal{B} = \{1, y_1, y_2, y_1y_2\}$ be a basis of $\mathbb{K}(x_1, x_2)(y_1, y_2)$ as a vector space over $\mathbb{K}(x_1, x_2)$, and consider the matrix that represents in its columns the coefficients in $\mathbb{K}(x_1, x_2)$ using the basis $\mathcal{B}$ to represent powers of $\delta$, namely $\delta^0, \delta^1, \delta^2, \delta^3$.

$$M = \begin{pmatrix} 1 & 0 & x_1^2f(x_2) + x_2^2f(x_1) & 0 \\ 0 & x_2 & 0 & 3x_1^2x_2f(x_2) + f(x_1)x_2^3 \\ 0 & x_1 & 0 & 3x_2^2x_1f(x_1) + f(x_2)x_1^3 \\ 0 & 0 & 2x_1x_2 & 0 \end{pmatrix}$$

The determinant of this matrix is nonzero i.e. this matrix has rank 4, then $\mathbb{K}(\mathbb{J}_{\mathcal{H}}) = \mathbb{K}(x_1 + x_2, x_1x_2, x_1y_2 + x_2y_1)$ because of the previous diagram. □

Moreover, to get the minimum polynomial of $\delta$, the column for $\delta^4$ in terms of the basis $\mathcal{B}$:

$$b = \begin{pmatrix} x_1^4f(x_2)^2 + 6x_1^2x_2^2f(x_1)f(x_2) + f(x_1)^2x_2^4 \\ 0 \\ 0 \\ 4x_1^3x_2f(x_2) + 4x_1x_2^3f(x_1) \end{pmatrix}$$

Solving the system $M\alpha = b$, where $\alpha = (\alpha_0, \alpha_2, \alpha_3, \alpha_4)^T$, and $\alpha_i \in \mathbb{K}(x_1, x_2)$ we have that

$$\begin{aligned}
\alpha_0 &= -(f(x_1)^2 x_2^4 + x_1^4 f(x_2)^2) + 2x_1^2 x_2^2 f(x_1) f(x_2)\\
\alpha_1 &= 0\\
\alpha_2 &= 2x_2^2 f(x_1) + 2x_1^2 f(x_2)\\
\alpha_3 &= 0.
\end{aligned}$$

Writing $\alpha_0$ and $\alpha_2$ in terms of $A = x_1 + x_2$ and $B = x_1 x_2$ gives us:

$$\begin{aligned}
\alpha_0 =& - A^6B^4 - 2a_3A^4B^4 + 6A^4B^5 + 2a_0A^5B^2 + 2a_1A^4B^3 - a_3^2A^2B^4\\
&+ 10a_3A^2B^5 - 9A^2B^6 + 2a_0a_3A^3B^2 - 10a_0A^3B^3 + 2a_1a_3A^2B^3\\
&- 10a_1A^2B^4 + 4a_3^2B^5 - 8a_3B^6 + 4B^7 - a_0^2A^4 - 2a_0a_1A^3B - 8a_0a_3AB^3\\
&+ 8a_0AB^4 - a_1^2A^2B^2 - 8a_1a_3B^4 + 8a_1B^5 + 4a_0^2A^2B + 8a_0a_1AB^2 + 4a_1^2B^3\\
\alpha_2 =& 2A^3B^2 + 2a_3AB^2 - 6AB^3 + 2a_0A^2 + 2a_1AB + 4a_2B^2 - 4a_0B
\end{aligned}$$

The minimal polynomial of $\delta$ is of degree 4 since $[\mathbb{K}(A, B, \delta) : \mathbb{K}(A, B)] = 4$ by Proposition 3 and is $\delta^4 - \delta^2\alpha_2 - \alpha_0$.

### 3.1 Explicit reduction of Jacobian generators

So far we have proven that we can use 3 generators to represent $\mathbb{K}(\mathbb{J}_{\mathcal{H}})$. We now will see how to work with three coordinates directly in $\mathbb{J}_{\mathcal{H}}$. Recall that the Mumford representation of a point $(A, B, C, D) \in \mathbb{J}_{\mathcal{H}}^{Aff}$ is given by the following coordinates in two cases for our affine model of $\mathbb{J}_{\mathcal{H}}$:

$$\begin{array}{ll}
\text{Case } 1 : D = [(x_1, y_1) + (x_2, y_2) - 2\infty] & \text{Case } 2 : D = [2(x_1, y_1) - 2\infty]\\
A = -(x_1 + x_2) & A = -2x_1\\
B = x_1x_2 & B = x_1^2\\
C = \dfrac{y_1 - y_2}{x_1 - x_2} & C = \dfrac{f'(x_1)}{2y_1}\\
D = \dfrac{x_1y_2 - x_2y_1}{x_1 - x_2} & D = \dfrac{2f(x_1) - x_1f'(x_1)}{2y_1}
\end{array} \tag{6}$$

Consider:

$$\frac{D}{C} = \frac{(x_1y_2 - x_2y_1)(y_1 + y_2)}{{y_1}^2 - {y_2}^2} = \frac{x_1f(x_2) - x_2f(x_1) + y_2y_1(x_1 - x_2)}{f(x_1) - f(x_2)}$$

We have some identities with symmetric polynomials computed in the function field of the curve $\mathcal{H}$ for case 1:

$$\begin{aligned}
s_1(A,B) &:= a_1 - a_2A + a_3(A^2-B) + a_4(2AB-A^3) + A^4 - B(3A^2-B) \\
&= \frac{f(x_1)-f(x_2)}{x_1-x_2} \\
s_2(A,B) &:= 2a_0 - a_1A + a_2(A^2-2B) + a_3(3AB-A^3) + a_4(A^4-4A^2B+2B^2) - A^5 - 5AB^2 + 5A^3B \\
&= f(x_1)+f(x_2) \\
s_3(A,B,C) &:= \tfrac{s_2(A,B)-C^2(A^2-4B)}{2} = y_2y_1 \\
s_4(A,B) &:= a_0 - a_1A + a_2(A^2-B) + a_3(2AB-A^3) + a_4(A^4-B(3A^2-B)) - A(A^2-3B)(A^2-B) \\
&= \frac{x_1f(x_1)-x_2f(x_2)}{x_1-x_2}
\end{aligned} \tag{7}$$

Moreover,

$$x_1f(x_2) - x_2f(x_1) = (x_1-x_2)(f(x_1)+f(x_2)) - (x_1f(x_1) - x_2f(x_2)).$$

This equality we will need to rewrite a part of the numerator of $\frac{D}{C}$.

Putting all together, we can express $D$ in terms of $A, B, C$ and we have:

$$D = \eta(A,B,C) = \frac{C(s_2(A,B) + s_3(A,B,C) - s_4(A,B))}{s_1(A,B)} \tag{8}$$

For case 2 is easy to check that:

$$\begin{aligned}
s_1(A,B) &= f'(x_1) \\
s_2(A,B) &= 2f(x_1) \\
s_3(A,B,C) &= f(x_1) \\
s_4(A,B) &= f(x_1) + x_1f'(x_1) \\
D = \eta(A,B,C) &= \frac{2f(x_1) - x_1f'(x_1)}{2y_1}
\end{aligned} \tag{9}$$

What this means is that we can get all the information of *most* of the divisors on the curve just by looking at the coordinates as elements of $\mathbb{K}(\mathbb{J}_{\mathcal{H}})$ because the four generators used in Mumford representation in the function field are related by a rational function $\eta \in \mathbb{K}(\mathbb{J}_{\mathcal{H}})$.

Consider the following map:

$$\begin{aligned}
\pi : \mathbb{J}_{\mathcal{H}}^{Aff} &\to \mathbb{A}^3 \\
(A,B,C,D) &\mapsto (A,B,C)
\end{aligned}$$

Let $\breve{\mathbb{J}}_{\mathcal{H}} := Im(\pi)$. We will study the failure of this map to be injective in order to characterize the divisors which can be used with 3 coordinates, and this will be shown to depend on the domain of definition of $\eta$.

## 4 Special reduced divisors

We have been working with $\mathbb{K}(\mathbb{J}_{\mathcal{H}})$ to get information of the coordinates that represent points of $\mathbb{J}_{\mathcal{H}}$. We have seen already that the coefficients of the polynomials that define the Mumford representation of a divisor as functions in $\mathbb{K}(\mathbb{J}_{\mathcal{H}})$ are related by the rational function $\eta \in \mathbb{K}(\mathbb{J}_{\mathcal{H}})$. In this section we will analyze when the first three coordinates of a point $(A, B, C, D) \in \mathbb{J}_{\mathcal{H}}^{Aff}$ can generate the fourth under some geometrical conditions in order to do arithmetic and represent jacobian points with the smaller object $\breve{\mathbb{J}}_{\mathcal{H}}$.

**Definition 2** *Let $\mathfrak{D} := (A, B, C, D) \in \mathbb{J}_{\mathcal{H}}^{Aff}$. $\mathfrak{D}$ is called* ***special*** *if*

$$\#\pi^{-1}(A, B, C) \neq 1.$$

The reason for working with $\breve{\mathbb{J}}_{\mathcal{H}}$ is because working directly with $\mathbb{J}_{\mathcal{H}}$ is usually difficult due to the known complicated embeddings of the jacobian to $\mathbb{P}^n$, see for example [Fly90] or [Gra90]. The main problem of $\mathbb{J}_{\mathcal{H}}^{Aff}$ in terms of cryptographic applications is that this affine part of the Jacobian loses information, as we have $\mathbb{J}_{\mathcal{H}}^{Aff} = \mathbb{J}_{\mathcal{H}} \setminus Im(\Theta)$.

Let $\mathcal{H}$ be a genus 2 curve given by the equation in (2) and $\mathbb{J}_{\mathcal{H}}$ its jacobian over $\mathbb{K}$. Let $\mathfrak{D} = (A, B, C, D) \in \mathbb{J}_{\mathcal{H}}^{Aff}$ we will see when $D = \eta(A, B, C) \in \mathbb{J}_{\mathcal{H}}$ is not defined. This is when $s_1(A, B) = 0$. We will identify all the special divisors and we will show how to work with them.

In terms of the geometry of $\mathcal{H}$, $s_1(A, B) = 0$ means $f(x_1) - f(x_2) = 0$ or $f'(x_1) = 0$ depending on the number of affine points in $Supp(\mathfrak{D})$, the possible cases are given by:

(I) $\mathfrak{D} = [(x_1, y_1) + (x_2, y_1) - 2\infty]$ with $x_1 \neq x_2$
(Ia) $\mathfrak{D} = [2(x_3, y_3) - 2\infty]$ where $Supp(\mathfrak{D}) \subset Supp(div(y - y_3))$
(II) $\mathfrak{D} = [(x_1, y_1) + (x_4, -y_1) - 2\infty]$ with $x_1 \neq x_4$

Case I means that $Supp(\mathfrak{D})$ has two points $P_1, P_2 \in \mathcal{H}$ that lie in a line of constant slope, this happens if $\mathfrak{D} = (A, B, 0, D)$.

Case Ia that $Supp(\mathfrak{D})$ has a double point $P_3 \in \mathcal{H}$ that lies in a line of constant slope, where $\mathfrak{D} = (A, B, 0, D)$.

Case II that $Supp(\mathfrak{D})$ has two points $P_1, P_4 \in \mathcal{H}$ with different $x$ coordinate and $y$ coordinate differing by sign, in this case $\mathfrak{D} = (A, B, C, D)$ with $C \neq 0$.

Let us consider Case I. The points $P_1 = (x_1, y_1), P_2 = (x_2, y_1) \in \mathcal{H}$ with $x_1 \neq x_2$ and $y_1 \neq 0$ define a divisor $\mathfrak{D} := [P_1 + P_2 - 2\infty] \in \mathbb{J}_{\mathcal{H}}$. Mumford representation of $\mathfrak{D}$ is given by $\langle (x - x_1)(x - x_2), y_1 \rangle$. Thus, we get the point $(-x_1 - x_2, x_1 x_2, 0, y_1) \in \mathbb{J}_{\mathcal{H}}^{Aff}$.

Similarly, if $\iota \in Aut_{\mathbb{K}}(\mathcal{H})$ is the hyperelliptic involution, then there is also a point $\bar{\mathfrak{D}} := [\iota P_1 + \iota P_2 - 2\infty] \in \mathbb{J}_{\mathcal{H}}$ which yields $(-x_1 - x_2, x_1 x_2, 0, -y_1) \in \mathbb{J}_{\mathcal{H}}^{Aff}$. With this we have that $\mathfrak{D}$ and $\bar{\mathfrak{D}}$ are special divisors on the jacobian, because $\mathfrak{D}$ and $\bar{\mathfrak{D}}$ map to the same point under $\pi$.

Case Ia is similar to Case I because we get the point $(-2x_3, x_3^2, 0, y_3) \in \mathbb{J}_{\mathcal{H}}^{Aff}$. This yields $\pi^{-1}(-2x_3, x_3^2, 0) \supseteq \{\mathfrak{D}, \bar{\mathfrak{D}}\}$ and so $\mathfrak{D}$ and $\bar{\mathfrak{D}}$ are also special.

The last Case II is different, on the one hand $s_1(-x_1-x_2, x_1x_4) = 0$ but on the other hand the divisor $\mathfrak{D}$ is not special. We have that $\mathfrak{D}$ defines the point $(A,B,C,D) = (-x_1-x_4, x_1x_4, \frac{2y_1}{x_1-x_4}, \frac{-y_1(x_1+x_4)}{x_1-x_4}) \in \mathbb{J}_{\mathcal{H}}^{Aff}$. Thus, the only divisor $\mathfrak{F}$ different from $\mathfrak{D}$ that could be in $\pi^{-1}(A,B,C)$ must have points in its support with the same $x$ coordinates as the points in the support of $\mathfrak{D}$. This condition leads us to $\mathfrak{F} = \bar{\mathfrak{D}}$ but $\bar{\mathfrak{D}} \notin \pi^{-1}(A,B,C)$ as $C \neq 0$ and $\pi(\bar{\mathfrak{D}}) = (A,B,-C)$. With this $\#\pi^{-1}(A,B,C) = 1$ hence $\mathfrak{D}$ is not special. We call the divisors in this Case II **anomalous**.

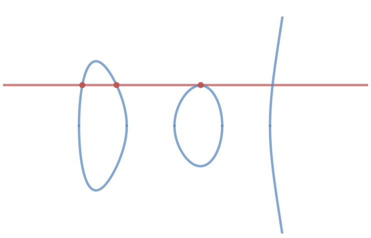

**Fig. 1.** Case I & Ia, $P_1, P_2, P_3$

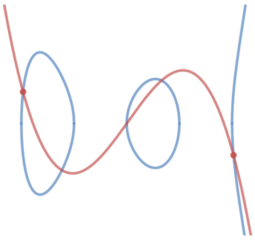

**Fig. 2.** Case II, $P_1, P_4$

**Proposition 4** *Let $\mathcal{H}$ be a hyperelliptic curve of genus 2 over a field $\mathbb{K}$ and let $(A,B,C,D) =: \mathfrak{D} \in \mathbb{J}_{\mathcal{H}}^{Aff}$ be non anomalous then $\mathfrak{D}$ is special iff $s_1(A,B) = 0$.*

*Proof.* As $\mathfrak{D}$ is assumed to be non-anomalous we have already seen that the condition $s_1(A,B) = 0$ implies that $\mathfrak{D}$ is special for the cases I and Ia.

Suppose that $\mathfrak{D}$ is special and $s_1(A,B) \neq 0$, then there exists $\mathfrak{D} \neq \mathfrak{F} \in \mathbb{J}_{\mathcal{H}}^{Aff}$ such that $\pi^{-1}(A,B,C) \supset \{\mathfrak{D}, \mathfrak{F}\}$. This gives us $\pi(\mathfrak{D}) = \pi(\mathfrak{F}) = (A,B,C)$ and the Mumford representations of these points are given by $\mathfrak{D} = \langle x^2+Ax+B, Cx+D\rangle$ and $\mathfrak{F} = \langle x^2+Ax+B, Cx+D'\rangle$ with $D \neq D'$. This can only happen in two situations:

The first situation is when $C = 0$, but as discussed in Case I and Ia we will have that $\mathfrak{F} = \bar{\mathfrak{D}}$ this implies that $s_1(A,B) = 0$ which is a contradiction.

The second situation is when $C \neq 0$. Here the points up to multiplicity in the support of $\mathfrak{D}$ lie in a line $\ell_1(x) = Cx + D$ and the points of the support of $\mathfrak{F}$ in $\ell_2(x) = Cx + D'$. Both have the same slope which can only occur if $D = D'$ hence $\mathfrak{D} = \mathfrak{F}$ which is a contradiction since $\mathfrak{D}$ is special. □

With this, we have characterized those divisors that can be unique described with three coordinates. If $\mathcal{S} \subset \mathbb{J}_{\mathcal{H}}$ are the special divisors then $\pi : \mathbb{J}_{\mathcal{H}}^{Aff} \setminus \mathcal{S} \to \check{\mathbb{J}}_{\mathcal{H}}$ is a bijection.

In the next section we will see how to represent special divisors in order to identify them with 2 bits of extra information, anomalous divisors will be kept in normal Mumford representation.

## 5 Representation of elements in $\breve{\mathbb{J}}_{\mathcal{H}}$

In order to work with special divisors in $\breve{\mathbb{J}}_{\mathcal{H}}$ and solve the lack of injectivity of $\pi$ for a computational approach, is enough to include 2 bits in the representation of the elements in $\breve{\mathbb{J}}_{\mathcal{H}}$ to indicate in $\mathfrak{D} = \langle u(x), v(x)\rangle$ which type of special reduced divisor is being represented as described before and work with it as an element of $\mathbb{J}_{\mathcal{H}}^{Aff}$ or as an element of $\breve{\mathbb{J}}_{\mathcal{H}}$.

Let $\mathfrak{D} = (A, B, C, D) \in \mathbb{J}_{\mathcal{H}}^{Aff}$ such that the Mumford representation is given by $\langle u(x), v(x)\rangle$. If $s_1(A, B) \neq 0$, then we represent $\mathfrak{D}$ in $\breve{\mathbb{J}}_{\mathcal{H}}$ as $(A, B, C)$, with bits 00 indicating that this is not a special nor anomalous reduced divisor, which is the general case.

If $s_1(A, B) = 0$ and $C = 0$ (Case I and Ia), then we represent $\mathfrak{D}$ in $\breve{\mathbb{J}}_{\mathcal{H}}$ as $\mathfrak{D} = (A, B, v(0))$ with the extra two bits 01, which will indicate that $C = 0$, so we will include the constant part of $v$ instead of the slope.

If $s_1(A, B) = 0$ and $C \neq 0$ (Case II), then the divisor is anomalous and we use the normal Mumford representation as we will need both coefficients of $v(x)$ to obtain $\mathfrak{D} \in \mathbb{J}_{\mathcal{H}}^{Aff}$.

This representation of elements in the jacobian saves one coordinate in must cases (generic case, case I and Ia) which can be practical and is possible to do arithmetic with them as we will see in the next section, limited to non special nor anomalous divisors.

As a remark, it is possible to minimize the number of points in cases I, Ia and II in the jacobian. One way is to find curves with a few rational points that generate a lot of rational points in the jacobian.

## 6 Addition on $\breve{\mathbb{J}}_{\mathcal{H}}$

We are going to see how addition on $\breve{\mathbb{J}}_{\mathcal{H}}$ is done using this reduced Mumford representation, modifying a little bit the addition in [CL11]. We have calculated explicitly that if $\mathcal{D}, \mathcal{E} \in \breve{\mathbb{J}}_{\mathcal{H}}$ such that $\mathcal{D} = (a, b, c)$ and $\mathcal{E} = (A, B, C)$ then the addition $\mathcal{D} \oplus \mathcal{E} = \mathcal{F} = (\alpha, \beta, \gamma)$ is given by first considering the following expressions.

$$\begin{aligned}
\varLambda :=& \eta(a, b, c) + \eta(A, B, C)\\
\varPsi :=& (C^2 - a_2 + A(A^2 - 2B + a_3) - b(a + A))\\
& \cdot (a(c + C) - \varLambda) + (A^2 - B + a_3 + a(a + A) - b)b(c + C)\\
\varTheta :=& (a(c + C) - \varLambda)\varLambda - b(c + C)^2\\
\varXi :=& (C^2 - a_2 - A(-A^2 + 2B - a_3) - b(a + A))(c + C)\\
& - \varLambda(-A^2 + B - a_3 - a(a + A) + b)
\end{aligned}$$

These expressions where obtained solving the system of valuations induced by the divisors $\mathcal{D}$ and $\mathcal{E}$ and then expressing the explicit result of the system.

After we arrange and adapt with our new reduction of the Mumford coordinates we get the following addition formulæ.

$$\alpha = A - a + \frac{2\varPsi}{\varXi} - \frac{\varTheta^2}{\varXi^2}$$
$$\beta = (A-a)\frac{\varPsi}{\varXi} + \frac{\varPsi^2}{\varXi^2} + (a+A)\frac{\varTheta^2}{\varXi^2} - (c+C)\frac{\varTheta}{\varXi}$$
$$\gamma = (a-\alpha)\frac{\varPsi}{\varTheta} - \alpha(a-\alpha)\frac{\varXi}{\varTheta} + (A-a)(a-\alpha)\frac{\varXi}{\varTheta} + (b-\beta)\frac{\varXi}{\varTheta} - c.$$

In this formulæ, we see that in order to be well defined, $\varXi$ and $\varTheta$ must be non-zero. This happens when the resulting divisor class $\mathcal{F}$ in the jacobian is not of the form $[(x,y)-\infty]$.

This is an example of the arithmetic in the jacobian using these reduced divisors and is unified as in [OD12] and improved by [CL11] which means that it works for doubling, adding and adding with non-disjoint support in the divisors, but the reduction can be adapted to other ways to do arithmetic on $\mathbb{J}_{\mathcal{H}}$.

If $s_1(\alpha,\beta)=0$ and $\gamma=0$ then the representation of $\mathcal{F}$ is done as in section 5 for the cases I,Ia. If $s_1(\alpha,\beta)=0$ and $\gamma\neq 0$ we are in the anomalous Case II, so the fourth coordinate in $\mathbb{J}_{\mathcal{H}}^{Aff}$ need to be included in the representation, which is given by $\delta = (c-\gamma)\frac{\varPsi}{\varTheta} - \gamma(a-\alpha)\frac{\varXi}{\varTheta} + (A-a)(b-\beta)\frac{\varXi}{\varTheta} - \eta(a,b,c)$.

## 7 Conclusion

We have characterized divisor classes in $\mathbb{J}_{\mathcal{H}}$ which can be represented in a more compact form compared with the Mumford representation finding a rational function $\eta \in \mathbb{K}(\mathbb{J}_{\mathcal{H}})$ such that $(A,B,C,\eta(A,B,C)) \in \mathbb{J}_{\mathcal{H}}^{Aff}$. This can be useful for cryptographic purposes as the public keys in discrete logarithm based systems in this context are divisor classes which can be stored in a more efficient way.

I would like to thank Jesus Barradas Berglind for his suggestions on earlier versions of this paper.

## References

[Can87] David G Cantor. Computing in the jacobian of a hyperelliptic curve. *Mathematics of computation*, 48(177):95–101, 1987.

[CF96] J.W.S. Cassels and E.V. Flynn. *Prolegomena to a middlebrow arithmetic of curves of genus 2*, volume 230. Cambridge University Press, 1996.

[Gra90] David Grant. Formal groups in genus two. *J. reine angew. Math*, 411(96):121, 1990.

[Fly90] E.V. Flynn. The jacobian and formal group of a curve of genus 2 over an arbitrary ground field. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 107, pages 425–441. Cambridge Univ Press, 1990.

[CL11] Craig Costello and Kristin Lauter. Group law computations on jacobians of hyperelliptic curves. In *Selected Areas in Cryptography*, pages 92–117. Springer, 2011.

[Mum84] David Mumford. *Tata Lectures on Theta II.* Birkhäuser, 1984.

[OD12] M. Joye O. Diao. Unified addition formulæ for hyperelliptic curve cryptosystems. 2012.

[HC14] Huseyin Hisil and Craig Costello. Jacobian coordinates on genus 2 curves. In *Advances in Cryptology–ASIACRYPT 2014*, pages 338-357. Springer, 2014.

[Lan05] Tanja Lange. Formulae for arithmetic on genus 2 hyperelliptic curves. *Applicable Algebra in Engineering, Communication and Computing*, 15(5):295–328, 2005.

[GHM08] Steven D Galbraith, Michael Harrison, and David J Mireles Morales. Efficient hyperelliptic arithmetic using balanced representation for divisors. In *Algorithmic number theory*, pages 342–356. Springer, 2008.

## Appendix: Code

The next MAGMA program implements the symmetric functions $s_1, s_2, s_3, s_4$, the arithmetic on $\mathbb{J}_{\mathcal{H}}$ and checks for a random Jacobian all the special and anomalous divisors and verifies that $\eta$ is well defined.

```
q := 101;
F := GF(q);
P<x> := PolynomialRing(F);
a0 := Random(F);
a1 := Random(F);
a2 := Random(F);
a3 := Random(F);
a4 := 0;

s1 := function(A,B)
return a1-a2*A+a3*(A^2-B)+a4*(2*B*A-A^3)+A^4-B*(3*A^2-B);
end function;
s2 := function(A,B)
return 2*a0-a1*A+a2*(A^2-2*B)+a3*(3*B*A-A^3)+a4*(A^4-4*B*A^2+2*B^2)-
A^5-5*A*B^2+5*B*A^3;
end function;
s3 := function(A,B,C)
return (s2(A,B)-(C^2)*(A^2-4*B))/2 ;
end function;
s4 := function(A,B)
return a0-a1*A+a2*(A^2-B)+a3*(2*A*B-A^3)+a4*(A^4-B*(3*A^2-B))-
A*(A^2-3*B)*(A^2-B) ;
end function;
eta := function(A,B,C)
return (C*(s2(A,B)+s3(A,B,C)-s4(A,B)))/s1(A,B) ;
end function;
E := function(A,B,C,a,b,c) return eta(A,B,C)+eta(a,b,c); end function;
p := function(A,B,C,a,b,c)
return (C^2-a2+A*(A^2-2*B+a3)-b*(a+A))*(a*(c+C)-E(A,B,C,a,b,c))+
(A^2-B+a3+a*(a+A)-b)*b*(c+C);
end function;
q := function(A,B,C,a,b,c)
return (a*(c+C)-E(A,B,C,a,b,c))*E(A,B,C,a,b,c)-b*(c+C)^2;
end function;
r := function(A,B,C,a,b,c)
return (C^2-a2-A*(-A^2+2*B-a3)-b*(a+A))*(c+C)-
E(A,B,C,a,b,c)*(-A^2+B-a3-a*(a+A)+b);
end function;
Jx := function(A,B,C,a,b,c)
return A-a+(2*p(A,B,C,a,b,c)/r(A,B,C,a,b,c))-
```

```
(q(A,B,C,a,b,c)/r(A,B,C,a,b,c))^2 ;
end function;
Jy := function(A,B,C,a,b,c)
return (A-a)*(p(A,B,C,a,b,c)/r(A,B,C,a,b,c))+
(p(A,B,C,a,b,c)/r(A,B,C,a,b,c))^2+(a+A)*(q(A,B,C,a,b,c)/r(A,B,C,a,b,c))^2-
(c+C)*q(A,B,C,a,b,c)/r(A,B,C,a,b,c);
end function;
Jz := function(A,B,C,a,b,c)
return (a-Jx(A,B,C,a,b,c))*(p(A,B,C,a,b,c)/q(A,B,C,a,b,c))-
(Jx(A,B,C,a,b,c)*(a-Jx(A,B,C,a,b,c))*r(A,B,C,a,b,c)/q(A,B,C,a,b,c))+
((A-a)*(a-Jx(A,B,C,a,b,c))*r(A,B,C,a,b,c)/q(A,B,C,a,b,c))+
(b-Jy(A,B,C,a,b,c))*(r(A,B,C,a,b,c)/q(A,B,C,a,b,c))-c;
end function;
Jadd := function(A,B,C,a,b,c)
return F!Jx(A,B,C,a,b,c),F!Jy(A,B,C,a,b,c),F!Jz(A,B,C,a,b,c); end function;
f := x^5 + a4*x^4 + a3*x^3 + a2*x^2 + a1*x +a0;
special:=0;
if Discriminant(f) ne 0
then
C := HyperellipticCurve(f);
J := Jacobian(C);
RJ := RationalPoints(J);
for i:= 1 to #J do
if Degree(RJ[i][1]) eq 2
then
a := Coefficient(RJ[i][1],1);
b := Coefficient(RJ[i][1],0);
c := Coefficient(RJ[i][2],1);
d := Coefficient(RJ[i][2],0);
if s1(a,b) ne 0
then
nd := eta(a,b,c);
if d ne nd
then
printf "This should not happen, %o,%o,%o,%o\n",a,b,c,d;
end if;
else
special := special+1;
end if;
end if;
end for;
else
printf "Chosen curve is singular, run this again\n";
end if;
printf "Found %o/%o divisors on the Jacobian\n",special,#J;
```