An inverse Jacobian algorithm for Picard curves

J.-C. Lario, A. Somoza, C. Vincent

J.-C. Lario et al. *Res. Number Theory* (2021) 7:32
https://doi.org/10.1007/s40993-021-00253-1

Research in Number Theory

RESEARCH

An inverse Jacobian algorithm for Picard curves

Joan-C. Lario[1], Anna Somoza[2*] and Christelle Vincent[3]

*Correspondence:
anna.somoza.henares@gmail.com
[2] Institut de recherche mathématique de Rennes, Université de Rennes 1, Rennes, France
Full list of author information is available at the end of the article

Abstract

We study the inverse Jacobian problem for the case of Picard curves over $\mathbb{C}$. More precisely, we elaborate on an algorithm that, given a small period matrix $\Omega \in \mathbb{C}^{3\times 3}$ corresponding to a principally polarized abelian threefold equipped with an automorphism of order 3, returns a Legendre–Rosenhain equation for a Picard curve with Jacobian isomorphic to the given abelian variety. Our method corrects a formula obtained by Koike–Weng (Math Comput 74(249):499–518, 2005) which is based on a theorem of Siegel. As a result, we apply the algorithm to obtain equations of all the isomorphism classes of Picard curves with maximal complex multiplication by the maximal order of the sextic CM-fields with class number at most 4. In particular, we obtain the complete list of maximal CM Picard curves defined over $\mathbb{Q}$. In the appendix, Vincent gives a correction to the generalization of Takase's formula for the inverse Jacobian problem for hyperelliptic curves given in [Balakrishnan–Ionica–Lauter–Vincent, LMS J. Comput. Math., 19(suppl. A):283-300, 2016].

Keywords: Picard curve, Hyperelliptic curves, Genus 3, Inverse Jacobian, Explicit algorithm

Mathematics Subject Classification: 14H25, 14H45, 14K25, 14Q05

1 Introduction

Let J be the map from the set M_g of isomorphism classes of algebraic curves of genus g defined over $\mathbb{C}$ to the set A_g of isomorphism classes of complex principally polarized abelian varieties of dimension g. In this context, the *inverse Jacobian problem* consists of identifying a model of the preimage via J of the class of a given principally polarized abelian variety, if it exists. This is a classic result in the case of curves of genus 1, and has also been solved for curves of genus 2 [26,36] and genus 3 [2,7,14,34,38,39].

In this paper we present an inverse Jacobian algorithm for the family of Picard curves. This was initially done by Koike and Weng in [14], but their exposition presents some gaps and mistakes that we fix here.

In Sect. 2 we give a formula to approximate the x-coordinates of the affine branch points of a Picard curve in terms of theta constants of its Jacobian, see Theorem 3. The given formula differs from the result in [14] by a third root of unity, see Remark 1.

In Sect. 3 we first characterize the image under J of this family of curves, and then develop the algorithm that takes the Jacobian of a Picard curve C and returns a Legendre–Rosenhain equation for C, see Algorithm 5. The main step of the algorithm is applying the formula of Theorem 3, so we first identify the objects needed to apply said formula, mainly the Riemann constant and the images by the Abel-Jacobi map of the affine branch points. Our algorithm makes the process of identifying these points explicit in Theorem 4, see Remark 3 for a comparison with the approach of [14].

Our correction of the algorithm allows us to re-obtain the results of [14] and extend the list of known maximal CM Picard curves, that is, Picard curves such that their Jacobians have endomorphism ring isomorphic to the maximal order of a sextic CM number field K. We obtain twenty-three new curves, displayed in Sect. 4, among which we include all maximal CM Picard curves defined over $\mathbb{Q}$. The corresponding CM-fields are collected from [23]. The computations have been performed using SageMath [35], and an implementation can be found at [31].

In the appendix, Vincent applies the tools introduced in Sect. 2 to correct a sign in the generalization of Takase's formula for the inverse Jacobian problem for hyperelliptic curves, given in [2].

The present paper is an extension and clarification of our earlier work [16] to include further improvements of the algorithm, such as Theorem 4.

2 A Thomae-like formula for Picard curves

Let C be a Picard curve defined over $\mathbb{C}$, that is, a genus-3 smooth, plane, projective curve given by the affine equation $y^3 = f(x)$ where f is a polynomial of degree 4. The curve C has an automorphism ρ of order 3 given by $(x, y) \mapsto (x, z_3 y)$ with $z_3 = \exp\left(\frac{2\pi i}{3}\right)$. This automorphism fixes the *affine branch points* $(t, 0)$ with $f(t) = 0$. The curve C has a unique point at infinity, with projective coordinates $(0 : 1 : 0)$, which is also fixed by the automorphism ρ.

Up to isomorphism, we can (and do) assume that C is given by a *Legendre–Rosenhain equation*

$$y^3 = x(x-1)(x-\lambda)(x-\mu). \tag{1}$$

Let $H^0(\omega_C)$ be the space of holomorphic differentials of C, let $H^0(\omega_C)^*$ be its dual and let $H_1(C, \mathbb{Z})$ be the first homology group of C. Following the literature, for example [4, Sect. 11.1], we define the Jacobian of C as $J(C) = H^0(\omega_C)^*/H_1(C, \mathbb{Z})$, and for $\omega = (\omega_1, \ldots, \omega_g)$ a basis of $H^0(\omega_C)$ and the base point $P_\infty = (0 : 1 : 0)$ we define the Abel-Jacobi map

$$\alpha : C \to J(C), \quad Q \mapsto \int_{P_\infty}^{Q} \omega,$$

and extend it additively to divisors of C.

Choosing a symplectic basis of $H_1(C, \mathbb{Z})$ gives rise to the isomorphism $J(C) \simeq \mathbb{C}^3/(\Omega\mathbb{Z}^3 + \mathbb{Z}^3)$, where Ω is a matrix in the Siegel upper half-space $\mathbf{H}_3 = \{Z \in \mathbb{C}^{3\times 3} : Z = Z^t, \mathrm{Im}(Z) > 0\}$, where $(\cdot)^t$ denotes transposition and $(\cdot) > 0$ denotes positive-definiteness. We say that Ω is *a (small) period matrix for* C.

The following two classical theorems, due to Riemann and Siegel respectively, deal with the zero locus of the Riemann theta functions and the values of a function of an algebraic curve on non-special divisors. Recall that the *Riemann theta function* $\theta : \mathbb{C}^g \times \mathbf{H}_g \to \mathbb{C}$ is

given by

$$\theta(z,\Omega)=\sum_{n\in\mathbb{Z}^g}\exp(\pi i n^t\Omega n+2\pi i n^t z),$$

and that a non-special divisor D is a divisor with $\ell(K-D)=0$ for K a canonical divisor of C.

Theorem 1 (Riemann's Vanishing Theorem, see [21, Corollary 3.6]) *Let C be a curve defined over $\mathbb{C}$ of genus g, let $J(C)$ be the Jacobian of C with period matrix $\Omega\in\mathbf{H}_g$ and let α be an Abel-Jacobi map of C. There is an element $\Delta\in J(C)$, called a Riemann constant with respect to α, such that the function $\theta(\cdot,\Omega)$ vanishes at $z\in\mathbb{C}^g$ if and only if there exist $Q_1,\dots,Q_{g-1}\in C$ that satisfy*

$$z\equiv\alpha(Q_1+\cdots+Q_{g-1})-\Delta \mod(\Omega\mathbb{Z}^g+\mathbb{Z}^g).$$

The choice of a base point determines uniquely the Riemann constant Δ, as shown by Mumford in Theorem 3.10 and Corollary 3.11 of [21].

Theorem 2 (Siegel [30, Theorem 11.3]) *Let C be a curve of genus g over $\mathbb{C}$, and let ϕ be a function on C with*

$$\operatorname{div}(\phi)=\sum_{i=1}^m A_i-\sum_{i=1}^m B_i.$$

Let $P\in C$ and let ω be a basis of $H^0(\omega_C)$ for which the Jacobian $J(C)$ has period matrix $\Omega\in\mathbf{H}_g$. Let Δ be the Riemann constant with respect to the Abel-Jacobi map α with base point P.

Choose paths from the base point P to A_i and B_i that satisfy

$$\sum_{i=1}^m\int_P^{A_i}\omega=\sum_{i=1}^m\int_P^{B_i}\omega.$$

Then, given an effective non-special divisor $D=P_1+\cdots+P_g$ of degree g that satisfies $P_j\notin\{A_i,B_i:1\le i\le m\}$, one has

$$\phi(D):=\phi(P_1)\cdots\phi(P_g)=E\prod_{i=1}^m\frac{\theta(\sum_{j=1}^g\int_P^{P_j}\omega-\int_P^{A_i}\omega-\Delta,\Omega)}{\theta(\sum_{j=1}^g\int_P^{P_j}\omega-\int_P^{B_i}\omega-\Delta,\Omega)},\tag{2}$$

where $E\in\mathbb{C}^\times$ is independent of D, and the integrals from P to P_j take the same paths both in the numerator and the denominator. □

Observe that in (2) we are evaluating the Riemann theta functions at points of the Jacobian.

We shall need a version of Theorem 2 in terms of Riemann theta constants. Given $c=(c_1,c_2)$ with $c_i\in\mathbb{R}^g$, the *Riemann theta constant (with characteristic c)* is the function $\theta[c]\colon\mathbf{H}_g\to\mathbb{C}$ given by

$$\theta\begin{bmatrix}c_1\\c_2\end{bmatrix}(\Omega)=\exp(\pi i c_1^t\Omega c_1+2\pi i c_1^t c_2)\theta(\Omega c_1+c_2,\Omega).\tag{3}$$

We use the following two elementary properties of the Riemann theta constants: They are even in c, that is,

$$\theta[c](\Omega)=\theta[-c](\Omega),\tag{4}$$

and they are quasi-periodic in c, that is, for $m = (m_1, m_2) \in \mathbb{Z}^{2g}$ one has

$$\theta[c+m](\Omega) = \exp(2\pi i c_1 m_2)\theta[c](\Omega). \tag{5}$$

Due to the quasi-periodicity of the Riemann theta constants, we must fix representatives in $\mathbb{R}^{2g}$ for the points of the Jacobian. Throughout, we consider the composition of the maps

$$C \xrightarrow{\alpha} J(C) \xrightarrow{\cdot} \mathbb{R}^{2g}/\mathbb{Z}^{2g} \xrightarrow{\widetilde{\cdot}} [0,1)^{2g} \tag{6}$$

where α is the Abel-Jacobi map, the map $\cdot$ identifies $J(C)$ with $\mathbb{R}^{2g}/\mathbb{Z}^{2g}$ via $\Omega c_1 + c_2 \mapsto (c_1, c_2)$ and $\widetilde{\cdot}$ maps a class in $\mathbb{R}^{2g}/\mathbb{Z}^{2g}$ to its representative with entries in $[0,1)$. For $P \in C$ we write $\widetilde{P}$ instead of $\widetilde{\alpha(P)}$; and in the case of a divisor $D = \sum n_P P$, we define $\widetilde{D} := \sum n_P \widetilde{P} \in \mathbb{R}^{2g}$. Note that with this definition for most divisors D we get that $\widetilde{D}$ and $\widetilde{\alpha(D)}$ are different.

With the definitions above, one can rewrite Theorem 2 in terms of Riemann theta constants as follows:

Corollary 1 *With the notation of* Theorem 2, *let* $a_i = ((a_i)_1, (a_i)_2)$ *(respectively* b_i*) be the element in* $\mathbb{R}^{2g}$ *that satisfies* $\int_P^{A_i} \omega = \Omega(a_i)_1 + (a_i)_2$ *(respectively* $\int_P^{B_i} \omega = \Omega(b_i)_1 + (b_i)_2$*). We have*

$$\phi(D) = E' \prod_{i=1}^{m} \frac{\theta\left[\widetilde{D} - a_i - \widetilde{\Delta}\right](\Omega)}{\theta\left[\widetilde{D} - b_i - \widetilde{\Delta}\right](\Omega)},$$

where $E' \in \mathbb{C}^\times$ *is also independent of* D.

Proof Observe that the exponential factor in (3) for Riemann theta constants can be written as $\exp(\pi i B(x,x))$ where B is the symmetric bilinear form given by

$$B(u,v) = u^t \begin{pmatrix} \Omega & \mathrm{id}_g \\ \mathrm{id}_g & 0 \end{pmatrix} v.$$

Let $Q(u) = B(u,u)$ and let $c = \widetilde{D} - \widetilde{\Delta}$. For $j = 1, \ldots, g$, let $x_j = \widetilde{P}_j$ and choose a path from P to P_j that satisfies $\int_P^{P_j} \omega = \Omega(x_j)_1 + (x_j)_2 \in \mathbb{C}^g$.

Let $E' \in \mathbb{C}^\times$ be defined by

$$E \prod_{i=1}^{m} \frac{\theta\left(\left(\sum_{j=1}^{g} \int_P^{P_j} \omega\right) - \int_P^{A_i} \omega - \Delta, \Omega\right)}{\theta\left(\left(\sum_{j=1}^{g} \int_P^{P_j} \omega\right) - \int_P^{B_i} \omega - \Delta, \Omega\right)} = E' \prod_{i=1}^{m} \frac{\theta\left[\widetilde{D} - a_i - \widetilde{\Delta}\right](\Omega)}{\theta\left[\widetilde{D} - b_i - \widetilde{\Delta}\right](\Omega)}.$$

We want to prove that E' does not depend on D. By (3) we get

$$\frac{E}{E'} = \exp\left(\pi i \sum_{i=1}^{m} (Q(c - a_i) - Q(c - b_i))\right),$$

so it suffices to show that $\sum_{i=1}^{m} (Q(c-a_i) - Q(c-b_i))$ does not depend on D. We have

$$\begin{aligned} \sum_{i=1}^{m} (Q(c-a_i) - Q(c-b_i)) &= \sum_{i=1}^{m} (Q(a_i) - Q(b_i) - 2B(c, a_i - b_i)) \\ &= \sum_{i=1}^{m} Q(a_i) - \sum_{i=1}^{m} Q(b_i) - 2B\left(c, \sum_{i=1}^{m} (a_i - b_i)\right), \end{aligned}$$

but we know

$$\sum_{i=1}^{m} \int_P^{A_i} \omega = \sum_{i=1}^{m} \int_P^{B_i} \omega,$$

so in terms of characteristics we obtain $\sum_{i=1}^{m}(a_i - b_i) = 0$ and then it follows that

$$\sum_{i=1}^{m}(Q(c-a_i) - Q(c-b_i)) = \sum_{i=1}^{m} Q(a_i) - \sum_{i=1}^{m} Q(b_i)$$

does not depend on D. □

Lemma 1 *Let C be a Picard curve defined over $\mathbb{C}$ given by $y^3 = x(x-1)(x-\lambda)(x-\mu)$, and consider the branch points $P_0 = (0,0)$, $P_1 = (1,0)$, $P_\lambda = (\lambda,0)$, $P_\mu = (\mu,0)$, and P_∞ at infinity. Let $J(C)$ be the Jacobian of C with period matrix Ω, let α be the Abel-Jacobi map with base point P_∞, and let $\Delta \in J(C)$ be the associated Riemann constant.*

Then, for every non-special divisor $D = R_1 + R_2 + R_3$, we have

$$x(D) = E\,\varepsilon(D)\left(\frac{\theta[\widetilde{D} - \widetilde{P}_0 - \widetilde{\Delta}](\Omega)}{\theta[\widetilde{D} - \widetilde{\Delta}](\Omega)}\right)^3,$$

where $\varepsilon(D) = \exp(6\pi i(\widetilde{D} - \widetilde{P}_0 - \widetilde{\Delta})_1(\widetilde{P}_0)_2)$, $E \in \mathbb{C}^\times$ is a constant independent of D and, as before, $x(D)$ is the product of the x-coordinates of each point in the divisor.

Proof Let ω be the basis of holomorphic differentials for which $J(C)$ has period matrix Ω. The divisor of the function x on C is $\operatorname{div}(x) = 3P_0 - 3P_\infty$, so in order to apply Corollary 1 for $\phi = x$ and $P = P_\infty$, we choose three 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

$$\int_{\gamma_1} \omega = \Omega(a_1)_1 + (a_1)_2 \in \mathbb{C}^3,$$

and paths γ_2, γ_3 from P_∞ to P_0 that satisfy

$$\sum_{k=1}^{3}\int_{\gamma_k} \omega = 0 \text{ in } \mathbb{C}^3. \tag{7}$$

Let a_2, a_3 be the elements in $\mathbb{R}^6$ that satisfy

$$\int_{\gamma_k} \omega = \Omega(a_k)_1 + (a_k)_2 \text{ for } k = 2, 3.$$

Then, by Corollary 1, we have

$$x(D) = E' \prod_{k=1}^{3} \frac{\theta[\widetilde{D} - a_k - \widetilde{\Delta}](\Omega)}{\theta[\widetilde{D} - \widetilde{\Delta}](\Omega)} \tag{8}$$

for some constant $E' \in \mathbb{C}^\times$ independent of D. Note that for $k = 1, 2, 3$ we have

$$\underline{P_0} = (a_k \bmod \mathbb{Z}^6),$$

so the differences $a_i - a_j$ for $i \neq j$ are integer vectors. Applying the quasi-periodicity property (5), Eq. (8) becomes

$$\phi(D) = E' \frac{\exp(2\pi i(\widetilde{D} - \widetilde{P}_0 - \widetilde{\Delta})_1(a_1 - a_2 + a_1 - a_3)_2)\,\theta[\widetilde{D} - \widetilde{P}_0 - \widetilde{\Delta}](\Omega)^3}{\theta[\widetilde{D} - \widetilde{\Delta}](\Omega)^3}.$$

But it follows from (7) that the sum $a_1 + a_2 + a_3$ is zero, so we obtain $a_1 - a_2 + a_1 - a_3 = 3a_1 = 3\widetilde{P}_0$ and the statement follows. □

The final step is to choose the right non-special divisors.

Theorem 3 *Let C be a Picard curve defined over $\mathbb{C}$ given by $y^3 = x(x-1)(x-\lambda)(x-\mu)$, and consider the branch points $P_0 = (0,0)$, $P_1 = (1,0)$, $P_\lambda = (\lambda,0)$, $P_\mu = (\mu,0)$, and P_∞ at infinity. Let $J(C)$ be the Jacobian of C with period matrix Ω, let α be the Abel-Jacobi map with base point P_∞, and let $\Delta \in J(C)$ be the associated Riemann constant. Then, for $\eta \in \{\lambda, \mu\}$, we have*

$$\eta = \varepsilon_\eta \left(\frac{\theta[\widetilde{P}_1 + 2\widetilde{P}_\eta - \widetilde{P}_0 - \widetilde{\Delta}](\Omega)}{\theta[2\widetilde{P}_1 + \widetilde{P}_\eta - \widetilde{P}_0 - \widetilde{\Delta}](\Omega)} \right)^3, \tag{9}$$

where $\varepsilon_\eta = \exp(6\pi i((\widetilde{P}_\eta - \widetilde{P}_1)_1(\widetilde{P}_0)_2 + \widetilde{\Delta}_1(3\widetilde{P}_1 + 3\widetilde{P}_\eta - 2\widetilde{\Delta})_2))$.

Proof We apply Lemma 1 twice, to the divisors $D_1 = P_1 + 2P_\eta$ and $D_2 = 2P_1 + P_\eta$, which are non-special as proven in [14, p. 506]. Then, we get

$$\begin{aligned} \eta = \frac{x(P_1)x(P_\eta)^2}{x(P_1)^2x(P_\eta)} &= \frac{E'\varepsilon(D_1)\left(\frac{\theta[\widetilde{P}_1 + 2\widetilde{P}_\eta - \widetilde{P}_0 - \widetilde{\Delta}](\Omega)}{\theta[\widetilde{P}_1 + 2\widetilde{P}_\eta) - \widetilde{\Delta}](\Omega)} \right)^3}{E'\varepsilon(D_2)\left(\frac{\theta[2\widetilde{P}_1 + \widetilde{P}_\eta - \widetilde{P}_0 - \widetilde{\Delta}](\Omega)}{\theta[2\widetilde{P}_1 + \widetilde{P}_\eta - \widetilde{\Delta}](\Omega)} \right)^3} \\ &= \frac{\varepsilon(D_1)}{\varepsilon(D_2)} \left(\frac{\theta[\widetilde{P}_1 + 2\widetilde{P}_\eta - \widetilde{P}_0 - \widetilde{\Delta}](\Omega)}{\theta[\widetilde{P}_1 + 2\widetilde{P}_\eta - \widetilde{\Delta}](\Omega)} \frac{\theta[2\widetilde{P}_1 + \widetilde{P}_\eta - \widetilde{\Delta}](\Omega)}{\theta[2\widetilde{P}_1 + \widetilde{P}_\eta - \widetilde{P}_0 - \widetilde{\Delta}](\Omega)} \right)^3. \end{aligned} \tag{10}$$

Moreover, using the symmetry (4) and quasi-periodicity (5) of the Riemann theta constants we also obtain

$$\begin{aligned} \theta[\widetilde{D}_2 - \widetilde{\Delta}](\Omega) &= \theta[-\widetilde{D}_2 + \widetilde{\Delta}](\Omega) \\ &= \theta[\widetilde{D}_1 - \widetilde{\Delta} + \underbrace{2\widetilde{\Delta} - 3\widetilde{P}_1 - 3\widetilde{P}_\eta)}_{\in \mathbb{Z}^6}](\Omega) \\ &= \exp(2\pi i(\widetilde{D}_1 - \widetilde{\Delta})_1(2\widetilde{\Delta} - 3\widetilde{P}_1 - 3\widetilde{P}_\eta)_2))\theta[\widetilde{D}_1 - \widetilde{\Delta}](\Omega) \end{aligned}$$

so that (10) becomes

$$\eta = \varepsilon_\eta \cdot \left(\frac{\theta[\widetilde{P}_1 + 2\widetilde{P}_\eta - \widetilde{P}_0 - \widetilde{\Delta}](\Omega)}{\theta[2\widetilde{P}_1 + \widetilde{P}_\eta - \widetilde{P}_0 - \widetilde{\Delta}](\Omega)} \right)^3,$$

with

$$\begin{aligned} \varepsilon_\eta &= \frac{\varepsilon(D_1)}{\varepsilon(D_2)} \exp(2\pi i(\widetilde{D}_1 - \widetilde{\Delta})_1(2\widetilde{\Delta} - 3\widetilde{P}_1 - 3\widetilde{P}_\eta)_2)^3 \\ &= \frac{\exp(6\pi i(\widetilde{P}_1 + 2\widetilde{P}_\eta - \widetilde{P}_0 - \widetilde{\Delta})_1(\widetilde{P}_0)_2)}{\exp(6\pi i(2\widetilde{P}_1 + \widetilde{P}_\eta - \widetilde{P}_0 - \widetilde{\Delta})_1(\widetilde{P}_0)_2)} \exp(6\pi i(\widetilde{D}_1 - \widetilde{\Delta})_1(2\widetilde{\Delta} - 3\widetilde{P}_1 - 3\widetilde{P}_\eta)_2) \\ &= \exp(6\pi i((\widetilde{P}_\eta - \widetilde{P}_1)_1(\widetilde{P}_0)_2 + \widetilde{\Delta}_1(3\widetilde{P}_1 + 3\widetilde{P}_\eta - 2\widetilde{\Delta})_2)) \end{aligned}$$

as desired. □

Remark 1 Compare the above formula in Theorem 3 with the ones given in [14, Eq. 9]. The formulas there are the same as in (9) replacing ε_η by 1, hence in general they do not hold due to the absence of the precise root of unity.

However, if we follow the original work by Picard [24, p. 131], then we obtain a particular form of the period matrix Ω (see also Shiga [27, Proposition I-3]) for which it is always the case that $\varepsilon_\lambda = \varepsilon_\mu = 1$. In such case, the formulas in [14] hold.

3 The algorithm

In this section we explain how to use the formula in Theorem 3 to obtain an inverse Jacobian algorithm for Picard curves, that is, an algorithm that, given the Jacobian of a Picard curve C, returns a model of C.

The following result characterizes the Jacobian of a Picard curve based on work of Koike–Weng and Estrada.

Proposition 1 *Let X be a simple principally polarized abelian variety of dimension 3 defined over an algebraically closed field k. If X has an automorphism φ of order 3, then we have that X is the Jacobian of a Picard curve. Furthermore, let ρ be the curve automorphism $\rho(x, y) = (x, z_3 y)$, and let ρ_* be the automorphism of the Jacobian that it induces. Then we get $\langle \varphi \rangle = \langle \rho_* \rangle$.*

Proof By Oort–Ueno [22], based on work by Matsusaka [18] and Hoyt [9], we have that since X is a simple principally polarized abelian variety of dimension 3 over an algebraically closed field, then it is the Jacobian of a curve. Let C be a curve with $X \cong J(C)$.

By Torelli's Theorem, see Milne [19, Sect. 12], there is some non-trivial automorphism ν of C that satisfies $\varphi = \pm\nu_*$. Then the automorphism ν^4, which we call η, satisfies $\eta_* = (\nu^4)_* = (\pm\nu)_*^4 = \varphi^4 = \varphi$, hence by the uniqueness in Torelli's Theorem we obtain that η has order 3.

Therefore, the degree of the map $\pi : C \to C/\langle\eta\rangle$ is also 3, and by the Riemann–Hurwitz formula one obtains that $C/\langle\eta\rangle$ has either genus 0 or 1. But X is simple, so the curve $C/\langle\eta\rangle$ is isomorphic to $\mathbb{P}^1$ and π has 5 ramification points.

Then $k(C)/k(C/\langle\eta\rangle)$ is a Kummer extension of degree 3, hence C is given by an equation of the form $y^3 = h(x)$ where h has 4 different roots. By Lemma 7.3 in Estrada [8, Appendix I], we obtain a model for C given by $y^3 = f(x)$ where f has degree 4 and distinct roots and η is either the automorphism ρ given by $(x, y) \mapsto (x, z_3 y)$ or its square. □

Remark 2 While the idea behind the proof is the same in Proposition 1 and in [14, Lemma 1], the assumptions in [14] are in a way more restrictive, as Koike and Weng focus on maximal CM Picard curves. Moreover, the proof in [14] has a gap, which is fixed exactly by our reference to Estrada [8, Appendix I].

We provide the proof above as an homage to Koike–Weng, but one could alternatively use the classifications of plane quartics and genus-3 hyperelliptic curves by their automorphism group to prove the result: by Propositions 1.1 and 1.2 in [17] one concludes that the only genus-3 curves with order-3 automorphisms that have simple Jacobians are Picard curves.

It follows from Proposition 1 that one can think of the input of the inverse Jacobian algorithm for Picard curves to be a period matrix $\Omega \in \mathbf{H}_3$ together with the rational representation of an automorphism of order 3. To give the curve we will compute the values of λ and μ in a Legrendre–Rosenhain equation of the curve.

First we want to determine the points in $\mathbb{C}^3/(\Omega\mathbb{Z}^3+\mathbb{Z}^3)$ that correspond to the Riemann constant Δ and the image of the branch points via α. The former is given by the following result due to Koike and Weng.

Proposition 2 (Koike–Weng [14, Lemma 10]) *Let $J(C)$ be the Jacobian of a Picard curve C, let ρ_* be the automorphism of $J(C)$ induced by the curve automorphism $\rho(x, y) = (x, z_3 y)$, and let $N = \begin{pmatrix} n_{11} & n_{12} \\ n_{21} & n_{22} \end{pmatrix} \in \mathrm{Sp}(6, \mathbb{Z})$ be the transposed rational representation of ρ_*. Then, the Riemann constant $\Delta \in J(C)$ is the unique 2-torsion point that satisfies*

$$\underline{\Delta} = (N^{-1})^t \underline{\Delta} + \frac{1}{2} \begin{pmatrix} (n_{21}^t n_{22})_0 \\ (n_{11}^t n_{12})_0 \end{pmatrix} =: N[\underline{\Delta}],$$

where $(\cdot)_0$ denotes the diagonal of the matrix as a column vector.

The following step is to identify the image under α of the branch points.

Theorem 4 *Let $J(C)$ be the Jacobian of a Picard curve C, let ρ_* be the automorphism of $J(C)$ induced by the curve automorphism $\rho(x, y) = (x, z_3 y)$. Let $\mathcal{B}$ be the set of affine branch points of C, let α be the Abel-Jacobi map with base point $P_\infty = (0 : 1 : 0)$, let Δ be the Riemann constant with respect to α and define*

$$\Theta_3 := \left\{ x \in J(C)[1 - \rho_*] : \theta[\underline{x} + \underline{\Delta}](\Omega) = 0 \right\}.$$

Then $\alpha(\mathcal{B})$ and $-\alpha(\mathcal{B})$ are the only subsets $\mathcal{T} \subset J(C)$ 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 $\mathcal{O}(\mathcal{T}) := \{\sum_{x \in \mathcal{T}} a_x x : a \in \mathbb{Z}^4_{\geq 0}, \sum_{x \in \mathcal{T}} a_x \leq 2\}$ satisfies*

$$\mathcal{O}(\mathcal{T}) = \Theta_3.$$

Proof We first show that $\alpha(\mathcal{B})$ and $-\alpha(\mathcal{B})$ satisfy (i)–(iii), and then we prove that these are the only possibilities.

That $\alpha(\mathcal{B})$ satisfies (i) follows from $\mathrm{div}(y) = \sum_{P \in \mathcal{B}} P - 4P_\infty$. That $\alpha(\mathcal{B})$ satisfies (ii) is proven by Koike and Weng in [14, Remark 8]. Next we prove that $\alpha(\mathcal{B})$ satisfies (iii). On the one hand, given $Q_1, Q_2 \in \mathcal{B} \cup \{P_\infty\}$ we have $\alpha(Q_1 + Q_2) \in \Theta_3$ by Riemann's Vanishing Theorem 1, and since we have $\alpha(P_\infty) = 0$, this implies

$$\left\{ \sum_{P \in \mathcal{B}} a_P \alpha(P) : a \in \mathbb{Z}^{\mathcal{B}}_{\geq 0}, \sum_{P \in \mathcal{B}} a_P \leq 2 \right\} \subseteq \Theta_3.$$

To prove the opposite inclusion, let $x \in \Theta_3$. Since x satisfies $\theta[\underline{x} + \underline{\Delta}](\Omega) = 0$, by Riemann's Vanishing Theorem 1 there exist $Q_1, Q_2 \in C$ such that we have $x = \alpha(Q_1 + Q_2)$. Moreover, since x is a $(1 - \rho_*)$-torsion point, we get

$$\alpha(Q_1 + Q_2) = \rho_*(\alpha(Q_1 + Q_2)) = \alpha(\rho(Q_1) + \rho(Q_2)),$$

hence there exists a function h on C such that $\mathrm{div}(h) = \rho(Q_1) + \rho(Q_2) - Q_1 - Q_2$. Note now that a Picard curve is non-hyperelliptic, since one checks that the canonical map is the embedding $(x : y : 1) \colon C \to \mathbb{P}^2$. Then we conclude that h is constant, since otherwise it has degree at most 2, hence the curve would be hyperelliptic. Therefore we have $\rho(Q_1) + \rho(Q_2) = Q_1 + Q_2$, but since ρ has order 3, the cardinality of the orbit of Q_i

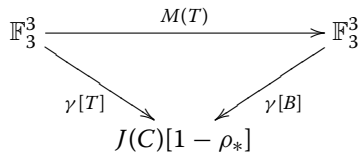
has length 3 or 1, so we obtain $\rho(Q_i) = Q_i$. Therefore Q_1 and Q_2 are branch points, so the other inclusion holds.

It is clear that $-\alpha(\mathcal{B})$ satisfies (i) and (ii). To see that it satisfies (iii), it is enough to prove that Θ_3 is invariant under the map $x \mapsto -x$. But this follows from the symmetry of the Riemann theta constants, see (4).

Next we prove that $\alpha(\mathcal{B})$ and $-\alpha(\mathcal{B})$ are, in fact, all the subsets that satisfy (i)–(iii).

Let B denote an ordering of $\alpha(\mathcal{B})$. Given a sequence $T = (t_1, t_2, t_3, t_4)$ in $J(C)^4$ of distinct elements such that the set $\{t_1, t_2, t_3, t_4\}$ satisfies (i)–(iii), we define the map $\gamma[T]\colon \mathbb{F}_3^3 \to J(C)[1-\rho_*]$ given by $r \mapsto \sum_{i=1}^3 r_i t_i$. By Remark 8 in Koike–Weng [14] we have $J(C)[1-\rho_*] \cong (\mathbb{Z}/3\mathbb{Z})^3$, thus it follows from (i) and (ii) that $\gamma[T]$ is a bijection.

Consider the diagram



where $M(T)$ is the unique invertible matrix in $\mathbb{F}_3^{3\times 3}$ that makes the diagram commutative. Note that choosing a matrix $M(T)$ determines T uniquely.

Let e_1, e_2, e_3 be the standard basis vectors of $\mathbb{F}_3^3$, 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

$$\mathcal{O}_0 = \left\{ \sum_{i=1}^4 a_i e_i : a \in \mathbb{Z}_{\geq 0}^4, \sum_{i=1}^4 a_i \leq 2 \right\} \subset \mathbb{F}_3^3.$$

One can check $\#\mathcal{O}_0 = 15$, and moreover we have $\gamma[T](\mathcal{O}_0) = \mathcal{O}(\{t_1, t_2, t_3, t_4\})$. If the set of elements of T satisfies (iii), then we have

$$\gamma[T](\mathcal{O}_0) = \mathcal{O}(\{t_1, t_2, t_3, t_4\}) = \Theta_3 = \gamma[B](\mathcal{O}_0),$$

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

We checked with SageMath [35] that there are exactly 48 invertible matrices in $\mathbb{F}_3^{3\times 3}$ that map $\mathcal{O}_0$ to itself. Since a matrix $M(T)$ determines T uniquely, there are 48 sequences $T \in J(C)^4$ that satisfy (i)–(iii). However, if we vary σ in the symmetric group of 4 letters and $s \in \{\pm 1\}$, then $s\sigma(B)$ gives 48 sequences, which are different. We conclude that $\alpha(\mathcal{B})$ and $-\alpha(\mathcal{B})$ are the only subsets of $J(C)$ with 4 elements that satisfy (i)–(iii). □

Remark 3 With Theorem 4, we make precise the idea hinted in Corollary 11 of Koike–Weng [14]. There, they claim the existence of a 4-element set that satisfies (i) and (ii), prove that $\alpha(\mathcal{B})$ does satisfy (i) and (ii), and assume without further comments that when one finds such a set, it is $\alpha(\mathcal{B})$.

This is problematic not only because they disregard the case where the set is $-\alpha(\mathcal{B})$ but especially because they do not consider (iii), since there exist 4-element sets in $J(C)$ that satisfy (i) and (ii) which are not $\alpha(\mathcal{B})$ or even $-\alpha(\mathcal{B})$.

In fact, there are $\#\,\mathrm{GL}_3(\mathbb{F}_3) = 11,232$ possible sequences $T \in J(C)^4$ that satisfy (i) and (ii), hence the probability of finding one that corresponds to a permutation of B is $1/468 \approx 0.002$.

We now have all the tools to state the algorithm.

Algorithm 5

Input: *A period matrix $\Omega \in \mathbf{H}_3$ of the Jacobian of a Picard curve C, and the transposed rational representation $N \in \mathbb{Z}^{6\times 6}$ of the automorphism of the Jacobian ρ_* induced by the curve automorphism $\rho(x, y) = (x, z_3 y)$.*

Output: *The complex values λ and μ in a Legendre–Rosenhain equation $y^3 = x(x-1)(x-\lambda)(x-\mu)$ for the Picard curve C.*

Steps:

1. *Let D be the unique solution of $N[D] = D$ in $\frac{1}{2}\mathbb{Z}^6/\mathbb{Z}^6$.*
2. *Compute the set*

$$\underline{\Theta_3} = \left\{ x \in \frac{1}{3}\mathbb{Z}^6/\mathbb{Z}^6 : N^t x = x \text{ and } \theta[x + D](\Omega) = 0 \right\}$$

   of cardinality 15.
3. *Let $T = \{t_1, t_2, t_3, t_4\} \subset \underline{\Theta_3}$ be a 4-element set that satisfies*
   i. $\sum_{i=1}^4 t = 0$,
   ii. $\{t_1, t_2, t_3\}$ are linearly independent over $\mathbb{Z}/3\mathbb{Z}$, and
   iii. $\{\sum_{i=1}^4 a_i t_i : (a_i)_i \in \mathbb{Z}^4_{\geq 0}, \sum_{i=1}^4 a_i \leq 3\} = \underline{\Theta_3}$.
4. *Compute*

$$\varepsilon_\lambda = \exp(6\pi i((\widetilde{t_3} - \widetilde{t_2})_1(\widetilde{t_1})_2 + (\widetilde{t_2} + 2\widetilde{t_3} - \widetilde{D})_1(2\widetilde{D} - 3(\widetilde{t_2} + \widetilde{t_3}))_2)),$$

$$\varepsilon_\mu = \exp(6\pi i((\widetilde{t_4} - \widetilde{t_2})_1(\widetilde{t_1})_2 + (\widetilde{t_2} + 2\widetilde{t_4} - \widetilde{D})_1(2\widetilde{D} - 3(\widetilde{t_2} + \widetilde{t_4}))_2)),$$

   and

$$\lambda = \varepsilon_\lambda \left(\frac{\theta[\widetilde{t_2} + 2\widetilde{t_3} - \widetilde{t_1} - \widetilde{D}](\Omega)}{\theta[2\widetilde{t_2} + \widetilde{t_3} - \widetilde{t_1} - \widetilde{D}](\Omega)} \right)^3,$$

$$\mu = \varepsilon_\mu \left(\frac{\theta[\widetilde{t_2} + 2\widetilde{t_4} - \widetilde{t_1} - \widetilde{D}](\Omega)}{\theta[2\widetilde{t_2} + \widetilde{t_4} - \widetilde{t_1} - \widetilde{D}](\Omega)} \right)^3.$$

5. *Return λ and μ.*

Remark 4 Algorithm 5 is a *mathematical* algorithm, but, because 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. For implementation details, we refer the reader to [32, Sect. 1.5].

Proof of Algorithm 5 Let $\Delta \in J(C)$ be the Riemann constant with respect to $P_\infty = (0 : 1 : 0)$ and let $\mathcal{B}$ be the set of affine branch points of C. By Proposition 2, the point Δ is the only one that satisfies $N[\underline{\Delta}] = \underline{\Delta}$ and is a 2-torsion point, that is, it satisfies $\underline{\Delta} \in \frac{1}{2}\mathbb{Z}^6/\mathbb{Z}^6$. We conclude $D = \underline{\Delta}$.

By Theorem 4, the sequence (t_1, t_2, t_3, t_4) is an ordering of either $\alpha(\mathcal{B})$ or $-\alpha(\mathcal{B})$. In the former case, the values λ, μ obtained in Step 4 are the x-coordinates of the affine branch

points different from (0, 0) and (0, 1). A quasi-periodicity argument similar to those in the proofs of Lemma 1 or Theorem 3 yields that in the latter case the same holds too. □

4 Computing maximal CM Picard curves

In this section, we present how to use Algorithm 5 to compute maximal CM Picard curves, that is, Picard curves such that their Jacobians have an endomorphism ring isomorphic to the maximal order of a sextic CM-field K.

Since ρ_* is an automorphism of order 3, the field K contains a primitive 3rd root of unity $\zeta_3 \in K$. In fact, the field K is determined by a totally real cubic field K_0 that satisfies $K = K_0(\zeta_3)$.

Van Wamelen [37] gives an algorithm that, given a CM-field K, lists all the isomorphism classes of period matrices of principally polarized abelian varieties with complex multiplication by $\mathcal{O}_K$. This method is based on the CM theory due to Shimura and Taniyama (see [29]) and we use the implementation in [33].

Applying said method to a sextic CM-field containing a primitive third root of unity $\zeta_3 \in K$, we obtain a list, say CM_K, of period matrices Ω corresponding to principally polarized abelian threefolds with CM by $\mathcal{O}_K$ with an order-3 automorphism associated to ζ_3. By Proposition 1, they are Jacobians of Picard curves. To then obtain the rational representation N of the order-3 automorphism is a matter of keeping track of the changes of basis throughout van Wamelen's method. We use the resulting list of pairs (Ω, N) as input for Algorithm 5.

When computing the Riemann theta constants in the algorithm implementation, we restrict the sum to a hypercube $[-B, B] \subset \mathbb{Z}^3$ for a certain value B that depends on the precision required and the minimum eigenvalue of the imaginary part of the period matrix. For efficiency, we would like the smallest eigenvalue of the imaginary part of Ω to be as big as possible, due to its role in the computation of the bound B. Since the isomorphism class of a principally polarized abelian variety only depends on the orbit of Ω under the action of $\mathrm{Sp}_{2g}(\mathbb{Z})$, this can be achieved by choosing a representative in a certain fundamental domain of $\mathbf{H}_g$. For this we use the implementation due to Kılıçer–Streng [10] of Algorithm 2 in Labrande–Thomé [15, Sect. 4.1] on our period matrix before applying Algorithm 5. For more details we refer the reader to [32, Sect. 1.5].

After numerically approximating the x-coordinates of the branch points of C with Algorithm 5, we obtain a polynomial

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

up to some precision, while the curve is actually isomorphic to $y^3 = h(x)$ for a certain polynomial h over a number field.

Given the quartic polynomial

$$p(x) = x^4 + g_2x^2 + g_3x + g_4 \text{ with } g_2, g_3 \neq 0$$

we define the *absolute invariants of* $p(x)$ as

$$j_1 = \frac{g_3^2}{g_2^3}, \qquad j_2 = \frac{g_4}{g_2^2}.$$

In order to find $h(x)$ from $f(x)$, we compute the absolute invariants of C by computing j_1 and j_2 for an isomorphic curve of the form $y^3 = x^4 + g_2x^2 + g_3x + g_4$. We use them to

obtain a numerical approximation of the class polynomials

$$H_{j_i}(x) = \prod_{\Omega \in \mathrm{CM}_K} (x - j_i(\Omega))$$

which have coefficients in the ring of integers of the moduli field of the curve. Once we recognize the exact polynomials we recover the pairs (j_1, j_2) by embedding the roots of H_{j_1}, H_{j_2} to $\mathbb{C}$ and comparing them with the numerical approximations obtained from f.

We then reconstruct an exact model $h(x)$ for each curve from the exact absolute invariants, obtaining

$$y^3 = h(x) = x^4 + j_1 x^2 + j_1^2 x + j_1^2 j_2.$$

Note that in order to be able to recognize the coefficients of H_{j_1} and H_{j_2} as algebraic numbers we have to compute λ and μ with enough precision.

Finally, one can use the algorithm in [5] to compute the endomorphism algebra of the Jacobian of the curve, confirming that the obtained curves have CM by the maximal order of the initial CM-field.

The list below contains models for all maximal CM Picard curves whose CM-field has class number $h \leq 4$. We get the sextic fields from [23, Table 3]. The authors of [13], working off an earlier version of this paper [16], give supporting evidence of the correctness of our examples. We have now confirmed the correctness of the models using the implementation of the algorithm in [5].

The examples (1)–(8), (13)–(14) include all the maximal CM Picard curves defined over $\mathbb{Q}$. The completeness of the list follows from Kılıçer [11, Theorem 4.3.1], as well as the fact that in examples (13)–(14) we also obtain three conjugate curves defined over K_0; see also [11, Table 3.1].

The examples (9)–(12) are defined over a cubic number field L such that the composition KL is the Hilbert class field of K. This follows from Shimura–Taniyama [28, Main Theorem 1], since we have $h_K = 3$ and the curves are not defined over $\mathbb{Q}$.

Remark 5 Examples (1)–(5) also appear in [14, Sect. 6.1]. Moreover, it is worth mentioning the existence of an algorithm to compute maximal CM plane quartics, see [12]. In particular, this algorithm can be used to compute maximal CM Picard curves, although less efficiently due to its more general scope. In fact, all the curves defined over $\mathbb{Q}$ that we give were independently found in [12].

Remark 6 It is also possible to use this algorithm to compute maximal CM Picard curves over finite fields, by obtaining first a rational model, and then reducing it modulo p. An alternative approach to this problem is given in [1] using the Chinese Reminder Theorem. In particular, see [1, Sect. 7] for an example using the CM-field in Example (2) and a comparison of the performance of both algorithms.

1. $y^3 = x^4 - x$, with K_0 defined by $\nu^3 - 3\nu - 1$.
2. $y^3 = x^4 - 2 \cdot 7^2 x^2 + 2^3 \cdot 7^2 x - 7^3$, with K_0 defined by $\nu^3 - \nu^2 - 2\nu + 1$.
3. $y^3 = x^4 - 2 \cdot 7^2 \cdot 13 x^2 + 2^3 \cdot 5 \cdot 13 \cdot 47 x - 5^2 \cdot 13^2 \cdot 31$, with K_0 defined by $\nu^3 - \nu^2 - 4\nu - 1$.
4. $y^3 = x^4 - 2 \cdot 7 \cdot 31 \cdot 73 x^2 + 2^{11} \cdot 31 \cdot 47 x - 7 \cdot 31^2 \cdot 11593$, with K_0 defined by $\nu^3 + \nu^2 - 10\nu - 8$.
5. $y^3 = x^4 - 2 \cdot 7 \cdot 43^2 \cdot 223 x^2 + 2^7 \cdot 11 \cdot 41 \cdot 43^2 \cdot 59 x - 11^2 \cdot 43^3 \cdot 419 \cdot 431$, with K_0 defined by $\nu^3 - \nu^2 - 14\nu - 8$.

6. $y^3 = x^4 - 2 \cdot 3^2 \cdot 5^2 \cdot 7^2 x^2 + 2^9 \cdot 7^2 \cdot 71\, x - 3^2 \cdot 5 \cdot 7^3 \cdot 2621$, with K_0 defined by $\nu^3 - 21\nu - 28$.
7. $y^3 = x^4 - 2^2 \cdot 3^2 \cdot 7^2 \cdot 37\, x^2 + 5 \cdot 7^2 \cdot 149 \cdot 257\, x - 2 \cdot 3^2 \cdot 5^2 \cdot 7^3 \cdot 2683$, with K_0 defined by $\nu^3 - 21\nu + 35$.
8. $y^3 = x^4 - 2 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13\, x^2 + 2^7 \cdot 11 \cdot 13 \cdot 59 \cdot 149\, x - 3^2 \cdot 5 \cdot 7 \cdot 13^2 \cdot 17 \cdot 17669$, with K_0 defined by $\nu^3 - 39\nu + 26$.
9. For K_0 defined by $\nu^3 - \nu^2 - 6\nu + 7$, and $w^3 = 19$, we obtain the three conjugate curves

$$y^3 = x^4 + (10w^2 - 2w - 70)\, x^2 + (96w^2 - 7w - 496)\, x + (235w^2 - 215w - 1101).$$

10. For K_0 defined by $\nu^3 - \nu^2 - 12\nu - 11$, and $w^3 = 37$, we obtain the three conjugate curves

$$\begin{aligned} y^3 = x^4 &+ (-2366w^2 + 490w + 24626)\, x^2 + (-257958w^2 - 686928w \\ &+ 5152928)\, x + (1226851w^2 - 56922233w + 176054907). \end{aligned}$$

11. For K_0 defined by $\nu^3 - 109\nu - 436$, and $w^3 = 109$, we obtain the three conjugate curves

$$\begin{aligned} y^3 = x^4 &+ \big(1115888872w^2 - 4007074778w - 6321528472\big)\, x^2 \\ &+ \big(-39141169182336w^2 + 294349080537984w - 512926132238464\big)\, x \\ &+ 816342009554519305w^2 - 9276324622428605048w \\ &+ 25684086855493144296. \end{aligned}$$

12. For K_0 defined by $\nu^3 - \nu^2 - 42\nu - 80$, and $w^3 = 127$, we obtain the three conjugate curves

$$\begin{aligned} y^3 = x^4 &+ \big(-92075757704w^2 + 319193013538w + 721950578888\big)\, x^2 \\ &+ \big(- 49404281036538240w^2 - 18281746350539328 0w + \\ &2167183294305193600\big)x + 21690511027003736433025w^2 - \\ &118803029086722205449800w + 49134882128483485627800. \end{aligned}$$

13. For K_0 defined by $\nu^3 - 61\nu - 183$, we have four curves. The first one is defined over $\mathbb{Q}$.

$$\begin{aligned} y^3 = x^4 &- 2 \cdot 3 \cdot 7 \cdot 61^2 \cdot 1289\, x^2 + 2^3 \cdot 3^7 \cdot 11 \cdot 41 \cdot 53 \cdot 61^2\, x \\ &- 3^2 \cdot 7 \cdot 11^2 \cdot 61^3 \cdot 419 \cdot 4663, \end{aligned}$$

and the three conjugates

$$\begin{aligned} y^3 = x^4 &+ \big(89264\nu^2 - 547484\nu - 4059720\big)\, x^2 + \big(- 29558196\nu^2 + 49526073\nu \\ &+ 772138494\big)x + 88325678\nu^2 - 16281030326\nu - 72348132021 \end{aligned}$$

14. For K_0 defined by $\nu^3 - \nu^2 - 22\nu - 5$, similarly one gets:

$$y^3 = x^4 + 2 \cdot 7 \cdot 67 \cdot 179\, x^2 + 2^3 \cdot 3^3 \cdot 5 \cdot 67 \cdot 137\, x + 5^2 \cdot 7 \cdot 67^2 \cdot 71 \cdot 89$$

and the three conjugates

$$\begin{aligned} y^3 = x^4 &+ \big(12222\nu^2 - 263088\nu - 1290744\big)\, x^2 + \big(- 19721880\nu^2 + 232016400\nu \\ &+ 1277237160\big)x + 11453819175\nu^2 - 62791404525\nu - 447679991475\,. \end{aligned}$$

Acknowledgements
The first two authors would like to thank Marco Streng and Christelle Vincent for useful discussions. They also thank the reviewers for their very helpful comments. The author of this appendix wishes to thank first and foremost Sorina Ionica, who verified the result independently with a proof that follows Takase's work more closely. She also thanks Marco Streng for first bringing to her attention the need to generalize Takase's work, and Anna Somoza for pointing out that her work on Picard curves could be adapted to obtain the correct sign. In addition, she thanks Jeroen Sijsling for performing computations confirming the correctness of the sign as computed in this appendix. Finally, she would like to extend her warmest thanks to the referees for their helpful suggestions which have made the writing stronger.

Author details
[1] Departament de Matemàtica Aplicada, Universitat Politècnica de Catalunya, Barcelona, Spain, [2] Institut de recherche mathématique de Rennes, Université de Rennes 1, Rennes, France, [3] Department of Mathematics and Statistics, University of Vermont, Burlington, VT, USA.

Appendix A (by Christelle Vincent)

Let C be a hyperelliptic curve of genus $g \geq 2$ defined over $\mathbb{C}$, and denote by $x\colon C \to \mathbb{P}^1$ a morphism of degree 2 from C to $\mathbb{P}^1$. Then x has $2g+2$ branch points which do not depend on the choice of x. We fix once and for all an ordering of these branch points, and denote them by $P_1, P_2, \ldots, P_{2g+2}$. Furthermore, for simplicity of notation in what follows we will denote

$$a_j = x(P_j). \tag{11}$$

The significance of these quantities is the following: If $x(P_j) \neq \infty$ for any j, then a model for C over $\mathbb{C}$ is given by

$$y^2 = \prod_{j=1}^{2g+2} (x - a_j), \tag{12}$$

whereas if there is k with $x(P_k) = \infty$, a model for C over $\mathbb{C}$ is given by

$$y^2 = \prod_{j \neq k} (x - a_j). \tag{13}$$

Our goal in this appendix is to show the following proposition, which generalizes a formula given by Takase [34, Theorem 1.1]. In the statement we use the notation $[a_l, a_m, a_k, a_\infty]$ for the cross-ratio

$$[a_l, a_m, a_k, a_\infty] = \frac{a_k - a_l}{a_k - a_m} \cdot \frac{a_\infty - a_m}{a_\infty - a_l}. \tag{14}$$

Proposition 3 *Let C be a hyperelliptic curve defined over $\mathbb{C}$, $x\colon C \to \mathbb{P}^1$ be a morphism of degree 2 with branch points $P_1, \ldots, P_{2g+2}$, and Ω be a (small) period matrix for $J(C)$, the Jacobian of C. Let k, l and m be distinct and belong to the set $\{1, 2, \ldots, 2g+2\}$, and fix P_∞ a distinguished branch point of x, $\infty \neq k, l, m$. Then, for $a_j = x(P_j)$ and η an eta-map associated to Ω and the base point P_∞ with corresponding U-set U_η, we have*

$$[a_l, a_m, a_k, a_\infty] = \exp(4\pi i(\eta_m - \eta_l)_1(\eta_k)_2) \left(\frac{\theta[\eta_{U_\eta \circ (V \cup \{k,l\})}](\Omega)\theta[\eta_{U_\eta \circ (W \cup \{k,l\})}](\Omega)}{\theta[\eta_{U_\eta \circ (V \cup \{k,m\})}](\Omega)\theta[\eta_{U_\eta \circ (W \cup \{k,m\})}](\Omega)} \right)^2, \tag{15}$$

where V and W are any sets that give a disjoint decomposition

$$\{1, 2, \ldots, 2g+1, 2g+2\} = V \cup W \cup \{k, l, m, \infty\}, \tag{16}$$

with $\#V = \#W = g - 1$.

As an immediate corollary, if we denote by λ_i for $i = 3, 4, \ldots, 2g+1$ the *Rosenhain invariants* of C, by which we mean the constants appearing in a choice of Rosenhain model

$$C : y^2 = x(x-1)\prod_{i=3}^{2g+1}(x-\lambda_i) \tag{17}$$

for the curve C, we obtain the following formula:

Corollary 2 *Let C be a hyperelliptic curve defined over $\mathbb{C}$, and fix a choice of Rosenhain model for C. Let P_∞ denote the point of C that is "at infinity" in the Rosenhain model of C, Ω be a choice of period matrix for $J(C)$, the Jacobian of C, and η be an eta-map associated to Ω and the base point P_∞ with corresponding U-set U_η. Then for $j \in \{3, 4, \ldots, 2g+1\}$, the Rosenhain invariants of C are given by the expression*

$$\lambda_j = \exp(4\pi i(\eta_j - \eta_2)_1(\eta_1)_2)\left(\frac{\theta[\eta_{U_\eta \circ (V\cup\{1,2\})}](\Omega)\theta[\eta_{U_\eta\circ(W\cup\{1,2\})}](\Omega)}{\theta[\eta_{U_\eta\circ(V\cup\{1,j\})}](\Omega)\theta[\eta_{U_\eta\circ(W\cup\{1,j\})}](\Omega)}\right)^2, \tag{18}$$

where V and W are two sets of cardinality $g-1$ such that

$$V \cup W = \{3, 4, \ldots, 2g+1\} \setminus \{j\}, \tag{19}$$

and the notation $\circ$ denotes the symmetric difference of two sets: For $S, T \subseteq \{1, 2, \ldots, 2g+2\}$, we have

$$S \circ T = (S \cup T) \setminus (S \cap T). \tag{20}$$

We now discuss briefly the history of this result and why this publication is necessary. In his work [34], Takase gives the formula presented in Proposition 3 in the special case where $a_\infty = \infty$, and only for certain choices of period matrix Ω for the Jacobian of C. These period matrices are those given by Mumford [20], using his "traditional" choice of symplectic basis for the first homology group of the Jacobian. This work was notably used by Weng in [39] to give models of hyperelliptic curves whose Jacobian has complex multiplication. Since our software [3] did not allow us to make the same choice of period matrix, for our computations we needed a more general result. Our earlier article [2, Theorem 4.5] claimed to give the formula for all period matrices (retaining the assumption that $a_\infty = \infty$), but unfortunately we found out later that there remained a mistake in the sign of λ_i, which had not been corrected to account for the general case.

The mistake was originally found by the authors of [12] as they worked to complete the list of curves of genus 3 defined over $\mathbb{Q}$ whose geometric endomorphism ring is a maximal order in a sextic field. For a specific period matrix in their list, the code provided in [3] did not yield a correct model for the hyperelliptic curve. Somoza, an author of this article, pointed out the "third root of unity" issue she had found and fixed in the Picard case, and after some trial and error we found that we had the same issue in the hyperelliptic case, with the exception that we were missing instead a second root of unity, or a sign.

The formula we finally give here is valid for all period matrices, and gives the correct value for λ_i. We note that the software available at [3] has been updated to be correct. As mentioned before, in addition to correcting the sign of λ_i, the formula given here is more general than that given by Takase, because here we do not assume that $a_\infty = \infty$, which explains why we compute the cross-ratio $[a_l, a_m, a_k, a_\infty]$ rather than the simpler quotient

$\frac{a_k-a_l}{a_k-a_m}$ as Takase does. As far as the proof is concerned, our proof does not follow that given by Takase, though it is possible to follow his method to arrive at the same result (though still with the assumption that $a_\infty = \infty$) as was done independently by Ionica in unpublished work. We note that this is not simpler or shorter than the proof we give here. The corrected formula has since been used in [6] to compute hyperelliptic class polynomials in genus 3.

A.1 Preliminaries

Following the technique used in the body of the paper, we will use Siegel's Theorem 2 applied to a suitable choice of function $\phi\colon C \to \mathbb{P}^1$ to obtain our results. To apply Siegel's Theorem, we first need a non-special divisor on C:

Lemma 2 *Let C be a hyperelliptic curve defined over $\mathbb{C}$, $x\colon C \to \mathbb{P}^1$ be a morphism of degree 2 from C to $\mathbb{P}^1$, and $P_1, \ldots P_{2g+2}$ be the branch points of x. Let $I \subset \{1, 2, \ldots, 2g+2\}$ be any subset of cardinality g. Then*

$$D = \sum_{i\in I} P_i \tag{21}$$

is a non-special divisor on C. In other words, any sum of g distinct branch points of x is a non-special divisor on C.

Proof We recall that a divisor D is non-special if $\ell(K - D) = 0$, where K is a canonical divisor on the curve C.

Fix P_∞ a branch point that is not in the support of D, and a model

$$s^2 = f(t) \tag{22}$$

for the hyperelliptic curve, where f is of degree $2g+1$ and P_∞ is the point at infinity. Then

$$\operatorname{div}(s) = \sum_{i\neq\infty} P_i - (2g+1)P_\infty, \quad \text{and} \quad \operatorname{val}_{P_\infty}(\operatorname{div}(t)) = -2. \tag{23}$$

We may then use

$$\operatorname{div}(dt) = \sum_{i\neq\infty} P_i - 3P_\infty \tag{24}$$

as a canonical divisor. Now suppose by way of contradiction that $\ell(\operatorname{div}(dt) - D) \geq 1$, so there exists a function f on C with

$$\operatorname{div}(f) \geq D - \operatorname{div}(dt). \tag{25}$$

Then certainly we have

$$\operatorname{div}(sf) \geq D - \operatorname{div}(dt) + \operatorname{div}(s) = \sum_{i\in I} P_i - (2g-2)P_\infty. \tag{26}$$

Now functions on C are rational functions in s and t, and functions on C with poles only at ∞ must be polynomials in s and t. Since $\operatorname{val}_{P_\infty}(s) = -(2g+1)$, the function sf is a polynomial in t, of degree less than or equal to $g-1$. However, such a polynomial cannot have g zeroes, one at each of the points in the support of D. From this contradiction we conclude that $\ell(K - D) = 0$ and D is non-special. □

Secondly, to connect our result to the established literature on hyperelliptic curves, we will need an eta-map associated to a period matrix Ω and a base point P_∞. We refer the

interested reader to either Poor's work [25] or our earlier work [2] for more details on these maps, and present here only the barest of facts necessary to keep this appendix readable. Let P_∞ be an arbitrary but fixed branched point of the degree 2 morphism $x\colon C \to \mathbb{P}^1$ fixed above, and recall that we have labeled the branch points of x to be $P_1, P_2, \ldots, P_{2g+2}$ (one of these is of course also labeled P_∞). As in the body of the paper, fix α an Abel-Jacobi map for C with base point P_∞. Then for $j \in \{1, 2, \ldots, 2g+2\}$, we write

$$\eta_j = \widetilde{P_j} \in \left\{0, \frac{1}{2}\right\}^{2g} \tag{27}$$

where $\widetilde{\cdot}$ is the map given in equation (6), and as in the body of the paper we denote the composition of the three maps by the last. The fact that the coordinates of η_j for each j are half-integers follows from the fact that $P_j - P_\infty$ is two-torsion in $J(C)$, see [20, Corollary 2.11]. Furthermore, for any subset $S \subseteq \{1, 2, \ldots, 2g+2\}$, we write

$$\eta_S = \sum_{j \in S} \eta_j. \tag{28}$$

Note that we use the same convention as in the body of the paper regarding summation of characteristics; see the paragraph immediately following Eq. (6) for a discussion of this convention. Because of this, it follows that

$$\eta_S = \widetilde{D_S}, \tag{29}$$

for

$$D_S = \sum_{j \in S} P_j. \tag{30}$$

We note that the dependence of the eta-map on the period matrix Ω happens explicitly via the map $\underline{\cdot}$.

Under these assumptions, there exists a subset $U_\eta \subseteq \{1, 2, \ldots, 2g+2\}$ such that

$$\eta_{U_\eta} \equiv \widetilde{\Delta} \pmod{\mathbb{Z}^{2g}} \tag{31}$$

where Δ is the Riemann constant associated to the choice of Abel-Jacobi map α that we made. We note that in fact there are several such sets; it is customary to choose one of even cardinality, and we have adopted in earlier work the convention that U_η should also contain ∞. This determines the set U_η uniquely. We call this set a *U-set corresponding to* η. Finally, one can show that if S is the complement of T inside of $\{1, 2, \ldots, 2g+2\}$, then

$$\eta_S = \eta_T. \tag{32}$$

A.2 Proof of the formula

With this notation and preliminaries in place, we may begin the proof. We begin with an auxiliary result:

Lemma 3 *Let P_j and P_∞ be two distinct branch points of the morphism x, α be an Abel–Jacobi map with base point P_∞, and γ be a path from P_∞ to P_j such that if $\widetilde{P_j} = \eta_j$ (where the map $\widetilde{\cdot}$ is as in Eq. (6)), then*

$$\int_\gamma \omega = \Omega(\eta_j)_1 + (\eta_j)_2. \tag{33}$$

In this case there exists a second path $\widetilde{\gamma}$ from P_∞ to P_j such that

$$\int_\gamma \omega + \int_{\widetilde{\gamma}} \omega = 0 \quad \text{in} \quad \mathbb{C}^g. \tag{34}$$

Proof We have that $\widetilde{P}_j = \eta_j \in \{0, \frac{1}{2}\}^{2g}$ (see Eq. (27) and the discussion surrounding it for this fact). From this it follows that if $L_\Omega = \Omega\mathbb{Z}^{2g} + \mathbb{Z}^{2g}$ is the lattice attached to the period matrix Ω, we have that

$$\int_\gamma \omega \in \frac{1}{2}L_\Omega, \tag{35}$$

or

$$2\int_\gamma \omega \in L_\Omega. \tag{36}$$

As a consequence, $\int_\gamma \omega$ and $-\int_\gamma \omega$ differ by an element of L_Ω, and since every L_Ω-translate of $\int_\gamma \omega$ is $\int_{\widetilde{\gamma}} \omega$ for some other path $\widetilde{\gamma}$ from P_∞ to P_j, it follows that there is $\widetilde{\gamma}$ from P_∞ to P_j such that

$$-\int_\gamma \omega = \int_{\widetilde{\gamma}} \omega. \tag{37}$$

□

We can now give the crucial part of the proof:

Lemma 4 *Let C be a hyperelliptic curve defined over $\mathbb{C}$, $x\colon C \to \mathbb{P}^1$ be a morphism of degree 2 with branch points $P_1, \ldots, P_{2g+2}$, and Ω be a period matrix for $J(C)$, the Jacobian of C. Let k, l and m be distinct and belong to the set $\{1, 2, \ldots, 2g+2\}$, and fix P_∞ a distinguished branch point of x, with $\infty \neq k, l, m$. Then, for $a_j = x(P_j)$, and η an eta-map associated to Ω and to the base point P_∞ with corresponding U-set U_η, we have*

$$[a_l, a_m, a_k, a_\infty] = \epsilon(k,l,m)\left(\frac{\theta[\eta_{S_l \circ U_\eta}](\Omega)\theta[\eta_{T_m \circ U_\eta}](\Omega)}{\theta[\eta_{S_m \circ U_\eta}](\Omega)\theta[\eta_{T_l \circ U_\eta}](\Omega)}\right)^2, \tag{38}$$

where

$$\epsilon(k,l,m) = \exp(4\pi i(\eta_m - \eta_l)_1(\eta_k)_2), \tag{39}$$

and for $j = l, m$, we have

$$T_j = V \cup \{j\}, \tag{40}$$

and

$$S_j = T_j \cup \{k\} = V \cup \{j,k\}, \tag{41}$$

where V is any set of cardinality $g-1$ such that $V \subset \{1, 2, \ldots, 2g+2\}$, $k, l, m, \infty \notin V$.

Proof To begin, fix $\infty \in \{1, 2, \ldots, 2g+2\}$, $\infty \neq k, l, m$, and let

$$x_k(P)\colon C \to \mathbb{P}^1 \tag{42}$$

be given by

$$x_k(P) = \frac{x(P) - x(P_k)}{x(P) - x(P_\infty)}. \tag{43}$$

Then the cross-ratio we seek is given by

$$[a_l, a_m, a_k, a_\infty] = \frac{x_k(P_l)}{x_k(P_m)}. \tag{44}$$

Next we fix a subset $V \subset \{1, 2, \ldots, 2g+2\}$ of cardinality $g-1$ such that $k, l, m, \infty \notin V$. (Note that this is possible since $2g-2 \geq g-1$ for $g \geq 1$.) Then the quantity which interests us is given by

$$[a_l, a_m, a_k, a_\infty] = \frac{x_k(P_l)\prod_{i\in V} x_k(P_i)}{x_k(P_m)\prod_{i\in V} x_k(P_i)}. \tag{45}$$

In addition, for $j = l, m$, the divisor

$$D_j = P_j + \sum_{i\in V} P_i \tag{46}$$

is a sum of g distinct branch points of x, and therefore an effective non-special divisor by Lemma 2.

Using the notation of Siegel's Theorem 2, we have

$$[a_l, a_m, a_k, a_\infty] = \frac{x_k(D_l)}{x_k(D_m)}, \tag{47}$$

and now wish to apply Corollary 1 to compute the quantities $x_k(D_l)$ and $x_k(D_m)$.

To do so, we note that

$$\operatorname{div}(x_k) = 2P_k - 2P_\infty \tag{48}$$

and that the supports of the divisors D_l and D_m avoid the support of $\operatorname{div}(x_k)$. As in the previous section, we denote by Δ the Riemann constant for the Abel-Jacobi map α of C with base point P_∞. In the application of Siegel's Theorem, we will choose the paths from P_∞ to P_∞ to be the trivial paths. As in Lemma 3, we fix a path γ from P_k to P_∞ such that

$$\int_\gamma \omega = \widetilde{P}_k = \Omega(\eta_k)_1 + (\eta_k)_2, \tag{49}$$

and denote by $\widetilde{\gamma}$ the path from P_k to P_∞ such that

$$\int_\gamma \omega + \int_{\widetilde{\gamma}} \omega = 0. \tag{50}$$

We have then that

$$\int_{\widetilde{\gamma}} \omega = -\widetilde{P}_k. \tag{51}$$

Finally, to simplify the notation, we further let

$$T_j = V \cup \{j\}, \tag{52}$$

for $j = l, m$, and replace the notation $\widetilde{P}_i$ with the notation η_i, using our convention for sums.

After these preliminaries, a straightforward application of Corollary 1 to $x_k(D_l)$ and $x_k(D_m)$ yields

$$[a_l, a_m, a_k, a_\infty] = \frac{x_k(D_l)}{x_k(D_m)} \tag{53}$$

$$= \left(\frac{\theta[\eta_{T_l} - \eta_k - \widetilde{\Delta}](\Omega)\theta[\eta_{T_l} + \eta_k - \widetilde{\Delta}](\Omega)}{\theta[\eta_{T_l} - \widetilde{\Delta}](\Omega)^2}\right) \div \left(\frac{\theta[\eta_{T_m} - \eta_k - \widetilde{\Delta}](\Omega)\theta[\eta_{T_m} + \eta_k - \widetilde{\Delta}](\Omega)}{\theta[\eta_{T_m} - \widetilde{\Delta}](\Omega)^2}\right). \tag{54}$$

To use the quasiperiodicity property of the theta function, we write

$$S_j = T_j \cup \{k\} = V \cup \{j, k\} \tag{55}$$

for $j = l, m$, so that we have

$$\eta_{T_j} + \eta_k = \eta_{S_j}, \tag{56}$$

since $k \notin T_j$. Then for $j = l, m$, the characteristics

$$\eta_{S_j} - \widetilde{\Delta} - 2\eta_k \quad \text{and} \quad \eta_{S_j} - \widetilde{\Delta} \tag{57}$$

differ by an integer vector, namely $-2\eta_k$.

Applying the quasi-periodicity property of the Riemann theta constant with characteristic given in equation (5), we obtain

$$\theta[\eta_{S_j} - \widetilde{\Delta} - 2\eta_k](\Omega) = \exp(4\pi i(\widetilde{\Delta} - \eta_{S_j})_1(\eta_k)_2)\theta[\eta_{S_j} - \widetilde{\Delta}](\Omega). \tag{58}$$

Therefore we have

$$\begin{aligned}[a_l, a_m, a_k, a_\infty] &= \left(\frac{\exp(4\pi i(\widetilde{\Delta} - \eta_{S_l})_1(\eta_k)_2)\theta[\eta_{S_l} - \widetilde{\Delta}](\Omega)^2}{\theta[\eta_{T_l} - \widetilde{\Delta}](\Omega)^2}\right) \\ &\quad \div \left(\frac{\exp(4\pi i(\widetilde{\Delta} - \eta_{S_m})_1(\eta_k)_2)\theta[\eta_{S_m} - \widetilde{\Delta}](\Omega)^2}{\theta[\eta_{T_m} - \widetilde{\Delta}](\Omega)^2}\right) \\ &= \exp(4\pi i(\eta_m - \eta_l)_1(\eta_k)_2)\left(\frac{\theta[\eta_{S_l} - \widetilde{\Delta}](\Omega)\theta[\eta_{T_m} - \widetilde{\Delta}](\Omega)}{\theta[\eta_{S_m} - \widetilde{\Delta}](\Omega)\theta[\eta_{T_l} - \widetilde{\Delta}](\Omega)}\right)^2. \end{aligned} \tag{59}$$

We finally handle the quantity $\widetilde{\Delta}$. First, we note that since $\widetilde{\Delta}$ is a vector with half-integer entries, $\widetilde{\Delta}$ and $-\widetilde{\Delta}$ differ by a vector with integer entries. Furthermore, as noted in Eq. (31), η_{U_η} and $\widetilde{\Delta}$ differ by a vector with integer entries. Therefore $-\widetilde{\Delta}$ and η_{U_η} differ by a vector with integer entries, say n:

$$-\widetilde{\Delta} = \eta_{U_\eta} + n. \tag{60}$$

Recalling our notation for the symmetric difference of two sets given in Eq. (20), we have that

$$\eta_{S_j} - \widetilde{\Delta} = \eta_{S_j} + \eta_{U_\eta} + n = \eta_{S_j \circ U_\eta} + 2\eta_{S_j \cap U_\eta} + n, \tag{61}$$

and

$$\eta_{T_j} - \widetilde{\Delta} = \eta_{T_j} + \eta_{U_\eta} + n = \eta_{T_j \circ U_\eta} + 2\eta_{T_j \cap U_\eta} + n, \tag{62}$$

for $j = l, m$. Once again we thus apply the quasi-periodicity property of the Riemann theta constant with characteristic to remove the integer vectors appearing in each characteristic. This time around, we note that since all of characteristics appearing above are half-integers, the sign $\exp(2\pi i x_1 m_2)$ from the transformation formula will be ± 1. Since all of the theta constants are now squared in the formula, the signs vanish and we finally obtain:

$$[a_l, a_m, a_k, a_\infty] = \exp(4\pi i(\eta_m - \eta_l)_1(\eta_k)_2)\left(\frac{\theta[\eta_{S_l \circ U_\eta}](\Omega)\theta[\eta_{T_m \circ U_\eta}](\Omega)}{\theta[\eta_{S_m \circ U_\eta}](\Omega)\theta[\eta_{T_l \circ U_\eta}](\Omega)}\right)^2. \tag{63}$$

This completes the proof. □

To finish the proof of Proposition 3, it remains now only to rewrite it so that the characteristics agree with Takase's and to verify that the signs agree. Indeed, the cross-ratio we compute here in this article agrees with the quotient computed by Takase, since in his article, Takase assumes that $a_\infty = \infty$. In that case, we have that

$$[a_l, a_m, a_k, a_\infty] = \frac{a_k - a_l}{a_k - a_m}. \tag{64}$$

We therefore turn our attention to the characteristics: Following Takase's notation, let W be the complement of $V \cup \{k, l, m, \infty\}$ in $\{1, 2, \ldots, 2g+2\}$. Then from the definitions it follows that

$$S_j = V \cup \{k, j\}, \tag{65}$$

for $j = l, m$. We also have that $T_l \cup \{\infty\}$ is the complement of $W \cup \{k, m\}$ in $\{1, 2, \ldots, 2g+2\}$, and $T_m \cup \{\infty\}$ is the complement of $W \cup \{k, l\}$. As a result,

$$((T_m \cup \{\infty\}) \circ U_\eta)^c = U_\eta \circ (W \cup \{k, l\}), \tag{66}$$

and

$$((T_l \cup \{\infty\}) \circ U_\eta)^c = U_\eta \circ (W \cup \{k, m\}). \tag{67}$$

Now by definition, we have that

$$\eta_\infty = 0, \tag{68}$$

since P_∞ is chosen to be the base point of the Abel-Jacobi map. Therefore we have

$$\eta_{(T_j \cup \{\infty\}) \circ U_\eta} = \eta_{T_j \circ U_\eta}, \tag{69}$$

for $j = l, m$. By Eq. (32), we have that

$$\eta_{(T_l \cup \{\infty\}) \circ U_\eta} = \eta_{U_\eta \circ (W \cup \{k,m\})} \tag{70}$$

and

$$\eta_{(T_m \cup \{\infty\}) \circ U_\eta} = \eta_{U_\eta \circ (W \cup \{k,l\})}. \tag{71}$$

Putting all of this together, we obtain

$$[a_l, a_m, a_k, a_\infty] = \exp(4\pi i(\eta_m - \eta_l)_1(\eta_k)_2) \left(\frac{\theta[\eta_{U_\eta \circ (V \cup \{k,l\})}](\Omega)\theta[\eta_{U_\eta \circ (W \cup \{k,l\})}](\Omega)}{\theta[\eta_{U_\eta \circ (V \cup \{k,m\})}](\Omega)\theta[\eta_{U_\eta \circ (W \cup \{k,m\})}](\Omega)} \right)^2. \tag{72}$$

To verify that the signs agree, we first begin by noting that the sign that we obtain is equal to

$$\exp(4\pi i(\eta_m - \eta_l)_1(\eta_k)_2) = \exp(4\pi i(\eta_l + \eta_m)_1(\eta_k)_2), \tag{73}$$

since both η_l and η_m have half-integer entries. We also note that before simplifying his expression, Takase has the sign written as

$$(-1)^{4(\eta_k)_1(\eta_l + \eta_m)_2} = \exp(4\pi i(\eta_k)_1(\eta_l + \eta_m)_2). \tag{74}$$

We prove that the two expressions are equal by proving that their product is 1. To do this, we define

$$e_2(\xi, \zeta) = \exp(4\pi i(\xi_1\zeta_2 - \xi_2\zeta_1)); \tag{75}$$

the significance of this function is that $e_2(\eta_i, \eta_j) = -1$ whenever $i \neq j$ (see [25, Lemma 1.4.13] or [2, Proposition 3.5]).

Then we have

$$\begin{aligned} &\exp(4\pi i(\eta_l + \eta_m)_1(\eta_k)_2)\exp(4\pi i(\eta_k)_1(\eta_l + \eta_m)_2) \\ &\qquad = \exp(4\pi i(\eta_l + \eta_m)_1(\eta_k)_2)\exp(-4\pi i(\eta_k)_1(\eta_l + \eta_m)_2) \\ &\qquad = e_2(\eta_l + \eta_m, \eta_k) \\ &\qquad = e_2(\eta_l, \eta_k)e_2(\eta_m, \eta_k) = 1 \end{aligned} \tag{76}$$

This completes the proof of Proposition 3.

We now end with the proof of Corollary 2:

Proof of Corollary 2 To obtain the values λ_i, we post-compose the degree 2 morphism $x\colon C \to \mathbb{P}^1$ with a linear fractional transformation of $\mathbb{P}^1$ sending $x(P_1)$ to 0, $x(P_2)$ to 1 and $x(P_{2g+2})$ to ∞. This new map is again a degree 2 morphism $C \to \mathbb{P}^1$, and so the result of Proposition 3 applies. In addition, we use that for this particular map, if $\lambda_j = x(P_j)$, then we have

$$\lambda_j = \frac{0 - \lambda_j}{0 - 1} = [\lambda_j, 1, 0, \infty] = \frac{x(P_1) - x(P_j)}{x(P_1) - x(P_2)}. \tag{77}$$

Therefore we fix $k = 1$, $l = 2$ and $m = j$ to obtain

$$\lambda_j = \exp(4\pi i(\eta_j - \eta_2)_1(\eta_1)_2)\left(\frac{\theta[\eta_{U_\eta \circ (V \cup \{1,2\})}](\Omega)\theta[\eta_{U_\eta \circ (W \cup \{1,2\})}](\Omega)}{\theta[\eta_{U_\eta \circ (V \cup \{1,j\})}](\Omega)\theta[\eta_{U_\eta \circ (W \cup \{1,j\})}](\Omega)}\right)^2. \tag{78}$$

□

Received: 5 June 2020 Accepted: 5 March 2021 Published online: 19 April 2021

References

1. Arora, S., Eisenträger, K.: Constructing Picard curves with complex multiplication using the Chinese remainder theorem. In: Proceedings of the Thirteenth Algorithmic Number Theory Symposium. Open Book Series, vol. 2, pp. 21–36. Mathematical Sciences Publishers, Berkeley (2019)
2. Balakrishnan, J.S., Ionica, S., Lauter, K., Vincent, C.: Constructing genus-3 hyperelliptic Jacobians with CM. *LMS J. Comput. Math.*, 19(suppl. A):283–300 (2016)
3. Balakrishnan, J.S., Ionica, S., Lauter, K., Vincent, C.: Genus 3. https://github.com/christellevincent/genus3 (2016)
4. Birkenhake, C., Lange, H.: Complex Abelian Varieties. Grundlehren der Mathematischen Wissenschaften, 2nd edn, vol. 302. Springer, Berlin (2004)
5. Costa, E., Mascot, N., Sijsling, J., Voight, J.: Rigorous computation of the endomorphism ring of a Jacobian. Math. Comput. **88**(317), 1303–1339 (2019). Implementation. https://github.com/edgarcosta/endomorphisms/
6. Dina, B.A., Ionica, S.: Genus 3 hyperelliptic curves with CM via Shimura reciprocity. Accepted for publication in the Proceedings of the ANTS 2020 Conference
7. Guàrdia, J.: On the Torelli problem and Jacobian Nullwerte in genus three. Mich. Math. J. **60**(1), 51–65 (2011)
8. Holzapfel, R.-P.: The Ball and Some Hilbert Problems. Lectures in Mathematics ETH Zürich. Birkhäuser Verlag, Basel. Appendix I by J. Estrada Sarlabous (1995)
9. Hoyt, W.L.: On products and algebraic families of Jacobian varieties. Ann. Math. **2**(77), 415–423 (1963)
10. Kılıçer, P., Streng, M.: LLL reduction of period matrices of genus 3 (2016). https://bitbucket.org/pkilicer/period-matrices-for-genus-3-cm-curves/
11. Kılıçer, P.: The CM class number one problem for curves. PhD thesis, Leiden University (2016)
12. Kilicer, P., Labrande, H., Lercier, R., Ritzenthaler, C., Sijsling, J., Streng, M.: Plane quartics over $\mathbb{Q}$ with complex multiplication. Acta Arith. **185**(2), 127–156 (2018)
13. Kılıçer, P., García, E.L., Streng, M.: Primes dividing invariants of CM Picard curves. Can. J. Math. **72**(2), 480–504 (2020)
14. Koike, K., Weng, A.: Construction of CM Picard curves. Math. Comput. **74**(249), 499–518 (2005)
15. Labrande, H., Thomé, E.: Computing theta functions in quasi-linear time in genus two and above. LMS J. Comput. Math. **19**(suppl. AsupplSuppl. A), 163–177 (2016)
16. Lario, J.-C., Somoza, A.: A note on Picard curves of CM-type. Unpublished (2016). arXiv:1611.02582v1
17. Lombardo, D., Lorenzo García, E., Ritzenthaler, C., Sijsling, J.: Decomposing Jacobians via Galois covers. Experimental Mathematics (2021, to appear)

18. Matsusaka, T.: On a characterization of a Jacobian variety. Mem. Coll. Sci. Univ. Kyoto Ser. A. Math. **32**, 1–19 (1959)
19. Milne, J.S.: Jacobian varieties. In: Cornell, G., Silverman, J.H. (eds.) Arithmetic Geometry, pp. 167–212. Springer, New York (1986)
20. Mumford, D.: Tata Lectures on Theta II. Progress in Mathematics, vol. 43. Birkhäuser Boston, Boston. Jacobian theta functions and differential equations. With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura (1984)
21. Mumford, D.: Tata Lectures on Theta. I. Modern Birkhäuser Classics. Birkhäuser Boston, Boston (2007). With the collaboration of C. Musili, M. Nori, E. Previato and M. Stillman, Reprint of the 1983 edition
22. Oort, F., Ueno, K.: Principally polarized abelian varieties of dimension two or three are Jacobian varieties. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 20:377–381, (1973)
23. Park, Y.-H., Kwon, S.-H.: Determination of all imaginary abelian sextic number fields with class number $\leq$ 11. Acta Arith. **82**(1), 27–43 (1997)
24. Picard, E.: Sur des fonctions de deux variables indépendantes analogues aux fonctions modulaires. Acta Math. **2**(1), 114–135 (1883)
25. Poor, C.: The hyperelliptic locus. Duke Math. J. **76**(3), 809–884 (1994)
26. Rosenhain, G., Weber, H., Witting, A.: Abhandlung über die functionen zweier variabler mit vier perioden: welche die inversen sind der ultra-elliptischen integrale erster klasse. Ostwalds Klassiker der exakten Wissenschaften. W, Engelmann (1895)
27. Shiga, H.: On the representation of the Picard modular function by θ constants. I, II. Publ. Res. Inst. Math. Sci. **24**(3), 311–360 (1988)
28. Shimura, G., Taniyama, Y.: Complex Multiplication of Abelian Varieties and Its Applications to Number Theory. Publications of the Mathematical Society of Japan, vol. 6. The Mathematical Society of Japan, Tokyo (1961)
29. Shimura, G., Taniyama, Y.: Complex Multiplication of Abelian Varieties and Its Applications to Number Theory. Publications of the Mathematical Society of Japan, Tokyo (1961)
30. Siegel, C.L.: Topics in Complex Function Theory, vol. II. Wiley Classics Library. Wiley, New York (1988)
31. Somoza, A.: Inverse Jacobian algorithms for Picard and CPQ curves (2018). https://github.com/anna-somoza/inverse-jacobian-alg/
32. Somoza, A.: Inverse Jacobian and related topics for certain superelliptic curves. PhD thesis, Leiden University and Universitat Politècnica de Catalunya (2019)
33. Streng, M.: REpository of complex multIPlication SageMath code. https://github.com/mstreng/recip
34. Takase, K.: A generalization of Rosenhain's normal form for hyperelliptic curves with an application. Proc. Jpn. Acad. Ser. A Math. Sci. **72**(7), 162–165 (1996)
35. The Sage Developers: SageMath, the Sage Mathematics Software System (Version 8.2). http://www.sagemath.org
36. Thomae, J.: Beitrag zur Bestimmung von $\vartheta(0, 0, \ldots 0)$ durch die Klassenmoduln algebraischer Functionen. J. Reine Angew. Math. **71**, 201–222 (1870)
37. van Wamelen, P.: Examples of genus two CM curves defined over the rationals. Math. Comput. **68**(225), 307–320 (1999)
38. Weber, H.: Theorie der abel'schen functionen vom geschlecht 3 (1876)
39. Weng, A.: A class of hyperelliptic CM-curves of genus three. J. Ramanujan Math. Soc. **16**(4), 339–372 (2001)

Publisher's Note