Inverse Jacobian and related topics for certain superelliptic curves

Somoza Henares, A.

The family of cyclic plane quintic curves

2

A *cyclic plane quintic curve* (from now on *CPQ curve*) over $\mathbb{C}$ is a genus-6 smooth, plane, projective curve given by the equation $Y^5 = f(X, Z)$ where f is a homogeneous polynomial of degree 5 with distinct roots. Such a curve has an automorphism ρ of order 5 given by $(X : Y : Z) \mapsto (X : z_5 Y : Z)$, with $z_5 = \exp(2\pi i/5)$. It fixes the points $(\alpha : 0 : \beta)$ with $f(\alpha, \beta) = 0$, the *branch points* of C.

The isomorphisms between CPQ curves are of the form

$$(X : Y : Z) \mapsto (aX + bZ : Y : cX + dZ).$$

Therefore, every ordering of the branch points gives rise to an isomorphic model with the three first branch points at $(0 : 0 : 1)$, $(1 : 0 : 1)$ and $(1 : 0 : 0)$. In that case, if we consider the patch $Z \neq 0$ and define the affine coordinates $x = X/Z$ and $y = Y/Z$, then a CPQ curve is determined by the x-coordinates of the remaining branch points $(\lambda, 0)$ and $(\mu, 0)$ as

$$y^5 = x(x-1)(x-\lambda)(x-\mu).$$

We refer to this form as a *Legendre-Rosenhain equation of a CPQ curve*.

In this chapter we present a method that, given the period matrix of the Jacobian of a CPQ curve, computes a numerical approximation of the equation of the curve. We follow the general idea of the algorithm for Picard curves presented in Chapter 1, and we highlight the similarities and differences between both cases.

The structure of the chapter runs parallel to that of Chapter 1. In Section 2.1, we give a formula to approximate the x-coordinates of the branch points of a CPQ curve in terms of quotients of Riemann theta constants on its Jacobian, see Theorem 2.1.7.

In Section 2.2, we show how to identify the points in the Jacobian needed to apply said formula, such as the Riemann constant and the images by the Abel-Jacobi map of the branch points, see Theorem 2.2.4. We also give an inverse Jacobian algorithm for CPQ curves, that is, an algorithm that given the Jacobian of a CPQ curve C returns the x-coordinates of the branch points of C, see Algorithm 2.2.6.

Finally, in Section 2.3 we discuss how to obtain exact models from the approximations given by the algorithm, and we show some interesting examples of curves obtained using it.

2.1 A Thomae-like formula

The goal of this section is to prove a result for CPQ curves analogous to Theorem 1.2.13, that is, a formula that gives the x-coordinates of the branch points as quotients of Riemann theta constants on the Jacobian using Siegel's Theorem 1.2.6. To do so, we start by identifying a family of non-special divisors.

Definition 2.1.1. Let C be a curve, and let ω be a regular differential of C. Given a point P, a local parameter u at P and a non-negative integer n, we define the n-th derivative of ω at P with respect to u to be the complex number

$$\partial_u^n \omega(P) = n!\, a_n,$$

for $\omega = \sum_{k\geq 0} a_k u^k\, du \in \mathcal{O}_P(C)du \cong \mathbb{C}[[u]]du$ the series of ω at the local ring $\mathcal{O}_P(C)$.

Example 2.1.2. Let C be a CPQ curve with equation

$$y^5 = x^4 - 6x^3 + 11x^2 - 6x.$$

At the point $P = (0, 0)$ the function y is a local parameter, and we can write x as

$$x = \frac{1}{6}(-y^5 + x^4 - 6x^3 + 11x^2)$$

If we substitute this equation into itself recursively, then we obtain x as a power series in y,

$$x = -\frac{1}{6}y^5 + \frac{11}{216}y^{10} - \frac{103}{3888}y^{15} + \dots .$$

Consider now the regular differential $\omega = dx/y^2$. We have

$$\omega = \frac{dx}{y^2} = (-\frac{5}{6}y^2 + \frac{55}{108}y^7 - \frac{515}{1296}y^{12} + \dots)dy.$$

Therefore, the zero derivative of ω at P with respect to y is

$$\partial_y^0 \omega(P) = 0,$$

and the second derivative of ω at P with respect to y is

$$\partial_y^2 \omega(P) = -\frac{5}{3}.$$

The following proposition characterizes non-special divisors.

Proposition 2.1.3 (Siegel [44, pg. 154])**.** Let C be a curve and let $\omega_1, \ldots, \omega_g$ be a basis of regular differentials of C.

Given a point P and a positive integer n_P, consider the $g \times n_P$ matrix $W(P, n_P)$ given by the first n_P derivatives of the differentials relative to a local parameter u at the point, that is

$$W(P, n_P) = \left(\partial_u^j \omega_i(P)\right)_{\substack{1 \le i \le g \\ 0 \le j \le n_P - 1}} \in \mathbb{C}^{g \times n_P}.$$

Given $D = \sum n_P P$ an effective degree-g divisor, we define the $g \times g$ matrix $W(D)$ as the concatenation of the matrices $W(P, n_P)$ for the points P in D.

The divisor D is non-special if and only if the matrix $W(D)$ is invertible. □

In order to apply this result to the case of CPQ curves we need to choose a basis of regular differentials.

Proposition 2.1.4. Let l be a prime and let C be a curve given by an equation

$$Y^l = F(X, Z) = \prod_{i=1}^{l} (\alpha_i X - \beta_i Z)$$

such that all the branch points $P_i = (\beta_i : 0 : \alpha_i)$ for $i = 1, \ldots, l$ are distinct. Let g be the genus of C, which satisfies $g = \frac{1}{2}(l-1)(l-2)$. Consider the affine coordinates $x = X/Z$ and $y = Y/Z$. The differentials

$$\left(\frac{x^i y^j dx}{y^{l-1}} : i, j \ge 0,\ i + j \le l - 3 \right)$$

form a basis of the space of holomorphic differentials $H^0(\omega_C)$ of C.

Proof. Following [8, Section 2.9], we define the Newton polygon $\mathcal{N}(C)$ of a plane curve C given by the equation $G(x, y) = 0$ as the convex hull of all points $(i, j) \in \mathbb{Z}^2$ for which the coefficient of $x^i y^j$ in G is non-zero.

For each interior integer point $(i, j) \in \mathcal{N}(C)$, one may construct a differential

$$\omega = \frac{x^{i-1} y^{j-1} dx}{\partial_y G(x, y)}.$$

We obtain g differentials, and they are all holomorphic and linearly independent (see [8, paragraph after Equation (2.52)]).

In the case at hand we have $G(x,y) = y^l - F(x,1)$, hence the Newton polygon $\mathcal{N}(C)$ is contained in the triangle T of vertices $(0,l)$, $(l,0)$ and $(0,0)$ and contains all the interior points of T. The result follows. □

Corollary 2.1.5. Given a CPQ curve C, the differentials

$$\left(\frac{dx}{y^4}, \frac{xdx}{y^4}, \frac{x^2dx}{y^4}, \frac{dx}{y^3}, \frac{xdx}{y^3}, \frac{dx}{y^2}\right)$$

form a basis of the space of holomorphic differentials $H^0(\omega_C)$. □

This result allows us to prove that our chosen divisors are non-special.

Proposition 2.1.6. Let C be a CPQ curve and let $\mathcal{B}$ be the set of branch points of the curve C. Let $P, Q, R \in \mathcal{B}$ be distinct. Then the divisor $P + 2Q + 3R$ is non-special.

Proof. Consider the basis of differentials in Corollary 2.1.5 and compute the matrix $W(P+2Q+3R)$ as defined in Proposition 2.1.3. One checks that it has maximal rank, hence by Proposition 2.1.3 the divisor is non-special. □

We can now state a formula that gives the x-coordinates of the branch points of a CPQ curve in terms of quotients of Riemann theta constants.

Theorem 2.1.7. Let C be a CPQ curve over $\mathbb{C}$ given by a Legendre-Rosenhain equation

$$Y^5 = X(X-Z)(X-\lambda Z)(X-\mu Z)Z,$$

and consider the points $P_t = (t:0:1)$ for $t \in \{0, 1, \lambda, \mu\}$ and $P_\infty = (1:0:0)$. Let $J(C)$ be the Jacobian of C with period matrix $\Omega \in \mathbf{H}_6$, let α be the Abel-Jacobi map with base point P_∞, let Δ be the Riemann constant with respect to α, and let $\{\eta, \nu\} = \{\lambda, \mu\}$. We have

$$\eta = \varepsilon_\eta \left(\frac{\theta[\widetilde{P_1} + 2\widetilde{P_\eta} + 3\widetilde{P_\nu} - \widetilde{P_0} - \widetilde{\Delta}](\Omega)}{\theta[\widetilde{P_1} + 2\widetilde{P_\eta} + 3\widetilde{P_\nu} - \widetilde{\Delta}](\Omega)} \frac{\theta[2\widetilde{P_1} + \widetilde{P_\eta} + 3\widetilde{P_\nu} - \widetilde{\Delta}](\Omega)}{\theta[2\widetilde{P_1} + \widetilde{P_\eta} + 3\widetilde{P_\nu} - \widetilde{P_0} - \widetilde{\Delta}](\Omega)} \right)^5,$$

where $\varepsilon_\eta = \exp(10\pi i((\widetilde{P_\eta} - \widetilde{P_1})_1(\widetilde{P_0})_2))$.

Proof. Let ω be the basis of holomorphic differentials for which $J(C)$ has period matrix Ω. The divisor of the function x is $\operatorname{div}(x) = 5P_0 - 5P_\infty$. Then, in order to apply Corollary 1.2.10 for $\phi = x$ and $P = P_\infty$, we choose five times the zero path from P_∞ to itself; the path γ_1 from P_∞ to P_0 that for $a_1 = \widetilde{P_0}$ satisfies

$$\int_{\gamma_1} \omega = \Omega(a_1)_1 + (a_1)_2 \in \mathbb{C}^6;$$

and, for $k = 2, \ldots, 5$, some paths γ_k from P_∞ to P_0 that satisfy

$$\sum_{k=1}^{5} \int_{\gamma_k} \omega = 0 \text{ in } \mathbb{C}^6.$$

For $k = 2, \ldots, 5$ we denote by a_k be the element in $\mathbb{R}^{12}$ that satisfies

$$\int_{\gamma_k} \omega = \Omega(a_k)_1 + (a_k)_2.$$

By Corollary 1.2.10, given an effective divisor D of degree 6 we have

$$\phi(D) = E' \prod_{k=1}^{5} \frac{\theta[\widetilde{D} - a_k - \widetilde{\Delta}](\Omega)}{\theta[\widetilde{D} - \widetilde{\Delta}](\Omega)} \tag{2.1}$$

for some constant E' independent of D.

Consider now the divisors $D_\eta = P_1 + 2P_\eta + 3P_\nu$ and $D_1 = 2P_1 + P_\eta + 3P_\nu$, which are general because of Proposition 2.1.6, and divide the corresponding equalities given by (2.1). We obtain

$$\begin{aligned} \eta &= \frac{\phi(P_\eta)}{\phi(P_1)} = \frac{\phi(D_\eta)}{\phi(D_1)} \\ &= \prod_{k=0}^{5} \left(\frac{\theta[\widetilde{P_1} + 2\widetilde{P_\eta} + 3\widetilde{P_\nu} - a_k - \widetilde{\Delta}](\Omega)}{\theta[\widetilde{P_1} + 2\widetilde{P_\eta} + 3\widetilde{P_\nu} - \widetilde{\Delta}](\Omega)} \frac{\theta[2\widetilde{P_1} + \widetilde{P_\eta} + 3\widetilde{P_\nu} - \widetilde{\Delta}](\Omega)}{\theta[2\widetilde{P_1} + \widetilde{P_\eta} + 3\widetilde{P_\nu} - a_k - \widetilde{\Delta}](\Omega)} \right). \end{aligned} \tag{2.2}$$

The result then follows from applying the quasi-periodicity property of the Riemann theta constants to the equation (2.2), as we did in the proof of Theorem 1.2.13. □

2.2 The inverse Jacobian algorithm

The end goal of this section is to provide an algorithm that, given a period matrix of the Jacobian of a CPQ curve and the rational representation of its induced automorphism ρ_*, returns a numerical approximation of the x-coordinates of the branch points of C.

The main step in the algorithm is based on Theorem 2.1.7. To apply that theorem we need to identify the Riemann constant of C with respect to an Abel-Jacobi map α with a branch point as base point and the image by α of the branch points on $J(C)$.

We start by characterizing the Riemann constant of a CPQ curve.

Corollary 2.2.1. Let C be a CPQ curve, let ρ be the automorphism given by $(x, y) \mapsto (x, z_5 y)$. Let α be an Abel-Jacobi map with a branch point as base point. The Riemann constant with respect to α is the only point $\Delta \in J(C)$ with

(1) $\Delta \in J(C)[2]$, and
(2) ${}^t\rho_r(\rho_*)[\Delta] = \Delta$.

Proof. Let $P_0 \in \mathcal{B}$ be the base point of the Abel-Jacobi map α. By Proposition 1.2.4 the Riemann constant satisfies $2\Delta = \alpha(\kappa)$ for κ a canonical divisor. Since we have

$$\operatorname{div}\left(\frac{(x - x(P_0))^2 dx}{y^4}\right) = 10P_0,$$

we conclude that Δ is a 2-torsion point, that is, the point Δ satisfies (1). Moreover, by Proposition 1.3.4 we have $\Delta = \rho_r(\rho_*)[\Delta']$ for Δ' the Riemann constant with respect to $\rho(P_0)$. But since P_0 is fixed by ρ, the point Δ satisfies (2).

To prove that it is the only point that satisfies (1) and (2), assume that there exist $\Delta^1, \Delta^2 \in J(C)$ that satisfy (1) and (2). By (2) we have

$$\underline{\Delta}^1 - \underline{\Delta}^2 = {}^t\rho_r(\rho_*)[\underline{\Delta}^1] - {}^t\rho_r(\rho_*)[\underline{\Delta}^2] = \rho_r(\rho_*)^{-1}(\underline{\Delta}^1 - \underline{\Delta}^2),$$

thus $\Delta^1 - \Delta^2$ is an element of $J(C)[1 - \rho_*^4] \subseteq J(C)[5]$. But by (1), the difference $\Delta^1 - \Delta^2$ is also a 2-torsion point, hence we conclude $\Delta^1 - \Delta^2 = 0$. □

Next we are interested in identifying the images of the branch points in the Jacobian. We aim to state a theorem analogous to Theorem 1.3.6 for CPQ curves, hence we start by studying the $(1 - \rho_*)$-torsion of the Jacobian.

Proposition 2.2.2. Let l be a prime, let C be a curve given by an equation

$$Y^l = F(X, Z) = \prod_{i=1}^{l} (\alpha_i X - \beta_i Z)$$

such that all the branch points $P_i = (\beta_i : 0 : \alpha_i)$ for $i = 1, \ldots, l$ are distinct, and let $\mathcal{B}$ be the set of branch points. Let ρ be the automorphism of C given by $\rho(X : Y : Z) = (X : z_l Y : Z)$ with $z_l = \exp(2\pi i/l)$. We have

$$J(C)[1 - \rho_*] = \langle [P_i - P_l] : 1 \leq i < l \rangle,$$

where all the points $[P_i - P_l]$ are distinct and satisfy $\sum_{i=1}^{l-1} [P_i - P_l] = 0$.

One of the steps in the proof is to compute $\#J(C)[1 - \rho_*] = \deg(1 - \rho_*)$. To do so, we use the following lemma.

Lemma 2.2.3 (Birkenhake-Lange [2, Section 5.1])**.** Let $X = V/\Lambda$ be an abelian variety over $\mathbb{C}$, and let $f \in \mathrm{End}(X)$ be an endomorphism with characteristic polynomial $P_f^r(t) := \det(t\,\mathrm{id}_\Lambda - \rho_r(f))$. Then for all $n \in \mathbb{Z}$ we have

$$\deg(n - f) = P_f^r(n). \qquad \square$$

Proof of Proposition 2.2.2. Let $\mathcal{B} = \{P_i : 1 \le i \le l\}$ be the set of branch points of C, define the group $\mathcal{D} := \{D \in \mathrm{Div}^0(C) : \mathrm{Supp}(D) \subseteq \mathcal{B}\} \cong \mathbb{Z}^{l-1}$, and consider the map

$$\begin{aligned} \Psi : \mathcal{D} &\to \mathrm{Pic}^0(C)[1 - \rho_*] = J(C)[1 - \rho_*], \\ D &\mapsto [D]. \end{aligned}$$

We start by computing the kernel of Ψ. Let $D \in \mathcal{D}$ be a principal divisor, say $D = \mathrm{div}(h)$. Then h satisfies

$$\mathrm{div}(h \circ \rho) = \rho^* D = D = \mathrm{div}(h),$$

so we get $h \circ \rho = c \cdot h$ for some $c \in \mathbb{C}^\times$. Actually, we obtain $c = z_l^m$ for some $m \in \mathbb{Z}/l\mathbb{Z}$.

Consider now $x = X/Z$ and $y = Y/Z$, define the function

$$g = \frac{Y}{\alpha_l X - \beta_l Z} = \frac{y}{\alpha_l x - \beta_l},$$

and note that it satisfies $g^m \circ \rho = z_l^m g^m$ and $\mathrm{div}(g) = \sum_{P \in \mathcal{B}} P - lP_l \in \mathcal{D}$.

It follows that the function $h/g^m \in \mathbb{C}(x)[y]/(y^l - F(x,1))$ satisfies

$$\frac{h}{g^m} \circ \rho = \frac{h}{g^m},$$

so that we actually have $h/g^m \in \mathbb{C}(x)$ and we can write $h = g^m f$ for some function $f \in \mathbb{C}(x)$ whose divisor is also in $\mathcal{D}$.

Since the function f only depends on x, the morphism $f : C \to \mathbb{P}^1$ factors through $C/\langle\rho\rangle$. Thus the divisor of f is the pullback by $\pi : C \to C/\langle\rho\rangle$ of a function f' on $\mathbb{P}^1$ of degree l and which is ramified at the branch points of C.

We conclude

$$D = \mathrm{div}(h) = m\,\mathrm{div}(g) + \pi^*\,\mathrm{div}(f') = m\,\mathrm{div}(g) + l \cdot D' \text{ for some } D' \in \mathcal{D},$$

and therefore we obtain

$$\ker \Psi \subseteq l\mathcal{D} + \mathbb{Z}\,\mathrm{div}(g). \tag{2.3}$$

Clearly we have $\operatorname{div}(g) \in \ker \Psi$. Moreover, for $k = 1, \ldots, l$, the function

$$\phi_k = \frac{\alpha_k X - \beta_k Z}{\alpha_l X - \beta_l Z}$$

has divisor $\operatorname{div} \phi_k = lP_k - lP_l$, so we obtain $l\mathcal{D} \subseteq \ker \Psi$; and the equality in (2.3) holds.

Altogether we obtain $\operatorname{Im} \Psi \cong \mathcal{D}/\ker \Psi \cong (\mathbb{Z}/l\mathbb{Z})^{l-1}/\langle (1, \ldots, 1) \rangle$, so $\operatorname{Im} \Psi$ has l^{l-2} elements.

Since the minimal polynomial of the automorphism ρ_* is the cyclotomic polynomial $\prod_{k=1}^{l-1}(x - z_l^k) \in \mathbb{Q}[x]$, which is irreducible, and its characteristic polynomial has degree $2g = (l-1)(l-2)$, we get

$$P_f^r(t) = \prod_{k=1}^{l-1}(x - z_l^k)^{l-2} \in \mathbb{Q}[x].$$

Then by Lemma 2.2.3 we obtain

$$\deg(1 - \rho_*) = \prod_{k=1}^{l-1}(1 - z_l^k)^{l-2} = l^{l-2}.$$

It follows that $J(C)[1-\rho_*]$ has l^{l-2} elements, so we conclude that Ψ is surjective and the result follows. □

We can now prove the theorem that allows us to identify the image of the branch points in the Jacobian.

Theorem 2.2.4. Let $J(C)$ be the Jacobian of a CPQ curve C with period matrix $\Omega \in \mathbf{H}_6$, let ρ_* be the automorphism on $J(C)$ induced by the curve automorphism $\rho(x, y) = (x, z_5 y)$ and let $\mathcal{B}$ be the set of branch points of C. Let Δ be the only point in $J(C)[2]$ that satisfies $\rho_r(\rho_*)[\Delta] = \Delta$ and define

$$\Theta_5 := \{x \in J(C)[1 - \rho_*] : \theta[\underline{x} + \underline{\Delta}](\Omega) = 0\}.$$

Then there exists a subset $\mathcal{T} \subseteq J(C)$ of four elements such that:

(i) the sum $\sum_{x \in \mathcal{T}} x$ is zero,
(ii) $\mathcal{T}$ is a set of generators of $J(C)[1 - \rho_*]$, and
(iii) the set $\mathcal{O}(\mathcal{T}) := \{\sum_{x \in \mathcal{T}} a_x x : a \in \mathbb{Z}^4_{\geq 0}, \sum_{x \in \mathcal{T}} a_x \leq 5\}$ satisfies

$$\mathcal{O}(\mathcal{T}) = \Theta_5.$$

Furthermore, for every such subset there exists $\kappa \in \mathbb{F}_5^\times$ and $Q \in \mathcal{B}$ for which $\mathcal{T}$ satisfies

$$\mathcal{T} = \{\kappa[P - Q] : P \in \mathcal{B} \backslash \{Q\}\}.$$

Proof. Let $Q \in \mathcal{B}$ and let $\mathcal{S}_Q$ denote the set $\{[P-Q] : P \in \mathcal{B}\backslash\{Q\}\}$

We start by proving that $\mathcal{S}_Q$ satisfies (i)–(iii), and then we prove so for $\kappa\mathcal{S}_Q$ with $\kappa \in \mathbb{F}_5^\times$. Finally we prove that the sets $\kappa\mathcal{S}_Q$ as κ ranges over $\mathbb{F}_5^\times$ and Q over $\mathcal{B}$ are the only 4-element sets in $J(C)$ that satisfy (i)–(iii). We assume without loss of generality that Q is an affine point (because no statement depends on the model).

That $\mathcal{S}_Q$ satisfies (i) follows from

$$\operatorname{div}\left(\frac{y}{x-x(Q)}\right) = \sum_{P\in\mathcal{B}} P - 5Q.$$

That $\mathcal{S}_Q$ satisfies (ii) follows from Proposition 2.2.2.

Next we prove that $\mathcal{S}_Q$ satisfies (iii). Let α be the Abel-Jacobi map with a branch point $P' \in \mathcal{B}$ as base point so by Corollary 2.2.1 the point Δ is the Riemann constant with respect to α.

Given $Q_1, \ldots, Q_5 \in \mathcal{B}$, we have $\alpha(Q_1 + \cdots + Q_5) \in \Theta_5$ by the Riemann Vanishing Theorem 1.2.2. We also have $5\alpha(Q) = 0$, since the divisor of the function $(x - x(Q))/(x - x(P'))$ is $5Q - 5P'$. Therefore we write

$$\alpha(Q_1 - Q) + \cdots + \alpha(Q_5 - Q) = \alpha(Q_1 + \cdots + Q_5) \in \Theta_5,$$

which by definition of $\mathcal{O}(S_Q)$ implies

$$\mathcal{O}(\mathcal{S}_Q) \subseteq \Theta_5. \tag{2.4}$$

To prove that it is actually an equality, we show that the sets have the same cardinality.

First we give a lower-bound for $\#\Theta_5$ via computing $\#\mathcal{O}(S_Q)$. Given a sequence $T = (t_1, t_2, t_3, t_4)$ such that the set $\{t_1, t_2, t_3, t_4\}$ has 4 elements and satisfies (i)–(ii), we define the map $\gamma[T] : \mathbb{F}_5^3 \to J(C)[1-\rho_*]$ that maps $r \in \mathbb{F}_5^3$ to the sum $\sum_{i=1}^3 r_i t_i \in J(C)[1-\rho_*]$. Note that $\gamma[T]$ is a bijection.

Let e_1, e_2, e_3 be the standard basis vectors of $\mathbb{F}_5^3$, and let $e_4 = -e_1 - e_2 - e_3$, so for $i = 1, \ldots, 4$ we have $\gamma[T](e_i) = t_i$. Consider

$$\mathcal{O}_0 = \left\{ \sum_{i=1}^4 a_i e_i : a \in \mathbb{Z}^4_{\geq 0}, \sum_{i=1}^4 a_i \leq 5 \right\} \subseteq \mathbb{F}_5^3.$$

One can check $\#\mathcal{O}_0 = 101$, and moreover we have $\gamma[T](\mathcal{O}_0) = \mathcal{O}(\{t_1, \ldots, t_4\})$.

In particular, we obtain $\#\mathcal{O}(\mathcal{S}_Q) = 101$ and thus by (2.4) we get

$$\#\Theta_5 \geq 101. \tag{2.5}$$

Next we give an upper-bound for $\#\Theta_5$. By Proposition 2.1.6 the divisors $3P + 2Q + R$ with P, Q, R distinct branch points are non-special, that is, they

satisfy $\deg D = g$ and $\dim \mathcal{L}(\kappa - D) = 0$. Therefore by the Riemann-Roch Theorem they are the only effective divisor in their class. In particular, if P, Q, R are different from P' then we have $\alpha(3P+2Q+R) \neq \alpha(Q_1+\cdots+Q_5)$ for every $Q_1, \ldots, Q_5 \in C$, so by Riemann's Vanishing Theorem 1.2.2 we obtain that $\theta[3\underline{P} + 2\underline{Q} + \underline{R} - \underline{\Delta}](\Omega)$ is non-zero.

There are 24 such divisors with $\{P, Q, R\} \not\ni P'$, which in turn determine 24 distinct divisor classes, hence we conclude

$$\#\{x \in J(C)[1-\rho_*] : \theta[x + \underline{\Delta}](\Omega) \neq 0\} \geq 24. \tag{2.6}$$

Since by Proposition 2.2.2 we have $\#J(C)[1-\rho_*] = 125$, it follows that both (2.5) and (2.6) are equalities and therefore $\mathcal{S}_Q$ satisfies (iii).

Next we consider the sets $\kappa\mathcal{S}_Q$ with $\kappa \in \mathbb{F}_5^\times$. It is clear that $\kappa\mathcal{S}_Q$ also satisfies (i)–(ii). We checked with Magma [3] that $\mathcal{O}_0$ is invariant under the map $x \mapsto \kappa x$ for $\kappa \in \mathbb{F}_5^\times$, and we have the equality

$$\gamma[\kappa T](\mathcal{O}_0) = \gamma[T](\kappa\mathcal{O}),$$

so it follows that (iii) also holds for $\kappa\mathcal{S}_Q$.

Finally, we prove that the 4-element sets κS_Q for $\kappa \in \mathbb{F}_5^\times$ and $Q \in \mathcal{B}$ are the only 4-element sets in $J(C)$ that satisfy (i)–(iii). To do so, let B denote an ordering of $\mathcal{S}_{P'} = \alpha(\mathcal{B})\backslash\{0\}$, consider a sequence $T = (t_1, t_2, t_3, t_4) \in J(C)^4$ such that the set $\{t_1, t_2, t_3, t_4\}$ has 4 elements and satisfies (i)–(iii), and let $\gamma[T]$ be the bijection defined above. Consider the diagram

$$\begin{array}{ccc} \mathbb{F}_5^3 & \xrightarrow{\quad M(T) \quad} & \mathbb{F}_5^3 \\ & {\scriptstyle\gamma[T]}\searrow \quad \swarrow{\scriptstyle\gamma[B]} & \\ & J(C)[1-\rho_*] & \end{array}$$

where $M(T)$ is the unique invertible matrix in $\mathbb{F}_5^{3\times 3}$ that makes the diagram commutative. Note that choosing a matrix $M(T)$ determines T uniquely.

If the set of elements of T satisfies (iii), then we get

$$\gamma[T](\mathcal{O}_0) = \mathcal{O}(\{t_1, t_2, t_3, t_4\}) = \Theta_5 = \gamma[B](\mathcal{O}_0),$$

and thus $\mathcal{O}_0$ is stable under $M(T)$.

We checked with Magma [3] that there are exactly 480 invertible matrices in $\mathbb{F}_5^{3\times 3}$ that map $\mathcal{O}_0$ to itself. Since a matrix $M(T)$ determines T uniquely, there are 480 sequences $T \in J(C)^4$ that satisfy (i)–(iii). However, if we vary $\kappa \in \mathbb{F}_5^\times$, the point $Q \in \mathcal{B}$, and the labeling of the elements in $\mathcal{S}_Q$ we get 480 sequences, and they are different by the equality in (2.3), see proof of Proposition 2.2.2. We conclude that κS_Q for $\kappa \in \mathbb{F}_5^\times$ and $Q \in \mathcal{B}$ are the only 4-element subsets of $J(C)$ that satisfy (i)–(iii). □

From the proof above we obtain the following result.

Corollary 2.2.5. With the notation in Theorem 1.3.6, we get

$$\#\Theta_5 = 101.$$ □

We have now all the tools to give the inverse Jacobian algorithm.

Algorithm 2.2.6

Input: The Jacobian of a CPQ curve C, given by a period matrix $\Omega \in \mathbf{H}_6$, and ρ_* the automorphism on the Jacobian induced by the curve automorphism $\rho(x,y) = (x, z_5 y)$, given by its rational representation $N \in \mathbb{Z}^{12\times 12}$.

Output: Two pairs (l,m) of which at least one is the pair (λ,μ) in a Legendre-Rosenhain equation $y^5 = x(x-1)(x-\lambda)(x-\mu)$ of the CPQ curve C.

1. Let D be the unique solution of $N[D] = D$ in $\frac{1}{2}\mathbb{Z}^{12}/\mathbb{Z}^{12}$.
2. Compute
$$\underline{\Theta_5} = \left\{ \frac{1}{5}\mathbb{Z}^{12}/\mathbb{Z}^{12} : Nx = x \text{ and } \theta[x+D](\Omega) = 0 \right\}.$$
3. Let $X = \{x_1, x_2, x_3, x_4\} \subseteq \underline{\Theta_5}$ be a 4-element set that satisfies
   I. $\sum_{x\in X} x = 0$,
   II. $\{x_1, x_2, x_3\}$ are linearly independent, and
   III. $\{\sum_{x\in X} a_x x : a \in \mathbb{Z}^X_{\geq 0}, \sum_{x\in X} a_x \leq 5\} = \underline{\Theta_5}$.
4. For each $T = \{t_1, t_2, t_3, t_4\} \in \{X, 2X\}$ compute
$$\varepsilon_l = \exp(10\pi i((\widetilde{t_3} - \widetilde{t_2})_1 (\widetilde{t_1})_2)),$$
$$\varepsilon_m = \exp(10\pi i((\widetilde{t_4} - \widetilde{t_2})_1 (\widetilde{t_1})_2),$$
and
$$l_T = \varepsilon_l \left(\frac{\theta[\widetilde{t_2} + 2\widetilde{t_3} + 3\widetilde{t_4} - \widetilde{t_1} - \widetilde{D}](\Omega)}{\theta[\widetilde{t_2} + 2\widetilde{t_3} + 3\widetilde{t_4} - \widetilde{D}](\Omega)} \frac{\theta[2\widetilde{t_2} + \widetilde{t_3} + 3\widetilde{t_4} - \widetilde{D}](\Omega)}{\theta[2\widetilde{t_2} + \widetilde{t_3} + 3\widetilde{t_4} - \widetilde{t_1} - \widetilde{D}](\Omega)} \right)^5,$$
$$m_T = \varepsilon_m \left(\frac{\theta[\widetilde{t_2} + 2\widetilde{t_4} + 3\widetilde{t_3} - \widetilde{t_1} - \widetilde{D}](\Omega)}{\theta[\widetilde{t_2} + 2\widetilde{t_4} + 3\widetilde{t_3} - \widetilde{D}](\Omega)} \frac{\theta[2\widetilde{t_2} + \widetilde{t_4} + 3\widetilde{t_3} - \widetilde{D}](\Omega)}{\theta[2\widetilde{t_2} + \widetilde{t_4} + 3\widetilde{t_3} - \widetilde{t_1} - \widetilde{D}](\Omega)} \right)^5.$$
5. Return (l_X, m_X) and (l_{2X}, m_{2X}).

Warning 2.2.7. As we already saw in the case of Picard curves, Algorithm 2.2.6 is a *mathematical* algorithm but, since it involves infinite sums, complex numbers and exponentials, it cannot be run on a Turing machine or a physical computer. To do so one needs to truncate the sum on the Riemann theta constants, approximate complex numbers and keep track of the error propagation, see Section 1.5 for more details on how to do that.

After applying the algorithm, we obtain two candidates for the approximations of λ and μ. One may then use an algorithm to check which results are correct.

Let (l, m) be one of the pairs from the output, let C be the associated Legendre-Rosenhain equation and let $\Omega' \in \mathbf{H}_6$ satisfy $J(C) \cong \mathbb{C}^6/\Omega'\mathbb{Z}^6 + \mathbb{Z}^6$. If the pair (l, m) is an approximation of (λ, μ), then there exists an isomorphism between $\mathbb{C}^6/\Omega\mathbb{Z}^6 + \mathbb{Z}^6$ and $\mathbb{C}^6/\Omega'\mathbb{Z}^6 + \mathbb{Z}^6$.

One could find such an isomorphism using methods like the numerical computation of homomorphisms in Costa-Mascot-Sijsling-Voight [7].

Remark 2.2.8. In all the cases where we have applied Algorithm 2.2.6 (see Section 2.3), both pairs (l_X, m_X) and (l_{2X}, m_{2X}) yielded isomorphic curves.

Proof of Algorithm 2.2.6. Let $\mathcal{B}$ be the set of branch points of C. By Theorem 2.2.4, the set X in Step 3 is equal to $\{\kappa\underline{[P - P_\infty]} : P \in \mathcal{B}\backslash\{P_\infty\}\}$ for a certain $\kappa \in \mathbb{F}_5^\times$ and $P_\infty \in \mathcal{B}$. We assume without loss of generality $P_\infty = (1 : 0 : 0)$, and that C is given by a Legendre-Rosenhain equation. Let α be the Abel-Jacobi map with base point P_∞. Then we obtain

$$\alpha(\mathcal{B})\backslash\{0\} \in \{X, 2X, -X, -2X\}.$$

Let $\Delta \in J(C)$ be the Riemann constant Δ with respect to P_∞. By Corollary 2.2.1, the Riemann constant Δ is the only point in $J(C)$ that is a 2-torsion point, hence satisfies $\underline{\Delta} \in \frac{1}{2}\mathbb{Z}^{12}/\mathbb{Z}^{12}$, and also satisfies $N[\Delta] = \Delta$. We conclude $D = \underline{\Delta}$ and by Theorem 2.1.7, the pair (l_T, m_T) as in Step 6 is the pair (λ, μ) for some $T \in \{X, 2X, -X, -2X\}$.

Furthermore, since the Riemann theta constants are symmetric and quasi-periodic, the values of l and m do not change if we replace $\widetilde{t_i}$ by $-\widetilde{t_i}$, thus we only need to consider $T \in \{X, 2X\}$, which completes the proof. □

As a consequence of the proof we obtain the following result.

Corollary 2.2.9. If the automorphism given in the input on Algorithm 2.2.6 is ρ_*^k for some $k \in \{2, 3, 4\}$, then the output is also correct.

Proof. Note that the automorphism in the input only plays a role in Steps 1 and 2 of Algorithm 1.3.9, to determine the Riemann constant and the $(1 - \rho_*)$-torsion points in $J(C)$.

Let $k \in \{2, 3, 4\}$ and let α be an Abel-Jacobi map with a branch point as base point. Note that ρ^k fixes the branch points on C. Therefore, by Proposition 1.3.4 the Riemann constant with respect to α satisfies ${}^t\rho_r(\rho_*^k)[\Delta] = \Delta$. It follows that, for $M = {}^t\rho_r(\rho_*^k)$, the characteristic D in Step 1 satisfies $M[D] = D$. We also get

$$\left\{x \in \frac{1}{5}\mathbb{Z}^{12}/\mathbb{Z}^{12} : Mx = N^k x = x \text{ and } \theta[x + D](\Omega) = 0\right\} = \underline{\Theta_5}. \qquad \square$$

2.3 Some CM examples

As in the Picard case (see Section 1.5), after numerically approximating the x-coordinates of the branch points of a CPQ curve with Algorithm 2.2.6, we obtain a polynomial

$$f(x) = x(x-1)(x-\lambda)(x-\mu) \in \mathbb{C}[x]$$

up to some precision. However, the curve may actually be isomorphic to $y^5 = h(x)$ for a certain polynomial h over a number field.

In this case, in order to find h from f we use the invariants of quintic binary forms, recognize them as algebraic numbers and reconstruct h from the exact invariants. This was originally done by Clebsch in [6] and recently implemented by Noordsij in [32, 31].

Note that in order to be able to recognize the invariants as algebraic numbers we have to compute λ and μ with enough precision.

Next we include a list of CPQ curves computed with our algorithm. Analogously to what we saw for Picard curves in Section 1.5, we define a *maximal CM CPQ curve* as a CPQ curve such that its Jacobian has endomorphism ring isomorphic to the maximal order of a degree-12 number field K. We will see in Chapter 4 that K contains a primitive 5th root of unity $\zeta_5 \in K$, and is determined by a totally real cubic field K_0 that satisfies $K = K_0(\zeta_5)$.

For details on how to obtain period matrices for the Jacobians of maximal CM CPQ curves and the corresponding automorphism from the field K see Section 4.1.

Using Algorithm 2.2.6 we computed numerical approximations of some maximal CM curves. Here we present the resulting CPQ curves which are numerically close (and conjecturally equal) to the maximal CM curves. In Chapter 4 we will see that, in particular, this list contains conjectural models for all CPQ curves defined over $\mathbb{Q}$ with maximal CM over $\mathbb{C}$.

We obtained the following curves:

(1) $y^5 = x^4 - 24x^3 + 3x^2 + x$ with K_0 defined by $x^3 - 3x - 1$.
(2) $y^5 = x^4 - 7x^2 + 7x$ with K_0 defined by $x^3 - x^2 - 2x + 1$.
(3) $y^5 = x^4 - 390x^2 + 13000x + 257725$ with K_0 defined by $x^3 - x^2 - 4x - 1$.
(4) $y^5 = x^4 + 1290x^2 + 35000x + 228525$ with K_0 defined by $x^3 - 12x - 14$.