ISSN: 1017-060X (Print)

ISSN: 1735-8515 (Online)

Bulletin of the Iranian Mathematical Society

Vol. 43 (2017), No. 6, pp. 1989–2016

Title:

A descent method for explicit computations on curves

Author(s):

K. Filom

Published by the Iranian Mathematical Society
http://bims.ims.ir

Bull. Iranian Math. Soc.
Vol. 43 (2017), No. 6, pp. 1989–2016
Online ISSN: 1735-8515

A DESCENT METHOD FOR EXPLICIT COMPUTATIONS ON CURVES

K. FILOM

(Communicated by Rahim Zaare-Nahandi)

Abstract. It is shown that the knowledge of a surjective morphism $X \to Y$ of complex curves can be effectively used to make explicit calculations. The method is demonstrated by the calculation of $j(n\tau)$ (for some small n) in terms of $j(\tau)$ for the elliptic curve with period lattice $(1, \tau)$, the period matrix for the Jacobian of a family of genus-2 curves complementing the classic calculations of Bolza and explicit general formulae for branched covers of an elliptic curve with exactly one ramification point.
Keywords: Algebraic curves, branched covers, elliptic curves.
MSC(2010): Primary: 14Q05; Secondary: 14H30, 14H45, 14H52.

1. Introduction

In [8] it is shown how certain calculations on curves, for instance, construction of ramified coverings with prescribed ramifications, can be effectively implemented by invoking the geometry of a class of dessins d'enfants (*proper* dessins) and reducing the calculations to those on $\mathbb{CP}^1$. See also [11] and [12] for other approaches such as degeneration techniques or the theory of origamis. The essence of the method in [8] is that the additional structure of a proper dessin provides a morphism of the curve X to the complex line that allows one to reduce calculations on X to those on $\mathbb{CP}^1$ (*descent*) where one has standard coordinates. The principal purpose of this paper is to develop this idea in a more general algebraic framework and in effect free the technique from the geometry of dessins d'enfants. In this setting, one makes uses of surjective morphisms $X \to Y$ of curves and exploits symmetries inherent in the morphism (if they exist) to *descend* calculations to "simpler" curves, the calculations that usually amount to solving a system of polynomial equations. This makes the technique more flexible and wider applications become possible. The technique is best demonstrated through applications to several special cases where in

Article electronically published on 30 November, 2017.
Received: 13 July 2016, Accepted: 15 December 2016.

many of them $X \to Y$ is a morphism of hyperelliptic curves and the simpler morphism is the map induced on $\mathbb{CP}^1$.

In Section 2 we consider isogenies $f : E' \to E$ of elliptic curves of fixed degrees. A period $\tau \in \mathbb{H}$ (the upper half plane) of E and the parameter λ in a Legendre form $y^2 = x(x-1)(x-\lambda)$ of E are related by $j(\tau) = 256\frac{(\lambda^2-\lambda+1)^3}{(\lambda^2-\lambda)^2}$. Up to the action of $\mathrm{SL}_2(\mathbb{Z})$, there are only finitely many τ''s that can serve as a period for E'. On the other hand, finding the map $h : \mathbb{CP}^1 \to \mathbb{CP}^1$ obtained by factoring f through hyperelliptic involutions yields a Legendre representation and hence the j-invariant of E'. This shows that $j(\tau')$ belongs to a finite list of closed expressions in terms of λ. For example, when $D := \deg f \in \{2, 3\}$ and $\tau' = D\tau$, one will get expressions for $j(D\tau)$ in terms of λ. The rest of Section 2 concentrates on the case of self-isogenies $f : E \to E$ of degree D. The functions $h : \mathbb{CP}^1 \to \mathbb{CP}^1$ induced by these self-isogenies form a new class of meromorphic functions on $\mathbb{CP}^1$ with a very special ramification structure that will be introduced and studied carefully. They correspond to certain systems with $2D$ equations and $2D$ unknowns including λ. Solving such a system provides us with an explicit formula for $f : E \to E$ along with $j(E)$, cf. Examples 2.10, 2.11.

In the third section, we study covers of an elliptic curve E by genus-2 curves. The literature on Riemann surfaces of genus 2 is very extensive and the works of Bolza [2] or the seminal work of Igusa [6] on the moduli space of genus-2 curves are relevant to our discussion. In fact, as we shall see in Section 3 and Section 5, the geometric point of view of looking at curves as ramified covers of $\mathbb{CP}^1$ allows one to give a simple description of some moduli and Hurwitz spaces by the invariant theory of finite groups.

The group action that arises in constructing the moduli space of genus-2 Riemann surfaces is the action outlined in (3.1) of $\langle \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5 \rangle \cong \mathrm{S}_6$ on certain domain $\mathbb{D}$ in $\mathbb{C}^3$. Finding invariants under this action amounts to classifying invariants of genus-2 Riemann surfaces or equivalently, binary sextics over $\mathbb{C}$. This has been accomplished completely over an algebraically closed field of arbitrary characteristic in the paper [6] by Igusa. This paper is hard to read as Igusa tries to formulate invariants that work for all characteristics simultaneously, especially for characteristic 2 where the Rosenhain normal form fails. If we exclude characteristics $2, 3, 5$, the paper [9] presents a simpler purely algebraic treatment of Igusa's results based on the machinery of invariant theory developed by Hilbert. The author has tried to compute generators for this invariant subfield over $\mathbb{C}$ by simpler methods. In fact, this is not hard to achieve as long as one is concerned with the action of the subgroup $\langle \sigma_1, \sigma_2, \sigma_3, \sigma_4 \rangle \cong \mathrm{S}_5$. This might lead to a simpler calculation of three desired invariants of the Rosenhain form once one figures out how to complete the picture by entering the last generator σ_5. See the Remark 3.1 for more details.

The existence of a morphism $C \to E$ puts constraints on the periods of

the Jacobian $J(C)$ of the genus-2 curve C. Using our technique, we obtain a normalized period matrix (as an element of the Siegel upper half plane of degree 2) of a genus-2 curve C which admits degree-2 morphisms onto two non-isomorphic elliptic curves E_1, E_2 in terms of periods $\tau_1, \tau_2 \in \mathbb{H}$ of those elliptic curves. This clarifies the meaning of an unspecified parameter in the work of Bolza and the corresponding entry in the table in [1, p. 340].

In Section 4 we address the main problem of [11], i.e., constructing coverings of an elliptic curve with a unique ramification point.

We finish with a short section on genus-3 curves to illustrate that, even in non-hyperelliptic cases, one may *descend* the important computational problem of writing down an equation of a branched cover to solving an appropriate system of polynomial equations.

2. **Isogenies of elliptic curves**

Consider an elliptic curve E in the Legendre form

$$E_\lambda = \left\{y^2 = x(x-1)(x-\lambda)\right\} (\lambda \in \mathbb{C} - \{0,1\})$$

and let $\tau \in \mathbb{H}$, where $\mathbb{H}$ denotes the upper half plane, be one of its periods: $E \cong \frac{\mathbb{C}}{\mathbb{Z}+\mathbb{Z}\tau}$. Recall that two numbers give rise to Legendre representations of the same elliptic curve if and only if they are equivalent under the following action of the symmetric group S_3 on $\mathbb{C} - \{0,1\}$:

$$\lambda \mapsto \lambda, \frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}, \frac{\lambda-1}{\lambda}. \tag{2.1}$$

Relative to the Legendre representation, j-function can be described as $\lambda \mapsto 256\frac{(\lambda^2-\lambda+1)^3}{(\lambda^2-\lambda)^2}$ which up to scaling is the unique rational function invariant under this action and parametrizes the moduli space $\mathcal{M}_{1,1} = (\mathbb{C} - \{0,1\})/\mathrm{S}_3$ of elliptic curves. On the other hand, it is also a modular function for $\Gamma(1)$ whose q-expansion, $q = \mathrm{e}^{2\pi \mathrm{i}\tau}$, is:

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + 20245856256q^4 + \cdots .$$

Let $f : E' \to E$ be a degree-D isogeny of elliptic curves. Fixing D and with the prior knowledge of the Legendre form $y^2 = x(x-1)(x-\lambda)$ and a period $\tau \in \mathbb{H}$ for E, our goal is to compute a Legendre representation $y^2 = x(x-1)(x-\lambda')$ for E'. Periods τ' of E' are exactly images of τ under integer 2×2 matrices of determinant D in the action of $\mathrm{GL}_2^+(\mathbb{R})$ on the upper half plane. This set, i.e. $\left\{\frac{a\tau+b}{c\tau+d} \mid a,b,c,d \in \mathbb{Z}, ad-bc = D\right\}$, decomposes as union of finitely many $\mathrm{SL}_2(\mathbb{Z})$-orbits and provides us with a finite list of points (denoted by τ') in the upper half plane whose corresponding Legendre form representations (that is λ') is going to be investigated by studying certain meromorphic function $h : \mathbb{CP}^1 \to \mathbb{CP}^1$ of degree D.

The degree-D homomorphism $f : E' \to E$ is simply a degree-D unbranched

cover of the underlying compact Riemann surfaces of genus 1 which respects the hyperelliptic involutions and maps the identity to identity. In each of E, E' one may assume that the identity element is the point at infinity where $x, y \to \infty$. This, together with the fact that f respects the hyperelliptic involution $(x, y) \mapsto (x, -y)$, implies that $f : E' = \{y^2 = x(x-1)(x-\lambda')\} \to E = \{y^2 = x(x-1)(x-\lambda)\}$ can be written as $(x, y) \mapsto \big(h(x), g(x)y\big)$ where $h, g \in \mathbb{C}(x)$ with h the meromorphic function of the same degree D induced by f on $\mathbb{CP}^1$. Note that $h(\infty) = \infty$. Considering ramifications of maps in the commutative diagram:

$$(\star) \qquad \begin{array}{ccc} E' & \xrightarrow{f} & E \\ {\scriptstyle (x,y)\mapsto x}\downarrow & & \downarrow{\scriptstyle (x,y)\mapsto x} \\ \mathbb{CP}^1 & \xrightarrow{h} & \mathbb{CP}^1 \end{array}$$

we deduce the following constraints on h and hence on λ':

- $h(\infty) = \infty$;
- the multiplicity of h at each ramification point is two and hence there are $2D-2$ ramification points according to the Riemann-Hurwitz formula;
- the branch values of h belong to the set $\{0, 1, \lambda, \infty\}$;
- the multiplicity of h at points $0, 1, \lambda', \infty$ is one and its value at any of them lies in $\{0, 1, \lambda, \infty\}$.

The plan is to start with D, τ, λ, form a finite list of $\mathrm{SL}_2(\mathbb{Z})$-orbits of τ''s by exhibiting representatives, determine available λ''s –at which the value of $j : \mathbb{C} - \{0, 1\} \to \mathbb{C}$ may be easily calculated –by studying the preceding functions h and finally use q-expansion to find out a τ' from our first list corresponds to which of the values $j(\lambda')$ just obtained.

It should be mentioned that since the map f from the elliptic curve $y^2 = x(x-1)(x-\lambda')$ to $y^2 = x(x-1)(x-\lambda)$ is given by $(x, y) \mapsto \big(h(x), g(x)y\big)$, in the field $\mathbb{C}(x)$ the element $\frac{h(x)(h(x)-1)(h(x)-\lambda)}{x(x-1)(x-\lambda')}$ is a perfect square, namely $g(x)^2$. Conversely, any h with this property determines an isogeny f: take $g(x) \in \mathbb{C}(x)$ to be a square root of the above function and then $f : (x, y) \mapsto \big(h(x), g(x)y\big)$ is a well-defined isogeny $E' \to E$.

Let us apply this to $D = 2$. Any integer 2×2 matrix of determinant 2 may be written as an element of $\mathrm{SL}_2(\mathbb{Z})$ multiplied from right by one of matrices $\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$, $\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$ or $\begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}$. Consequently, having $\tau \in \mathbb{H}$ and a corresponding $\lambda \in \mathbb{C} - \{0, 1\}$ in hand, we are going to derive values of $j : \mathbb{H} \to \mathbb{C}$ at points $2\tau, \frac{\tau}{2}, \frac{\tau+1}{2}$ from its value at τ. From these constraints, the degree-2 map $h : \mathbb{CP}^1 \to \mathbb{CP}^1$ has two ramification points each of multiplicity two where ramification values are two members of $\{0, 1, \lambda\}$ and moreover, the fiber over the

remaining value in this set consists of two points in $\{0,1,\lambda'\}$. The point left in this set is mapped to ∞. It must be mentioned that these conditions on $h(x)$ are also sufficient in the sense that they guarantee $\frac{h(x)(h(x)-1)(h(x)-\lambda)}{x(x-1)(x-\lambda')}\in\mathbb{C}(x)$ is a perfect square so any such a $h(x)$ fits in the bottom of a diagram like $(\star)$ whose top row is a degree-2 isogeny f from $E'=\left\{y^2=x(x-1)(x-\lambda')\right\}$ to $E=\left\{y^2=x(x-1)(x-\lambda)\right\}$. Substituting λ,λ' with the other points in their S_3-orbit via combining h from the left with one of Möbius transformations $x\mapsto 1-x$ or $1-\frac{x}{\lambda}$ and from the right with one of Möbius transformations $x\mapsto 1-x$ or $\lambda'(1-x)$ (which all fix ∞), without any loss of generality we may concentrate only on the case where under h: $\lambda',\infty\mapsto\infty$, $0,1\mapsto 0$ and the set of branch values is $\{1,\lambda\}$. Note that $\tilde{\lambda}\mapsto 1-\tilde{\lambda}$ and $\tilde{\lambda}\mapsto\frac{1}{\tilde{\lambda}}$ generate the action of the symmetric group S_3 on $\mathbb{C}-\{0,1\}$ that remains $j:\mathbb{C}-\{0,1\}\to\mathbb{C}$ –in which we are interested –invariant, cf. (2.1). Hence, $h(x)=\frac{kx(x-1)}{x-\lambda'}$ and since $1,\lambda$ are branch values, discriminant of the quadratic polynomials $kx(x-1)-(x-\lambda')$ and $kx(x-1)-\lambda(x-\lambda')$ must vanish. This leads to a very simple system of equations with unknowns k,λ' whose solutions are $k=\sqrt{\lambda},\lambda'=\frac{1}{4}\left(\sqrt{\lambda}+\frac{1}{\sqrt{\lambda}}+2\right)$. Thus, the j-invariant of E' is in the form of:

$$256\frac{\left[\left(\frac{1}{4}\left(\sqrt{\lambda}+\frac{1}{\sqrt{\lambda}}+2\right)\right)^2-\frac{1}{4}\left(\sqrt{\lambda}+\frac{1}{\sqrt{\lambda}}+2\right)+1\right]^3}{\left[\left(\frac{1}{4}\left(\sqrt{\lambda}+\frac{1}{\sqrt{\lambda}}+2\right)\right)^2-\frac{1}{4}\left(\sqrt{\lambda}+\frac{1}{\sqrt{\lambda}}+2\right)\right]^2}=16\frac{\left(\lambda+\frac{1}{\lambda}+14\right)^3}{\left(\lambda+\frac{1}{\lambda}-2\right)^2},$$

where λ varies in its S_3 orbit $\left\{\lambda,1-\lambda,\frac{1}{\lambda},\frac{1}{1-\lambda},\frac{\lambda-1}{\lambda},\frac{\lambda}{\lambda-1}\right\}$. Consequently:

Theorem 2.1. *Let $\tau\in\mathbb{H}$ and $\lambda\in\mathbb{C}-\{0,1\}$ be such that $j(\tau)=256\frac{(\lambda^2-\lambda+1)^3}{(\lambda^2-\lambda)^2}$. Then:*

$$\left\{j\left(2\tau\right),j\left(\frac{\tau}{2}\right),j\left(\frac{\tau+1}{2}\right)\right\}=\left\{16\frac{\left(u+\frac{1}{u}+14\right)^3}{\left(u+\frac{1}{u}-2\right)^2}\middle|u\in\left\{\lambda,1-\lambda,\frac{\lambda-1}{\lambda}\right\}\right\}.$$

The same procedure can be repeated when the degree D of rows in $(\star)$ is 3 although expressions are much more tedious. First, note that any 2×2 integer matrix of determinant 3 has a description as a product of an element of $\mathrm{SL}_2(\mathbb{Z})$ by one of matrices $\begin{bmatrix}3&0\\0&1\end{bmatrix}$, $\begin{bmatrix}1&0\\0&3\end{bmatrix}$, $\begin{bmatrix}1&1\\0&3\end{bmatrix}$ or $\begin{bmatrix}1&-1\\0&3\end{bmatrix}$. So we hope to recover some numbers among $j(3\tau),j\left(\frac{\tau}{3}\right),j\left(\frac{\tau+1}{3}\right),j\left(\frac{\tau-1}{3}\right)$ with the assumption that τ is specified along with $j(\tau)$ in the form of $j(\lambda)=256\frac{(\lambda^2-\lambda+1)^3}{(\lambda^2-\lambda)^2}$. Secondly, we are going to accomplish this via studying certain types of meromorphic functions of degree 3. These meromorphic functions $h:\mathbb{CP}^1\to\mathbb{CP}^1$ obey the constraints explained before in the case of $D=2$. Again, by composing with suitable Möbius maps, without changing the S_3 orbits of λ or λ', we may

assume that $0 \mapsto 0, 1 \mapsto 1, \lambda' \mapsto \lambda, \infty \mapsto \infty$. Therefore, branch values of h are exactly $0, 1, \lambda, \infty$, where over each h precisely has one ramification point of multiplicity two and one point of multiplicity one. These non-critical points are $0, 1, \lambda', \infty$, respectively. Once more, these constraints are also sufficient, that is any such a function h results in a degree-3 isogeny of elliptic curves making $(\star)$ commutative. Hence, in order to get the value of j-invariant at one of the four points of the upper half plane associated with τ above, we will try to exhibit such a function in terms of λ. Since $h(0) = 0$, $h(\infty) = \infty$ and $0, \infty$ are ramification values: $h(x) = \frac{xP(x)}{Q(x)}$ where $P(x)$ and $Q(x)$ are quadratic polynomials of discriminant zero. Equalities $h(1) = 1, h(\lambda') = \lambda$ yield $Q(1) = P(1), Q(\lambda') = \frac{\lambda'}{\lambda}P(\lambda')$. So after writing them in terms of the basis $\left\{(x-1)^2, (x-1)(x-\lambda'), (x-\lambda')^2\right\}$ for the space of polynomials of degree less than 3, we conclude that for some suitable $t \in \mathbb{C} - \{0, -1\}$:

$$h(x) = \frac{x\big((x-1)^2 + 2t(x-1)(x-\lambda') + t^2(x-\lambda')^2\big)}{\frac{\lambda'}{\lambda}(x-1)^2 + 2t\sqrt{\frac{\lambda'}{\lambda}}(x-1)(x-\lambda') + t^2(x-\lambda')^2}. \tag{2.2}$$

The only condition left is that $1, \lambda$ must be critical values of $h(x)$, i.e. numerators of $h(x) - 1$ and $h(x) - \lambda$ have multiple roots, the polynomials which may be written as:

$$\begin{cases} (x-1)\left[(x-1)(x-\frac{\lambda'}{\lambda}) + 2t\left(x - \sqrt{\frac{\lambda'}{\lambda}}\right)(x-\lambda') + t^2(x-\lambda')^2)\right], \\ (x-\lambda')\left[(x-1)^2 + 2t\left(x - \sqrt{\lambda\lambda'}\right)(x-1) + t^2(x-\lambda)(x-\lambda')\right]. \end{cases}$$

Vanishing of discriminants of quadratic polynomials that appeared in brackets yields a system with unknowns t, λ':

$$\begin{cases} \left(1 + \frac{\lambda'}{\lambda} + 2t\left(\sqrt{\frac{\lambda'}{\lambda}} + \lambda'\right) + 2t^2\lambda'\right)^2 = 4(t+1)^2\left(\sqrt{\frac{\lambda'}{\lambda}} + t\lambda'\right)^2, \\ \left(2 + 2t\left(\sqrt{\lambda\lambda'} + 1\right) + t^2(\lambda + \lambda')\right)^2 = 4(t+1)^2\left(1 + t\sqrt{\lambda\lambda'}\right)^2. \end{cases}$$

We are looking for solutions in terms of λ. Assuming $\lambda \neq \lambda'$, the second equation gives us the identity $4 + 4t\left(\sqrt{\lambda\lambda'} + 1\right) + t^2(\sqrt{\lambda} + \sqrt{\lambda'})^2 = 0$ while with dividing the first equation by the second one, we have:

$$\frac{1 + \frac{\lambda'}{\lambda} + 2t\left(\sqrt{\frac{\lambda'}{\lambda}} + \lambda'\right) + 2t^2\lambda'}{2 + 2t\left(\sqrt{\lambda\lambda'} + 1\right) + t^2(\lambda + \lambda')} = \pm\frac{\sqrt{\lambda'}}{\sqrt{\lambda}}.$$

Choosing plus sign, this identity reduces to $t^2=\frac{1}{\sqrt{\lambda\lambda'}}$. Combining it with $4+4t\left(\sqrt{\lambda\lambda'}+1\right)+t^2\left(\sqrt{\lambda}+\sqrt{\lambda'}\right)^2=0$ that appeared before gives us:

$$\left(\lambda+\lambda'+6\sqrt{\lambda\lambda'}\right)^2=16\left(1+\sqrt{\lambda\lambda'}\right)^2\sqrt{\lambda\lambda'}.$$

Hence, fixing λ, for any λ' satisfying this equation and t given by $t^2=\frac{1}{\sqrt{\lambda\lambda'}}$, $h(x)$ in (2.2) will be a degree-3 meromorphic function on $\mathbb{CP}^1$ with the desired properties. This is reflected in:

Theorem 2.2. *Let $\tau\in\mathbb{H}$ and $\lambda\in\mathbb{C}-\{0,1\}$ be such that $j(\tau)=256\frac{(\lambda^2-\lambda+1)^3}{(\lambda^2-\lambda)^2}$. If $\lambda'\in\mathbb{C}-\{0,1\}$ satisfies*

$$\left(\lambda+\lambda'+6\sqrt{\lambda\lambda'}\right)^2=16\left(1+\sqrt{\lambda\lambda'}\right)^2\sqrt{\lambda\lambda'},$$

then $256\frac{(\lambda'^2-\lambda'+1)^3}{(\lambda'^2-\lambda')^2}$ belongs to the set $\left\{j(3\tau),j\left(\frac{\tau}{3}\right),j\left(\frac{\tau+1}{3}\right),j\left(\frac{\tau-1}{3}\right)\right\}$.

Note that Theorems 2.1, 2.2 essentially present explicit solutions of the modular equations for $\Gamma_0(2)$, $\Gamma_0(3)$ which are obtained by geometric methods. These explicit solutions may be used to derive modular equations of higher degrees. For instance, Theorem 2.1 implies that the modular equation for $\Gamma_0(4)$, i.e. the algebraic dependence relation between $j(2\tau),j\left(\frac{\tau}{2}\right)$, is just the equation that elements $16\frac{\left(\lambda+\frac{1}{\lambda}+14\right)^3}{\left(\lambda+\frac{1}{\lambda}-2\right)^2},16\frac{\left(1-\lambda+\frac{1}{1-\lambda}+14\right)^3}{\left(1-\lambda+\frac{1}{1-\lambda}-2\right)^2}$ of $\mathbb{C}(\lambda)$ satisfy which may be calculated easily with aid of a computer algebra package.

Example 2.3. Suppose $\lambda=-1$ which corresponds to the square lattice, i.e. $\tau=\mathrm{i}$, and elliptic curve $y^2=x^3-x$. Employing Theorem 2.2, our objective is to derive closed forms for:

$$j(3\mathrm{i})\approx \mathrm{e}^{6\pi}+744+196884\mathrm{e}^{-6\pi}\approx 153553679.3967,$$

$$j\left(\frac{\pm1+\mathrm{i}}{3}\right)\approx -\mathrm{e}^{3\pi}+744-196884\mathrm{e}^{-3\pi}+21493760\mathrm{e}^{-6\pi}\approx -11663.3962.$$

The complex number $\sqrt{\lambda'}$ should be a root of

$$(x^2+6\mathrm{i}x-1)^2-16\mathrm{i}x(1+\mathrm{i}x)^2=x^4+28\mathrm{i}x^3-6x^2-28\mathrm{i}x+1.$$

Finding roots with help of some computer software implies that our choices for $\sqrt{\lambda'}$ are $-\mathrm{i}\left(2+\sqrt{3}\right)\left(\sqrt{2}\pm\sqrt[4]{3}\right)^2$ and $-\mathrm{i}\left(2-\sqrt{3}\right)\left(\sqrt{2}\pm\mathrm{i}\sqrt[4]{3}\right)^2$ which give us:

$$\lambda'=-\left(2+\sqrt{3}\right)^2\left(\sqrt{2}\pm\sqrt[4]{3}\right)^4\quad\text{or}\quad\lambda'=-\left(2-\sqrt{3}\right)^2\left(\sqrt{2}\pm\mathrm{i}\sqrt[4]{3}\right)^4.$$

In each of them, numbers are reciprocal. So let us only concentrate on $\lambda'=-\left(2+\sqrt{3}\right)^2\left(\sqrt{2}+\sqrt[4]{3}\right)^4$ and $\lambda'=-\left(2-\sqrt{3}\right)^2\left(\sqrt{2}-\mathrm{i}\sqrt[4]{3}\right)^4$. They satisfy quadratic equations $\lambda'^2+2\left(193+112\sqrt{3}\right)\lambda'+1=0$ and λ'^2+

$2\left(193-112\sqrt{3}\right)\lambda'+1=0$ respectively, the fact that extremely simplifies evaluating $j(\lambda)=256\frac{(\lambda^2-\lambda+1)^3}{(\lambda^2-\lambda)^2}$ at them (see the footnote to Example 2.10):

$$\begin{cases} j(\lambda)\big|_{-\left(2+\sqrt{3}\right)^2\left(\sqrt{2}+\sqrt[4]{3}\right)^4}=64\left(387+224\sqrt{3}\right)^3\left(97-56\sqrt{3}\right)\approx 153553679.3967,\\ j(\lambda)\big|_{-\left(2-\sqrt{3}\right)^2\left(\sqrt{2}+\mathrm{i}\sqrt[4]{3}\right)^4}=64\left(387-224\sqrt{3}\right)^3\left(97+56\sqrt{3}\right)\approx -11663.3967. \end{cases}$$

Comparing with the approximations obtained from q-expansion before, we deduce that $j(3\mathrm{i})=64\left(387+224\sqrt{3}\right)^3\left(97-56\sqrt{3}\right)$ and $j\left(\frac{\pm 1+\mathrm{i}}{3}\right)$ is its Galois conjugate $64\left(387-224\sqrt{3}\right)^3\left(97+56\sqrt{3}\right)$.

Now, we begin studying self-isogenies $f:E\to E$ where $E=\frac{\mathbb{C}}{\mathbb{Z}+\mathbb{Z}\tau}$ for a $\tau\in\mathbb{H}$. The elliptic curve E has complex multiplication, or equivalently τ satisfies a quadratic equation over the rationals, if and only if there exists such a f which is not an obvious multiplication map $P\mapsto nP\,(n\in\mathbb{Z})$. In particular, this is the case when D is not a perfect square. This is the content of the following easy proposition whose proof is left to the reader.

Proposition 2.4. *With the hypothesis just mentioned, τ and f should be in the form of $\tau=\frac{1}{2b}\left(u+\sqrt{4D-a^2}\mathrm{i}\right)$ $\quad[z]\mapsto\left[\left(\frac{a-u}{2}+b\tau\right)z\right]$ where u,b,a are integers with $\mid a\mid<2\sqrt{D}$ and $4b|u^2+4D-a^2$.*

Next, we switch to our geometric point of view. Let $y^2=x(x-1)(x-\lambda)$ be a Legendre representation of E. Again, since this self-isogeny respects the hyperelliptic involution we can decompose $f:\left\{y^2=x(x-1)(x-\lambda)\right\}\to\left\{y^2=x(x-1)(x-\lambda)\right\}$ as $(x,y)\mapsto(h(x),yg(x))$ and form a commutative diagram similar to $(\star)$:

$(\star\star)$

$$\begin{array}{ccc} E & \xrightarrow{f} & E \\ {\scriptstyle (x,y)\mapsto x}\downarrow & & \downarrow{\scriptstyle (x,y)\mapsto x} \\ \mathbb{CP}^1 & \xrightarrow{h} & \mathbb{CP}^1. \end{array}$$

There are analogous constraints as before but with λ' replaced with λ:

- $h(\infty)=\infty$;
- the function h has $2D-2$ ramification points each with multiplicity two;
- the branch values of h belong to the set $\{0,1,\lambda,\infty\}$;
- the multiplicity of h at each of points $0,1,\lambda,\infty$ is one and its value at any of them lies in $\{0,1,\lambda,\infty\}$.

Suppose $D>2$ is a non-square and the degree-D meromorphic function h satisfies our constraints. It has $2D-2$ ramification points each with multiplicity two, and at most four ramification values, namely $0,1,\lambda,\infty$, with at most $\lfloor\frac{D}{2}\rfloor$ ramification points above any of them. We conclude that all of them are branch values as otherwise there will be at most $3\lfloor\frac{D}{2}\rfloor$ ramification points. But

$3\lfloor\frac{D}{2}\rfloor < 2D-2$ for any $D \in \mathbb{N}$ except for $D = 1, 2, 4$ which were excluded. Thus, branch values of $h : \mathbb{CP}^1 \to \mathbb{CP}^1$ are precisely $0, 1, \lambda, \infty$.

When D is odd, $4\lfloor\frac{D}{2}\rfloor = 2D-2$ and therefore over each branch value $0, 1, \lambda$ or ∞, h has one non-critical and $\frac{D-1}{2}$ critical points of multiplicity two. But points $0, 1, \lambda$ and $\infty \in h^{-1}(\infty)$ are non-critical points in critical fibers. Hence, from the previous discussion, there is a permutation σ of $\{0, 1, \lambda\}$ such that $h(x) = \sigma(x) \quad \forall x \in \{0, 1, \lambda\}$. We have three different situations: σ is either identity, a transposition or a three cycle. Because of the aforementioned symmetries between $0, 1, \lambda$, two former cases –without any change in the value of $j(\lambda)$ –reduce to $\sigma(0) = 0, \sigma(1) = \lambda, \sigma(\lambda) = 1$ and $\sigma(0) = 1, \sigma(1) = \lambda, \sigma(\lambda) = 0$, respectively. In conclusion:

Corollary 2.5. *For an odd non-square D, the degree-D meromorphic function $h : \mathbb{CP}^1 \to \mathbb{CP}^1$, which is the $\mathbb{CP}^1$-component of f in Proposition 2.4, may be assumed to satisfy:*

- *Branch values of h are precisely $0, 1, \lambda, \infty$. Over each h possesses $\frac{D-1}{2}$ points of multiplicity two and a point of multiplicity one from the set $\{0, 1, \lambda, \infty\}$;*
- *$h(\infty) = \infty$ and either* $\begin{cases} h(0) = 0 \\ h(1) = 1 \\ h(\lambda) = \lambda \end{cases}$ *or* $\begin{cases} h(0) = 0 \\ h(1) = \lambda \\ h(\lambda) = 1 \end{cases}$ *or* $\begin{cases} h(0) = 1 \\ h(1) = \lambda \\ h(\lambda) = 0 \end{cases}$.

When D is even, there are at most $\lfloor\frac{D}{2}\rfloor = \frac{D}{2}$ ramification points in any of four critical fibers. The fiber above ∞ contains the point ∞ of multiplicity one which yields the upper bound $\frac{3D}{2} + (\frac{D}{2} - 1) = 2D - 1$ for the number of ramification points of h albeit this number is actually $2D - 2$. We deduce that there are only two possibilities: either h has $\frac{D}{2} - 2$ ramification points above ∞ whereas the number of its ramification points above any of ramification values $0, 1, \lambda$ achieves the maximum $\frac{D}{2}$, or, h has $\frac{D}{2} - 1$ ramification points in the fiber above ∞ and also in the fiber above one of $0, 1, \lambda$ while possesses $\frac{D}{2}$ ramification points above the remaining two values in $\{0, 1, \lambda, \infty\}$. In the latter case, there are four branch values $0, 1, \lambda, \infty$ where there are $\frac{D}{2} - 1$ points of multiplicity two and two points of multiplicity one over two of $0, 1, \lambda$ and $\frac{D}{2}$ points of multiplicity two over any of two remaining branch values. Employing the symmetries in (2.1), we may assume that the branch value other than ∞ whose fiber contains a non-critical point is 0. Constraints on h imply that $0, 1, \lambda, \infty$ constitute the set of points of multiplicity one in the critical fibers $h^{-1}(0), h^{-1}(\infty)$ and besides, $\infty \in h^{-1}(\infty)$. Therefore, either $0, \lambda \in h^{-1}(0), 1 \in h^{-1}(\infty)$ or $0, 1 \in h^{-1}(0), \lambda \in h^{-1}(\infty)$ or $1, \lambda \in h^{-1}(0), 0 \in h^{-1}(\infty)$. Replacing $\big(h(x), \lambda\big)$ with $\big(\frac{h(\lambda x)}{\lambda}, \frac{1}{\lambda}\big)$, the first case transforms to the second one. We conclude that essentially there are only three different cases for even D's:

Corollary 2.6. *For an even non-square $D > 2$, the degree-D meromorphic function $h : \mathbb{CP}^1 \to \mathbb{CP}^1$, which is the $\mathbb{CP}^1$-component of f in Proposition 2.4, may be assumed to satisfy:*

- *Branch values of h are precisely $0, 1, \lambda, \infty$. Either h possesses two points of multiplicity one from $\{0, 1, \lambda, \infty\}$ and $\frac{D}{2} - 1$ points of multiplicity two over each of $0, \infty$ and $\frac{D}{2}$ points of multiplicity two over each of $1, \lambda$, or, it has $\frac{D}{2}$ points of multiplicity two over each of $0, 1, \lambda$ and $\frac{D}{2} - 2$ points of multiplicity two along with four points $0, 1, \lambda, \infty$ of multiplicity one over the value ∞;*
- *either $h(0) = h(1) = h(\lambda) = h(\infty) = \infty$ or $\begin{cases} h(1) = h(\lambda) = 0 \\ h(0) = h(\infty) = \infty \end{cases}$ or $\begin{cases} h(0) = h(1) = 0 \\ h(\lambda) = h(\infty) = \infty \end{cases}$.*

For any of three possibilities outlined in either of Corollaries 2.5 or 2.6 for odd and even D's respectively, it is easy to verify $\frac{h(x)(h(x)-1)(h(x)-\lambda)}{x(x-1)(x-\lambda)}$ is square of another meromorphic function. Thus, exhibiting such a pair $\big(h(x), \lambda\big)$ and then computing $j(\lambda) = 256\frac{(\lambda^2-\lambda+1)^3}{(\lambda^2-\lambda)^2}$ always leads to a j-invariant of an elliptic curve which admits an endomorphism of degree D which is to say, the value of the modular j-function at one point from our finite list of representatives of those τ's in the upper half plane that are associated with D in Proposition 2.4. In each of six cases that appeared in 2.5 and 2.6, in order to determine $\big(h(x), \lambda\big)$ there is a polynomial system of equations to solve which arises from comparing coefficients in different sides of some polynomial identities. These identities hold because of properties of h. For instance, assuming $h(x) = k\frac{x\prod_{i=1}^{\frac{D-1}{2}}(x-\alpha_i)^2}{\prod_{i=1}^{\frac{D-1}{2}}(x-\beta_i)^2}$ in the first set of conditions in Corollary 2.5, there are constraints on numerators of $h(x) - 1$ and $h(x) - \lambda$ which are reflected in system (2.3) below.

Theorem 2.7. *Let $D > 2$ be non-square. Associate three systems of equations with D by equating the coefficients in the following three groups of polynomial identities for odd D's:*

$$(2.3)\quad \begin{cases} kx\prod_{i=1}^{\frac{D-1}{2}}(x-\alpha_i)^2 - \prod_{i=1}^{\frac{D-1}{2}}(x-\beta_i)^2 = k(x-1)\prod_{i=1}^{\frac{D-1}{2}}(x-\gamma_i)^2, \\ kx\prod_{i=1}^{\frac{D-1}{2}}(x-\alpha_i)^2 - \lambda\prod_{i=1}^{\frac{D-1}{2}}(x-\beta_i)^2 = k(x-\lambda)\prod_{i=1}^{\frac{D-1}{2}}(x-\delta_i)^2; \end{cases}$$

$$(2.4)\quad \begin{cases} kx\prod_{i=1}^{\frac{D-1}{2}}(x-\alpha_i)^2 - \prod_{i=1}^{\frac{D-1}{2}}(x-\beta_i)^2 = k(x-\lambda)\prod_{i=1}^{\frac{D-1}{2}}(x-\gamma_i)^2, \\ kx\prod_{i=1}^{\frac{D-1}{2}}(x-\alpha_i)^2 - \lambda\prod_{i=1}^{\frac{D-1}{2}}(x-\beta_i)^2 = k(x-1)\prod_{i=1}^{\frac{D-1}{2}}(x-\delta_i)^2; \end{cases}$$

(2.5)
$$\begin{cases} k(x-\lambda)\prod_{i=1}^{\frac{D-1}{2}}(x-\alpha_i)^2-\prod_{i=1}^{\frac{D-1}{2}}(x-\beta_i)^2=kx\prod_{i=1}^{\frac{D-1}{2}}(x-\gamma_i)^2,\\ k(x-\lambda)\prod_{i=1}^{\frac{D-1}{2}}(x-\alpha_i)^2-\lambda\prod_{i=1}^{\frac{D-1}{2}}(x-\beta_i)^2=k(x-1)\prod_{i=1}^{\frac{D-1}{2}}(x-\delta_i)^2; \end{cases}$$

or the following three group of polynomial identities for even D's:

(2.6)
$$\begin{cases} k\prod_{i=1}^{\frac{D}{2}}(x-\alpha_i)^2-x(x-1)(x-\lambda)\prod_{i=1}^{\frac{D}{2}-2}(x-\beta_i)^2=k\prod_{i=1}^{\frac{D}{2}}(x-\gamma_i)^2,\\ k\prod_{i=1}^{\frac{D}{2}}(x-\alpha_i)^2-\lambda x(x-1)(x-\lambda)\prod_{i=1}^{\frac{D}{2}-2}(x-\beta_i)^2=k\prod_{i=1}^{\frac{D}{2}}(x-\delta_i)^2; \end{cases}$$

(2.7)
$$\begin{cases} k(x-1)(x-\lambda)\prod_{i=1}^{\frac{D}{2}-1}(x-\alpha_i)^2-x\prod_{i=1}^{\frac{D}{2}-1}(x-\beta_i)^2=k\prod_{i=1}^{\frac{D}{2}}(x-\gamma_i)^2,\\ k(x-1)(x-\lambda)\prod_{i=1}^{\frac{D}{2}-1}(x-\alpha_i)^2-\lambda x\prod_{i=1}^{\frac{D}{2}-1}(x-\beta_i)^2=k\prod_{i=1}^{\frac{D}{2}}(x-\delta_i)^2; \end{cases}$$

(2.8)
$$\begin{cases} kx(x-1)\prod_{i=1}^{\frac{D}{2}-1}(x-\alpha_i)^2-(x-\lambda)\prod_{i=1}^{\frac{D}{2}-1}(x-\beta_i)^2=k\prod_{i=1}^{\frac{D}{2}}(x-\gamma_i)^2,\\ kx(x-1)\prod_{i=1}^{\frac{D}{2}-1}(x-\alpha_i)^2-\lambda(x-\lambda)\prod_{i=1}^{\frac{D}{2}-1}(x-\beta_i)^2=k\prod_{i=1}^{\frac{D}{2}}(x-\delta_i)^2; \end{cases}$$

where each system has $2D$ equations and $2D$ unknowns which are $k\neq 0$ along with pairwise distinct numbers λ, α_i's, β_i's, γ_i's, δ_i's in $\mathbb{C}-\{0,1\}$. The values that $j(\lambda)=256\frac{(\lambda^2-\lambda+1)^3}{(\lambda^2-\lambda)^2}$ achieves over the solutions to the systems associated with D are exactly the values of the modular function $j:\mathbb{H}\to\mathbb{C}$ at points $\tau=\frac{1}{2b}\left(u+\sqrt{4D-a^2}\mathrm{i}\right)$ where u,a,b are integers with $\mid a \mid<2\sqrt{D}$ and $4b \mid u^2+4D-a^2$.

Remark 2.8. Any system from Theorem 2.7 consists of $2D$ unknowns and $2D$ equations. Hence, solving these systems is not by any means an efficient algorithm to calculate the j-invariant of elliptic curves with complex multiplication when it is compared to the classical algorithm (cf. [3]) of solving a single equation obtained from the Hilbert class polynomial. We want to emphasize that the significance of this point of view is not computing special values of the modular function more easily but the fact that it enables us to write down explicit equations in terms of Legendre forms not only for self-isogenies but also for isogenies (like what we did in order to derive Theorems 2.1, 2.2.) which quickly provides us with the j-invariant as well.

We might add that the class of meromorphic functions introduced in Corollaries 2.5, 2.6 are interesting from the dynamical point of view too if one looks at their iterations. They are examples of classical Lattès maps and are completely chaotic in the sense that the Julia set is the whole Riemann sphere as their critical points are not periodic nevertheless eventually periodic. See [10] for more details.

Remark 2.9. The conditions imposed on the number of branch values of $h:\mathbb{CP}^1\to\mathbb{CP}^1$ and also the computations one has to handle in order to

determine $h(x)$ through solving a system of polynomial equations, resemble to those of Belyi theory when a Belyi function on the Riemann sphere is needed to be recovered from its dessin. But our desired functions $h(x)$ are not Belyi because they possess four critical values instead of three and also there are restrictions on their fibers, the difference that makes this family of functions much more rigid. In the Belyi case we get finitely many solutions over $\bar{\mathbb{Q}}$ only after rigidifying the dessin with fixing three of its vertices whereas in our case, any of systems (2.3) through (2.8) has finite number of solutions all of them lying in $\bar{\mathbb{Q}}$, i.e. $h(x)$ is actually defined over algebraic numbers in the sense of $h(x) \in \bar{\mathbb{Q}}(x)$. To see the reason, note that $j(\lambda)$ and (therefore λ) is algebraic, being the j-invariant of an elliptic curve with complex multiplication. So the orbit of the set of branch values $\{0, 1, \lambda, \infty\}$ under $\mathrm{Gal}\big(\frac{\mathbb{C}}{\bar{\mathbb{Q}}}\big)$ is finite while the number of isomorphism classes of degree-D maps $\mathbb{CP}^1 \to \mathbb{CP}^1$ with a prescribed set of branch values is also finite as they are determined by their monodromy representation. So the $\mathrm{Gal}\big(\frac{\mathbb{C}}{\bar{\mathbb{Q}}}\big)$-orbit of h is finite up to isomorphisms of maps and therefore, invoking the criterion for arithmeticity mentioned in [5, p. 265], the meromorphic function h has a model over $\bar{\mathbb{Q}}$. But in the family of functions obeying the constraints for a fixed λ, there are only finitely many functions h' isomorphic to h as the number of Möbius transformations which preserve the set $\{0, 1, \lambda, \infty\}$ –which is simultaneously the set of critical values and the set of non-critical points of critical fibers for both h and h' –is finite. Thus, the number of choices for such a degree-D map h is finite and now as $\mathrm{Gal}\big(\frac{\mathbb{C}}{\bar{\mathbb{Q}}}\big)$ acts on them, they are defined over $\bar{\mathbb{Q}}$.

Example 2.10. Points below represent all of the $\mathrm{SL}_2(\mathbb{Z})$-orbits in Proposition 2.4 for $D = 3$:

$$\begin{aligned} &\frac{1}{2}\sqrt{4\times 3}\mathrm{i} = \sqrt{3}\mathrm{i},\ \frac{1}{2}\left(1+\sqrt{4\times 3-1^2}\mathrm{i}\right) = \frac{1+\sqrt{11}\mathrm{i}}{2},\\ &\frac{1}{2}\sqrt{4\times 3-2^2}\mathrm{i} = \sqrt{2}\mathrm{i},\ \frac{1}{2}\left(1+\sqrt{4\times 3-3^2}\mathrm{i}\right) = \frac{1+\sqrt{3}\mathrm{i}}{2}. \end{aligned} \tag{2.9}$$

When $D = 3$, the solutions to system (2.3) consists the following set of polynomial identities and its Galois conjugate

$$\begin{cases} -\frac{1}{3}x\big(x-(1+\mathrm{e}^{\frac{\pi\mathrm{i}}{3}})\big)^2 - \big(x-\frac{1+\mathrm{e}^{\frac{\pi\mathrm{i}}{3}}}{3}\big)^2 = -\frac{1}{3}(x-1)(x-\mathrm{e}^{\frac{2\pi\mathrm{i}}{3}})^2,\\ -\frac{1}{3}x\big(x-(1+\mathrm{e}^{\frac{\pi\mathrm{i}}{3}})\big)^2 - \mathrm{e}^{\frac{\pi\mathrm{i}}{3}}\big(x-\frac{1+\mathrm{e}^{\frac{\pi\mathrm{i}}{3}}}{3}\big)^2 = -\frac{1}{3}(x-\mathrm{e}^{\frac{\pi\mathrm{i}}{3}})(x+\mathrm{e}^{\frac{2\pi\mathrm{i}}{3}})^2, \end{cases}$$

where $\lambda = \mathrm{e}^{\frac{\pm\pi\mathrm{i}}{3}}$. The function $j(\lambda) = 256\frac{(\lambda^2-\lambda+1)^3}{(\lambda^2-\lambda)^2}$ vanishes at $\lambda = \mathrm{e}^{\pm\frac{\pi\mathrm{i}}{3}}$. It is a standard fact that the value zero of j-invariant corresponds to the hexagonal lattice and therefore the period $\tau = \frac{1+\sqrt{3}\mathrm{i}}{2}$ from the list (2.9).

For system (2.4) we have:

$$\begin{cases} -\frac{1}{3}x\big(x-\frac{\lambda+1}{2}\big)^2-\big(x-\frac{2\lambda}{\lambda+1}\big)^2=-\frac{1}{3}(x-\lambda)(x+1)^2, \\ -\frac{1}{3}x\big(x-\frac{\lambda+1}{2}\big)^2-\lambda\big(x-\frac{2\lambda}{\lambda+1}\big)^2=-\frac{1}{3}(x-1)(x+\lambda)^2, \end{cases} \quad \lambda=-7\pm4\sqrt{3};$$

$$\begin{cases} \frac{\lambda(t+1)^2}{(\lambda-t)^2}x\big(x-\frac{1+t\lambda}{1+t}\big)^2-\big(x-\frac{\lambda(1-t)}{\lambda-t}\big)^2=\frac{\lambda(t+1)^2}{(\lambda-t)^2}(x-\lambda)(x-t)^2, \\ \frac{\lambda(t+1)^2}{(\lambda-t)^2}x\big(x-\frac{1+t\lambda}{1+t}\big)^2-\lambda\big(x-\frac{\lambda(1-t)}{\lambda-t}\big)^2=\frac{\lambda(t+1)^2}{(\lambda-t)^2}(x-1)(x+t\lambda)^2, \end{cases} \begin{cases} t\in\{\pm\mathrm{i}\}, \\ \lambda\in\{3\pm2\sqrt{2}\}; \end{cases}$$

that leads to j-values:

$$256\frac{(\lambda^2-\lambda+1)^3}{(\lambda^2-\lambda)^2}\,|_{-7\pm4\sqrt{3}}=16\times15^3=54000, \quad 256\frac{(\lambda^2-\lambda+1)^3}{(\lambda^2-\lambda)^2}\,|_{3\pm2\sqrt{2}}=20^3=8000.$$[1]

After writing down the q-expansion up to four terms: $j\left(\sqrt{2}\mathrm{i}\right)\approx 7999.9977$ and $j\left(\sqrt{3}\mathrm{i}\right)\approx 53999.9924$. So we deduce that $j\left(\sqrt{2}\mathrm{i}\right)=20^3$ and $j\left(\sqrt{3}\mathrm{i}\right)=16\times15^3$. Finally, the system (2.5) for $D=3$ is the hardest to solve. Its solutions are polynomial identities below

$$\begin{cases} -\frac{16(t+1)^3}{(t+2)(3t+2)^3}(x-\frac{(t+2)^3(3t+2)}{16(t+1)^3})(x-\frac{(t+2)(3t+2)}{4(t+1)})^2-(x-\frac{(t+2)^2}{4(t+1)})^2 \\ =-\frac{16(t+1)^3}{(t+2)(3t+2)^3}x(x-\frac{(t+2)(3t+2)}{4(t+1)^2})^2, \\ \\ -\frac{16(t+1)^3}{(t+2)(3t+2)^3}(x-\frac{(t+2)^3(3t+2)}{16(t+1)^3})(x-\frac{(t+2)(3t+2)}{4(t+1)})^2-\frac{(t+2)^3(3t+2)}{16(t+1)^3}(x-\frac{(t+2)^2}{4(t+1)})^2 \\ =-\frac{16(t+1)^3}{(t+2)(3t+2)^3}(x-1)(x+\frac{t(3t+4)}{4(t+1)^2}-1)^2, \end{cases}$$

where $\lambda=\frac{(t+2)^3(3t+2)}{16(t+1)^3}$ and t is a root of $(3t+2)^4(t+2)^4-16t(t+1)^3(3t+4)^3$, a polynomial that factors as:

$$(3t^2+6t+4)\left[(3t^2+6t+4)^3-8t(3t^2+6t+4)^2-24t^2(3t^2+6t+4)-16t^3\right].$$

So either $t=-1\pm\frac{\mathrm{i}\sqrt{3}}{3}$ where $\lambda=\frac{1\mp\mathrm{i}\sqrt{3}\mathrm{i}}{2}$, at which $j(\lambda)$ vanishes and we are in the case of hexagonal elliptic curve again, or, t satisfies the quadratic equation $3t^2+6t+4=ut$ where $u^3-8u^2-24u-16=0$. In the latter situation, with help of a numerical software like MATLAB, one observes that for any of six t's just mentioned, the value of $j(\lambda)=256\frac{(\lambda^2-\lambda+1)^3}{(\lambda^2-\lambda)^2}$ at $\lambda=\frac{(t+2)^3(3t+2)}{16(t+1)^3}$ coincides with -32768 to six digits after the decimal point. The only τ left in list (2.9) is $\frac{1+\sqrt{11}\mathrm{i}}{2}$. It is well-known that $j\left(\frac{1+\sqrt{11}\mathrm{i}}{2}\right)$ equals $-32768=-2^{15}$ (for instance, check [3, p. 383], the fact that moreover is confirmed by the q-expansion:

$$j\left(\frac{1+\sqrt{11}\mathrm{i}}{2}\right)\approx-\mathrm{e}^{\pi\sqrt{11}}+744-196884\mathrm{e}^{-\pi\sqrt{11}}+21493760\mathrm{e}^{-2\pi\sqrt{11}}\approx-32767.9999.$$

[1] Here a simple observation was employed stating that $j(\lambda)=256\frac{(\lambda^2-\lambda+1)^3}{(\lambda^2-\lambda)^2}$ is equal to $256\frac{(\mu+1)^3}{\mu+2}$ at the roots of $\lambda^2+\mu\lambda+1=0$.

Example 2.11. When D is a perfect square, careful analysis of the multiplication by $n \in \mathbb{Z}$ map on an elliptic curve $E = \frac{\mathbb{C}}{\Lambda}$ shows that, even for such D's, any solution to one of our systems except systems (2.3) and (2.6) leads to a j-invariant computation because $f : P \mapsto \pm\sqrt{D}P$ either fixes all four critical points of the Weierstrass elliptic function or maps them all to the identity element $0 + \Lambda$.
For $D = 4$ in Proposition 2.4, a complete set of representatives of $\mathrm{SL}_2(\mathbb{Z})$-orbits is:

(2.10)

$$\frac{1}{2}\sqrt{4\times 4}\mathrm{i} = 2\mathrm{i},\ \frac{1}{4}\sqrt{4\times 4}\mathrm{i} = \mathrm{i},\ \frac{1}{2}\sqrt{4\times 4 - 2^2}\mathrm{i} = \sqrt{3}\mathrm{i},$$
$$\frac{1}{4}\left(2+\sqrt{4\times 4-2^2}\mathrm{i}\right) = \frac{1+\sqrt{3}\mathrm{i}}{2},\ \frac{1}{2}\left(1+\sqrt{4\times 4-3^2}\right) = \frac{1+\sqrt{7}\mathrm{i}}{2},$$
$$\frac{1}{2}\left(1+\sqrt{4\times 4-1^2}\mathrm{i}\right) = \frac{1+\sqrt{15}\mathrm{i}}{2},\ \frac{1}{4}\left(1+\sqrt{4\times 4-1^2}\mathrm{i}\right) = \frac{1+\sqrt{15}\mathrm{i}}{4}.$$

System (2.7) is much easier to solve and yields:

$$\begin{cases} -\frac{1}{4}(x-1)(x-\beta^2)(x+\beta)^2 - x(x-\beta)^2 = -\frac{1}{4}\left(x^2+(4\beta+2)x+\beta^2\right)^2, \\ -\frac{1}{4}(x-1)(x-\beta^2)(x+\beta)^2 - \beta^2 x(x-\beta)^2 = -\frac{1}{4}\left(x^2-(8\beta+2)x+\beta^2\right)^2, \end{cases}$$
$$\beta \in \{-3\pm 2\sqrt{2}\},\quad \lambda = \beta^2 \in \{17\pm 12\sqrt{2}\};$$

$$\begin{cases} \frac{\beta^2-1}{4(u+2\beta)}(x-1)(x-\beta^2)(x+\beta)^2 - x(x-\beta)^2 = \frac{\beta^2-1}{4(u+2\beta)}\left(x^2+ux+\beta^2\right)^2, \\ \frac{\beta^2-1}{4(u+2\beta)}(x-1)(x-\beta^2)(x+\beta)^2 - \beta^2 x(x-\beta)^2 = \frac{\beta^2-1}{4(u+2\beta)}\left(x^2-(u+4\beta)x+\beta^2\right)^2, \end{cases}$$
$$\beta \in \{\pm\mathrm{i}(2\pm\sqrt{3})\},\quad \lambda = \beta^2 \in \{-7\pm 4\sqrt{3}\},\quad u = \beta + 1 - \frac{(\beta+\frac{1}{\beta})(\beta-1)}{2}.$$

In the first solution, $j(\lambda) = 256\frac{(\lambda^2-\lambda+1)^3}{(\lambda^2-\lambda)^2}\ |_{17\pm 12\sqrt{2}} = 66^3 = 287496$ while for $\tau = 2\mathrm{i}$ in (2.10): $j(2i) \approx \mathrm{e}^{4\pi} + 744 + 196884\mathrm{e}^{-4\pi} + 21493760\mathrm{e}^{-8\pi} \approx 287495.9999$.
In the second solution to system (2.7) , $\lambda = -7\pm 4\sqrt{3}$ corresponds to $j\left(\sqrt{3}\mathrm{i}\right) = 16\times 15^3$, just like what we saw in the previous example.
In the case of system (2.8), some rather cumbersome algebraic manipulations culminate in the following identities as all of solutions to (2.8):

$$\begin{cases} \frac{t(t^2+1)}{2}x(x-1)\left(x-\frac{(t+1)^2}{2(t^2+1)}\right)^2 - (x-t^4)\left(x-\frac{(t+1)^2}{4t}\right)^2 = \frac{t(t^2+1)}{2}\left(x^2-(1+\frac{1}{t})x+t^3\right)^2, \\ \frac{t(t^2+1)}{2}x(x-1)\left(x-\frac{(t+1)^2}{2(t^2+1)}\right)^2 - t^4(x-t^4)\left(x-\frac{(t+1)^2}{4t}\right)^2 = \frac{t(t^2+1)}{2}\left(x^2-(t+1)x+t^5\right)^2, \end{cases}$$
$$t \in \left\{\frac{-1\pm\sqrt{7}\mathrm{i}}{4}, \frac{\sqrt{5}-1}{8}\left(1\pm\left(2\sqrt{3}+\sqrt{15}\right)\mathrm{i}\right), \frac{\sqrt{5}+1}{8}\left(-1\pm\left(2\sqrt{3}-\sqrt{15}\right)\mathrm{i}\right)\right\}, \lambda = t^4.$$

Then we should evaluate $j(\lambda) = 256\frac{(\lambda^2-\lambda+1)^3}{(\lambda^2-\lambda)^2}$ at $\lambda = t^4$ for the aforementioned values of t. When $t = \frac{-1\pm\sqrt{7}\mathrm{i}}{4}$, we have $\lambda = t^4 = \frac{1\pm 3\sqrt{7}\mathrm{i}}{32}$ at which the j-invariant is -15^3. On the other hand, truncating the q-expansion up to five terms shows

that $j\left(\frac{1+\sqrt{7}\mathrm{i}}{2}\right) \approx -3375$ to four digits after the decimal point. Therefore $j\left(\frac{1+\sqrt{7}\mathrm{i}}{2}\right) = -15^3$. For the other four values of t: [2]

$$\begin{cases} j(\lambda)\Big|_{\left(\frac{\sqrt{5}-1}{8}\left(1\pm\left(2\sqrt{3}+\sqrt{15}\right)\mathrm{i}\right)\right)^4} = \frac{(7-3\sqrt{5})^2(-1+3\sqrt{5})^3(15+3\sqrt{5})^3}{256} \approx 632.8334, \\ j(\lambda))\Big|_{\left(\frac{\sqrt{5}+1}{8}\left(-1\pm\left(2\sqrt{3}-\sqrt{15}\right)\mathrm{i}\right)\right)^4} = \frac{(7+3\sqrt{5})^2(-1-3\sqrt{5})^3(15-3\sqrt{5})^3}{256} \approx -191657.8328. \end{cases}$$

Writing down the q-expansion implies that these are j-values at points $\frac{1+\sqrt{15}\mathrm{i}}{4}$ and $\frac{1+\sqrt{15}\mathrm{i}}{2}$ from (2.10):

$$j\left(\frac{1+\sqrt{15}\mathrm{i}}{4}\right) \approx 744 - 21493760\mathrm{e}^{-\pi\sqrt{15}} + 20245856256e^{-2\pi\sqrt{15}} \approx 632.8334,$$
$$j\left(\frac{1+\sqrt{15}\mathrm{i}}{2}\right) \approx -\mathrm{e}^{\pi\sqrt{15}} + 744 - 196884\mathrm{e}^{-\pi\sqrt{15}} + 21493760\mathrm{e}^{-2\pi\sqrt{15}} \approx -191657.83286.$$

3. **Covers by genus-2 curves**

Consider a curve of genus 2 in its Rosenhain form:

$$C_{\lambda_1,\lambda_2,\lambda_3} = \{y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3)\},$$

with $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{C} - \{0, 1\}$ pairwise distinct. The complex structure of a Riemann surface of genus 2 is uniquely determined by the positions of six branch values of the degree-2 morphism $C \to \mathbb{CP}^1$. Therefore, there is a bijection between isomorphism classes of Riemann surfaces of genus 2 and 6-element subsets of $\mathbb{CP}^1$ modulo Möbius transformations. We can assume that these subsets contain $\{0, 1, \infty\}$, which is the case for the Rosenhain form. Then, one should answer this question: if a Möbius transformation β carries $\{0, 1, \infty, \lambda_1, \lambda_2, \lambda_3\}$ to another set of cardinality six $\{0, 1, \infty, \lambda_1', \lambda_2', \lambda_3'\}$, what are the choices for λ_i''s in terms of λ_i's? This provides us with an action of a finite group on the domain

$$\mathbb{D} = \left\{(\lambda_1, \lambda_2, \lambda_3) \in (\mathbb{C} - \{0, 1\})^3 \,\middle|\, \lambda_i \neq \lambda_j\right\}$$

which is the genus-2 analogue of the S_3-action on $\mathbb{C} - \{0, 1\}$ in (2.1). Conditioning on the size of $\beta(\{0, 1, \infty\}) \cap \{0, 1, \infty\}$, it is not hard to write down this

[2] We have to explain how these calculations have been carried out: in order to establish these polynomial identities, $t \neq 0, 1$ must be a root of $8t^5(t^2+1)-(t+1)^4$. A quadratic equation which has $\lambda = t^4$ as a root is determined by factorizing this polynomial and then a simple observation was employed which states that $j(\lambda) = 256\frac{(\lambda^2-\lambda+1)^3}{(\lambda^2-\lambda)^2}$ is equal to $256\frac{(\mu-1)^3}{\mu}$ at the roots of $\lambda^2 - \mu\lambda + \mu = 0$.

action. We outline the generators and the corresponding isomorphisms:

$$
\begin{aligned}
&\sigma_1 : (\lambda_1,\lambda_2,\lambda_3) \mapsto \left(\frac{1}{\lambda_1},\frac{\lambda_2}{\lambda_1},\frac{\lambda_3}{\lambda_1}\right), \quad \begin{cases} C_{\lambda_1,\lambda_2,\lambda_3} \overset{\cong}{\to} C_{\frac{1}{\lambda_1},\frac{\lambda_2}{\lambda_1},\frac{\lambda_3}{\lambda_1}} \\ (x,y) \mapsto \left(\frac{x}{\lambda_1}, \frac{y}{\lambda_1^{\frac{5}{2}}}\right) \end{cases} ; \\
&\sigma_2 : (\lambda_1,\lambda_2,\lambda_3) \mapsto \left(\frac{\lambda_1}{\lambda_2},\frac{1}{\lambda_2},\frac{\lambda_3}{\lambda_2}\right), \quad \begin{cases} C_{\lambda_1,\lambda_2,\lambda_3} \overset{\cong}{\to} C_{\frac{\lambda_1}{\lambda_2},\frac{1}{\lambda_2},\frac{\lambda_3}{\lambda_2}} \\ (x,y) \mapsto \left(\frac{x}{\lambda_2}, \frac{y}{\lambda_2^{\frac{5}{2}}}\right) \end{cases} ; \\
&\sigma_3 : (\lambda_1,\lambda_2,\lambda_3) \mapsto \left(\frac{\lambda_1}{\lambda_3},\frac{\lambda_2}{\lambda_3},\frac{1}{\lambda_3}\right), \quad \begin{cases} C_{\lambda_1,\lambda_2,\lambda_3} \overset{\cong}{\to} C_{\frac{\lambda_1}{\lambda_3},\frac{\lambda_2}{\lambda_3},\frac{1}{\lambda_3}} \\ (x,y) \mapsto \left(\frac{x}{\lambda_3}, \frac{y}{\lambda_3^{\frac{5}{2}}}\right) \end{cases} ; \\
&\sigma_4 : (\lambda_1,\lambda_2,\lambda_3) \mapsto (1-\lambda_1, 1-\lambda_2, 1-\lambda_3), \quad \begin{cases} C_{\lambda_1,\lambda_2,\lambda_3} \overset{\cong}{\to} C_{1-\lambda_1,1-\lambda_2,1-\lambda_3} \\ (x,y) \mapsto (1-x, \mathrm{i}y) \end{cases} ; \\
&\sigma_5 : (\lambda_1,\lambda_2,\lambda_3) \mapsto \left(\frac{1}{\lambda_1},\frac{1}{\lambda_2},\frac{1}{\lambda_3}\right), \quad \begin{cases} C_{\lambda_1,\lambda_2,\lambda_3} \overset{\cong}{\to} C_{\frac{1}{\lambda_1},\frac{1}{\lambda_2},\frac{1}{\lambda_3}} \\ (x,y) \mapsto \left(\frac{1}{x}, \frac{y}{(\lambda_1\lambda_2\lambda_3)^{\frac{1}{2}}\, x^3}\right) \end{cases} .
\end{aligned} \tag{3.1}
$$

The reader may easily verify that any two of involutions $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ satisfy the braid relation whereas the involution σ_5 commutes with $\sigma_1, \sigma_2, \sigma_3$ and satisfies the braid relation solely with σ_4. So there is a group isomorphism $\langle \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5 \rangle \overset{\cong}{\to} \mathrm{S}_6$ which maps $\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5$ to transpositions $(1\,2)$, $(1\,3)$, $(1\,4)$, $(1\,5)$ and $(5\,6)$ respectively. Thus, the moduli space $\mathcal{M}_2$ of genus-2 Riemann surfaces can be thought of as the quotient of the domain $\mathbb{D}$ in $\mathbb{C}^3$ by the action of S_6 described in (3.1).

The subfield $\mathbb{C}(\lambda_1,\lambda_2,\lambda_3)^{\mathrm{S}_6}$ is the field of invariants of the Rosenhain form over $\mathbb{C}$. The results of the paper [6] indicate that this invariant subfield is a rational function field. Thus, there are three algebraically independent rational functions in λ_i's that parametrize the moduli space $\mathcal{M}_2 = \mathbb{D}/\mathrm{S}_6$ of Riemann surfaces of genus 2. The interested reader can observe the complicated formulae for these "j-invariants for genus 2" on pages 111,112 of [9] along with the S_6 action described in (3.1) although with different generators.

Remark 3.1. Projectivizing the first four generators in (3.1), we get an action of S_5 on the polynomial ring $\mathbb{C}[x_0, x_1, x_2, x_3]$:

$$
\begin{aligned}
\tilde{\sigma}_1 &= (1\,2) : (x_0,x_1,x_2,x_3) \mapsto (x_1,x_0,x_2,x_3); \\
\tilde{\sigma}_2 &= (1\,3) : (x_0,x_1,x_2,x_3) \mapsto (x_2,x_1,x_0,x_3); \\
\tilde{\sigma}_3 &= (1\,4) : (x_0,x_1,x_2,x_3) \mapsto (x_3,x_1,x_2,x_0); \\
\tilde{\sigma}_4 &= (1\,5) : (x_0,x_1,x_2,x_3) \mapsto (-x_0, x_1-x_0, x_2-x_0, x_3-x_0).
\end{aligned}
$$

One should find the invariant subring under this action and then invariant rational functions in $\mathbb{C}(\lambda_1,\lambda_2,\lambda_3)^{S_5}$ are precisely ratios of two invariant homogeneous polynomials of the same degree. The generators described above are all "pseudo-reflection"s, i.e. linear transformations with exactly one eigenvalue different from one. Thus, the classical Chevalley-Shephard-Todd theorem implies that the invariant subring $\mathbb{C}[x_0,x_1,x_2,x_3]^{S_5}$ is generated by four algebraically independent homogeneous polynomials where the product of their degrees is $|S_5| = 120$. See [16] for the background material on the invariant theory of finite groups. One can write a computer program that finds a basis for homogeneous invariant polynomials of a given degree by averaging over the orbits of monomials of that degree. Using this idea, the author has computed homogeneous polynomials of degrees $2,3,4,5$ which generate the invariant subring. So the field $\mathbb{C}(\lambda_1,\lambda_2,\lambda_3)^{S_5=\langle\sigma_1,\sigma_2,\sigma_3,\sigma_4\rangle}$ is generated over $\mathbb{C}$ with three algebraically independent rational functions that are ratios of suitable powers of these polynomial generators evaluated at $(x_0,x_1,x_2,x_3)=(1,\lambda_1,\lambda_2,\lambda_3)$.

After this brief digression, let us go back to the unifying theme of this article which is to *descend* things via morphisms of algebraic curves. Suppose that f is a degree-2 morphism from the genus-2 curve $C=C_{\lambda_1,\lambda_2,\lambda_3}$ onto the elliptic curve $E=E_\lambda=\{y^2=x(x-1)(x-\lambda)\}$ which respects hyperelliptic involutions. This is precisely the situation where the genus-2 curve C has an order-2 automorphism σ other than the hyperelliptic involution and thus there is a degree 2 map from it onto the elliptic curve $C/\langle\sigma\rangle$. Now, form the commutative diagram:

$$(\star\star\star)\qquad \begin{array}{ccc} C_{\lambda_1,\lambda_2,\lambda_3} & \xrightarrow{\ f\ } & E_\lambda \\ {\scriptstyle (x,y)\mapsto x}\downarrow & & \downarrow{\scriptstyle (x,y)\mapsto x} \\ \mathbb{CP}^1 & \xrightarrow{\ h\ } & \mathbb{CP}^1. \end{array}$$

The fact that the top row is a morphism of hyperelliptic curves implies that f maps any of six Weierstrass points of $C_{\lambda_1,\lambda_2,\lambda_3}$ to one of four ramification points of the right column and thus the values of h at points $0,1,\infty,\lambda_1,\lambda_2,\lambda_3$ lie in $\{0,1,\infty,\lambda\}$. None of the Weierstrass points of $C_{\lambda_1,\lambda_2,\lambda_3}$ can be a ramification point of f: otherwise, for any arbitrary $0\neq\omega\in\Omega^1(E_\lambda)$, the non-zero holomorphic 1-form $f^*\omega$ on $C_{\lambda_1,\lambda_2,\lambda_3}$ vanishes at a Weierstrass point p. But since $2p$ is a canonical divisor, the divisor of $f^*\omega$ is precisely $2p$. This is absurd as $f^*\omega$ vanishes at the other ramification point of f as well. Therefore, the degree-2 map $h:\mathbb{CP}^1\to\mathbb{CP}^1$ has multiplicity one at all of points $0,1,\infty,\lambda_1,\lambda_2,\lambda_3$ and maps each of them to one of the values $0,1,\infty,\lambda$. Its fiber above any of these values cannot contain only one of these points as otherwise $(\star\star\star)$ implies that f has three points over the unique point of E over that value. Hence, except one value in $\{0,1,\infty,\lambda\}$ –which is necessarily ramified by diagram chasing –over any other value there are two distinct members of $\{0,1,\infty,\lambda_1,\lambda_2,\lambda_3\}$. Without

any loss of generality or change in the analytic structures of either $C_{\lambda_1,\lambda_2,\lambda_3}$ or E_λ, one may assume that

$$0,1 \mapsto 0, \quad \infty,\lambda_1 \mapsto \infty, \quad \lambda_2,\lambda_3 \mapsto 1, \quad \lambda \text{ a critical value of } h.$$

So h can be described as $h(x)=\frac{kx(x-1)}{x-\lambda_1}$ where $kx(x-1)-\lambda(x-\lambda_1)$ has a double root, i.e. $\lambda_1=\frac{(\lambda+k)^2}{4k\lambda}$ and moreover λ_2,λ_3 satisfy: $\frac{k\lambda_2(\lambda_2-1)}{\lambda_2-\lambda_1}=\frac{k\lambda_3(\lambda_3-1)}{\lambda_3-\lambda_1}=1$. We conclude that all of λ_i's may be written in terms of λ,k.

Proposition 3.2. *Any degree-2 morphism $C_{\lambda_1,\lambda_2,\lambda_3} \to E_\lambda$ between a genus-2 curve and an elliptic curve, after changing $(\lambda_1,\lambda_2,\lambda_3)$ and λ by suitable elements of their orbits under the actions of S_6 and S_3 (and composing with a translation of E_λ if necessary), fits in the following family:*

$$\begin{cases} f_{\lambda,k} : C_{\lambda_1(\lambda,k),\lambda_2(\lambda,k),\lambda_3(\lambda,k)} \to E_\lambda \\ (x,y) \mapsto \left(\frac{kx(x-1)}{x-\lambda_1(\lambda,k)}, \frac{k^{\frac{3}{2}}\left(x-\frac{k+\lambda}{2k}\right)}{(x-\lambda_1(\lambda,k))^2}y \right) \end{cases},$$

where $\lambda_1=\frac{(\lambda+k)^2}{4k\lambda}$ and $\lambda_2(\lambda,k),\lambda_3(\lambda,k)$ are roots of $\frac{kx(x-1)}{x-\lambda_1(\lambda,k)}=1$.

Remark 3.3. Classifying genus-2 curves that admit automorphisms other than the hyperelliptic involution is a very old problem and is solved completely in the classical paper [2] by careful study of binary sextics. According to this paper, any such a curve can be described as:

$$y^2=(x^2-1)(x^2-a^2)(x^2-b^2) \quad (a,b \in \mathbb{C}-\{0,\pm 1\}, a \neq \pm b). \tag{3.2}$$

Thus, we should be able to transform the genus-2 curve $C_{\lambda_1(\lambda,k),\lambda_2(\lambda,k),\lambda_3(\lambda,k)}$ in Proposition 3.2 to the form above. The deck transformation group of the map $x \mapsto \frac{kx(x-1)}{x-\lambda_1}$ in the bottom row of $(\star\star\star)$ is generated with the order-2 Möbius transformation $x \mapsto \frac{\lambda_1(x-1)}{x-\lambda_1}$ that cannot fix any of simple points of h appeared in $\{0,1,\infty,\lambda_1(\lambda,k),\lambda_2(\lambda,k),\lambda_3(\lambda,k)\}$. But any Möbius transformation of order 2 is conjugate with $x \mapsto -x$. So after applying an appropriate Möbius transformation to the previous set, one gets a set in the form of $\{\pm 1,\pm a,\pm b\}$.

In the rest of this section we imitate arguments of Theorems 2.1, 2.2 in order to extract information about periods of a genus-2 Riemann surface from the knowledge of existence of a morphism from it onto some elliptic curve whose period lattice is known. It is more convenient to work with the general form (3.2) of a genus-2 curve with "many automorphisms"[3] rather than that of Proposition 3.2. We are going to fix $C=\left\{y^2=(x^2-1)(x^2-a^2)(x^2-b^2)\right\}$ and exhibit different morphisms from it onto two elliptic curves which are

[3]The term is adopted from [6] and it refers to existence of a non-trivial automorphism other than the hyperelliptic involution.

its quotients under automorphisms $\sigma : (x,y) \mapsto (-x,y)$ and $\sigma' : (x,y) \mapsto (-x,-y)$.[4] These morphisms are:

$$\begin{cases} f : C = \left\{y^2 = (x^2-1)(x^2-a^2)(x^2-b^2)\right\} \to E := \left\{y^2 = (x-1)(x-a^2)(x-b^2)\right\} \\ (x,y) \mapsto \left(x^2, y\right) \end{cases}, \tag{3.3}$$
$$\begin{cases} f' : C = \left\{y^2 = (x^2-1)(x^2-a^2)(x^2-b^2)\right\} \to E' := \left\{y^2 = (x-1)\left(x-\frac{1}{a^2}\right)\left(x-\frac{1}{b^2}\right)\right\} \\ (x,y) \mapsto \left(\frac{1}{x^2}, \frac{iy}{ab x^3}\right). \end{cases}$$

Our goal is to describe a normalized period matrix of C in the Siegel upper half plane in terms of two periods $\tau, \tau' \in \mathbb{H}$ of E, E'. There is a classical method due to Bolza in [2] for calculating periods of Riemann surfaces with sufficiently large group of automorphisms. The reader may consult [1, Section 11.7], for a modern treatment of his approach where the table in [1, p. 340] presents several period matrices obtained in this way.

Let us think of C as two copies of $\mathbb{CP}^1$ which are glued together along three cuts between a and b, -1 and 1, $-a$ and $-b$ as depicted in Figure 1. Cycles

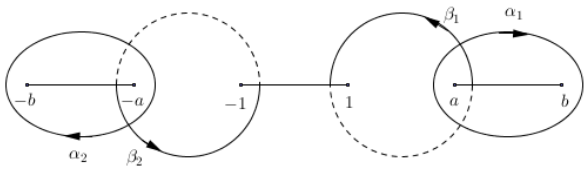

FIGURE 1. Constructing C by cutting and pasting.

$\alpha_1, \alpha_2, \beta_1, \beta_2$ form a symplectic basis for $\mathrm{H}_1(C,\mathbb{Z})$ where the full arcs are in the sheet we are working with and the dotted ones are in the other sheet. The induced map $\sigma_* : \mathrm{H}_1(C,\mathbb{Z}) \to \mathrm{H}_1(C,\mathbb{Z})$ takes α_i to α_{2-i} and β_i to and β_{2-i} whereas under $\sigma'_* : \mathrm{H}_1(C,\mathbb{Z}) \to \mathrm{H}_1(C,\mathbb{Z})$: $\alpha_i \mapsto -\alpha_{2-i}$ and $\beta_i \mapsto -\beta_{2-i}$. Fix the basis $\left\{\omega_1 = \frac{\mathrm{d}x}{y}, \omega_2 = \frac{x\mathrm{d}x}{y}\right\}$ for $\Omega^1(C)$. The matrix

$$Z = \begin{bmatrix} \int_{\alpha_1}\omega_1 & \int_{\alpha_2}\omega_1 \\ \int_{\alpha_1}\omega_2 & \int_{\alpha_2}\omega_2 \end{bmatrix}^{-1} \begin{bmatrix} \int_{\beta_1}\omega_1 & \int_{\beta_2}\omega_1 \\ \int_{\beta_1}\omega_2 & \int_{\beta_2}\omega_2 \end{bmatrix}$$

lies in the Siegel upper half plane of degree 2. Note that $\sigma^*\omega_1 = -\omega_1, \sigma^*\omega_2 = \omega_2$ while $\sigma'^*\omega_1 = \omega_1, \sigma'^*\omega_2 = -\omega_2$. Morphisms $f : C \to E$ and $f' : C \to E'$ send the homology basis of $\mathrm{H}_1(C,\mathbb{Z})$ to symplectic bases $\{\delta,\gamma\}$ and $\{\delta',\gamma'\}$ for $\mathrm{H}_1(E,\mathbb{Z})$ and $\mathrm{H}_1(E',\mathbb{Z})$ respectively which are depicted in figures below.

[4] In terms of $C_{\lambda_1(\lambda,k),\lambda_2(\lambda,k),\lambda_3(\lambda,k)}$, just note that the transformation $(\lambda,k) \mapsto \left(\frac{k^2}{\lambda}, -k\right)$ changes λ_i to $1-\lambda_i$ which is one of the transformations in (3.1). Hence $C_{\lambda_1(\lambda,k),\lambda_2(\lambda,k),\lambda_3(\lambda,k)}$ admits morphisms to both of elliptic curves E_λ , $E_{\frac{k^2}{\lambda}}$ that are non-isomorphic for generic values of k, λ.

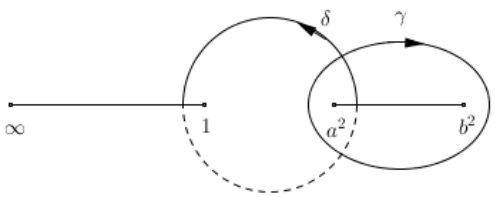

FIGURE 2. A symplectic homology basis for the elliptic curve E

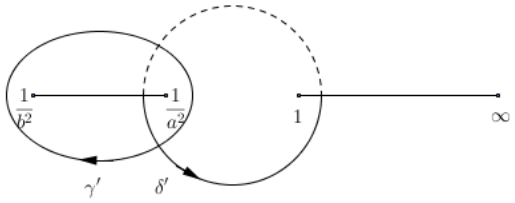

FIGURE 3. A symplectic homology basis for the elliptic curve E'

Since f, f' are quotient maps under the actions of σ, σ', due to the description of their actions on homology explained before:

$$f_*\alpha_1 = f_*\alpha_2 = \gamma, \quad f_*\beta_1 = f_*\beta_2 = \delta, \quad f'_*\alpha_1 = -f'_*\alpha_2 = \gamma', \quad f'_*\beta_1 = -f'_*\beta_2 = \delta'.$$

For non-zero holomorphic 1-forms $\omega = \frac{\mathrm{d}x}{y}$ on $E = \{y^2 = (x-1)(x-a^2)(x-b^2)\}$ and $\omega' = \frac{\mathrm{d}x}{y}$ on $E' = \{y^2 = (x-1)\left(x-\frac{1}{a^2}\right)\left(x-\frac{1}{b^2}\right)\}$, due to formulae of f, f' in (3.3), we have $f^*\omega = 2\frac{x\mathrm{d}x}{y} = 2\omega_2$ and $f'^*\omega' = 2ab\mathrm{i}\frac{\mathrm{d}x}{y} = (2ab\mathrm{i})\omega_1$. Combining with above:

$$\int_{\alpha_1}\omega_1 = -\int_{\alpha_2}\omega_1 = \frac{1}{2ab\mathrm{i}}\int_{\gamma'}\omega', \quad \int_{\beta_1}\omega_1 = -\int_{\beta_2}\omega_1 = \frac{1}{2ab\mathrm{i}}\int_{\delta'}\omega',$$
$$\int_{\alpha_1}\omega_2 = \int_{\alpha_2}\omega_2 = \frac{1}{2}\int_{\gamma}\omega, \quad \int_{\beta_1}\omega_2 = \int_{\beta_2}\omega_2 = \frac{1}{2}\int_{\delta}\omega.$$

Plugging in $Z = \begin{bmatrix}\int_{\alpha_1}\omega_1 & \int_{\alpha_2}\omega_1 \\ \int_{\alpha_1}\omega_2 & \int_{\alpha_2}\omega_2\end{bmatrix}^{-1}\begin{bmatrix}\int_{\beta_1}\omega_1 & \int_{\beta_2}\omega_1 \\ \int_{\beta_1}\omega_2 & \int_{\beta_2}\omega_2\end{bmatrix}$:

$$Z = \begin{bmatrix}\frac{1}{2ab\mathrm{i}}\int_{\gamma'}\omega' & -\frac{1}{2ab\mathrm{i}}\int_{\gamma'}\omega' \\ \frac{1}{2}\int_{\gamma}\omega & \frac{1}{2}\int_{\gamma}\omega\end{bmatrix}^{-1}\begin{bmatrix}\frac{1}{2ab\mathrm{i}}\int_{\delta'}\omega' & -\frac{1}{2ab\mathrm{i}}\int_{\delta'}\omega' \\ \frac{1}{2}\int_{\delta}\omega & \frac{1}{2}\int_{\delta}\omega\end{bmatrix} = \begin{bmatrix}\frac{\tau+\tau'}{2} & \frac{\tau-\tau'}{2} \\ \frac{\tau-\tau'}{2} & \frac{\tau+\tau'}{2}\end{bmatrix},$$

where $\tau := \frac{\int_\delta \omega}{\int_\gamma \omega}$ and $\tau' := \frac{\int_{\delta'}\omega'}{\int_{\gamma'}\omega'}$ from the upper half plane are periods for E and E'. We have shown:

Proposition 3.4. *For $a, b \in \mathbb{C} - \{0, \pm 1\}$ with $a \neq \pm b$, there are periods τ, τ' in the upper half plane for elliptic curves $E = \{y^2 = (x-1)(x-a^2)(x-b^2)\}$ and $E' = \left\{y^2 = (x-1)\left(x - \frac{1}{a^2}\right)\left(x - \frac{1}{b^2}\right)\right\}$ respectively, such that the matrix $\begin{bmatrix} \frac{\tau+\tau'}{2} & \frac{\tau-\tau'}{2} \\ \frac{\tau-\tau'}{2} & \frac{\tau+\tau'}{2} \end{bmatrix}$ from the Siegel upper half plane determines a period matrix for the genus-2 curve $C = \{y^2 = (x^2-1)(x^2-a^2)(x^2-b^2)\}$.*

Note that the period matrix above determines the Jacobian along with the theta divisor, i.e. one gets $J(C)$ as a principally polarized abelian variety.

Remark 3.5. In Section 2 we utilized the q-expansion approximation to find out a Legendre form obtained from solving equations corresponds to which of the periods we know beforehand. In principle, the same procedure can be carried out in the genus 2 case to verify whether the period matrix we got is the right choice for the hyperelliptic equation in hand, although the calculations are extremely cumbersome. Instead of j-invariant of elliptic curves, one should deal with three invariants of the Rosenhain form derived from the work of Igusa [6] and then write down first few terms of their expansion as Siegel modular forms of genus 2. This is the content of another paper by Igusa [7].

Remark 3.6. In practice, we take elliptic curves E and E' in Proposition 3.4 to have complex multiplication so that we know precisely what the periods τ, τ' are. One can also use a theorem due to Shioda and Mitani in [15] asserting that any abelian surface isogenous to a product of elliptic curves with complex multiplication, is itself isomorphic to a product of elliptic curves. So in the situation that E and E' are non-isogenous and both with complex multiplication, by the universal property of the Jacobian, degree-2 morphisms $f, f' : C \to E, E'$ induce a degree-4 isogeny $J(C) = \tilde{E} \times \tilde{E}' \to E \times E'$ that is given by components $\tilde{E} \to E$ and $\tilde{E}' \to E'$ which are degree-2 isogenies of elliptic curves. Using Theorem 2.1, we get all possible choices for the periods of $\tilde{E}$ and $\tilde{E}'$ in terms of τ and τ', respectively (and so period matrices for the torus $J(C)$) along with Legendre forms for these elliptic curves and thus a projective embedding of $J(C)$ via $\mathbb{CP}^2 \times \mathbb{CP}^2 \overset{\text{Segre map}}{\hookrightarrow} \mathbb{CP}^8$. With the help of Theorem 2.2, this idea can be generalized when we have morphisms of degrees 2 or 3 from C onto two non-isogenous elliptic curves with complex multiplication.

Example 3.7. Let us apply this method to $C = \left\{y^2 = (x^2-1)(x^2-a^2)\left(x^2 - \frac{1}{a^2}\right)\right\}$ where $a = \frac{1}{b}$ and elliptic curves E, E' in (3.3) are identical. The homology bases in Figures 2, 3 are related by $\gamma' = \gamma$ and $\delta' = \delta - \gamma$. So (following the same notations as before) $\tau' = \frac{\int_{\delta'} \omega}{\int_{\gamma'} \omega}$ is just $\frac{\int_{\delta} \omega}{\int_{\gamma} \omega} - 1 = \tau - 1$. Therefore, Proposition 3.4 states that $Z = \begin{bmatrix} \tau - \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \tau - \frac{1}{2} \end{bmatrix}$ is a normalized period matrix for C provided that τ is some suitable period of E in the upper half plane $\mathbb{H}$.

Let us analyze a specific case: the Bolza surface $y^2 = x^5 - x$ can be converted to the form of (3.2) after applying an appropriate Möbius transformation to roots of $x^5 - x$ along with ∞ in order to get six points in the form of $\pm 1, \pm a, \pm b$. By applying $z \mapsto \frac{z - \mathrm{e}^{\frac{\pi \mathrm{i}}{4}}}{z + \mathrm{e}^{\frac{\pi \mathrm{i}}{4}}}$, we arrive at $a^2 = \frac{1}{b^2} = \left(\frac{1+\mathrm{e}^{\frac{\pi \mathrm{i}}{4}}}{1-\mathrm{e}^{\frac{\pi \mathrm{i}}{4}}}\right)^2 = -3 - 2\sqrt{2}$ and $\lambda = -a^2 = 3 + 2\sqrt{2}$ in a Legendre form for the elliptic curve $E = E' = \left\{y^2 = (x-1)(x-a^2)\left(x - \frac{1}{a^2}\right)\right\}$. Using what has been done in Example 2.10, $\sqrt{2}\mathrm{i} \in \mathbb{H}$ is a period. So τ and $\tau' = \tau - 1$ both belong to the $\mathrm{SL}_2(\mathbb{Z})$-orbit of $\sqrt{2}\mathrm{i}$ while the latter is the ratio:

$$\frac{\int_{-3+2\sqrt{2}}^{1} \frac{\mathrm{d}x}{\sqrt{(x-1)(x+3-2\sqrt{2})(x+3+2\sqrt{2})}}}{\int_{-3-2\sqrt{2}}^{-3+2\sqrt{2}} \frac{\mathrm{d}x}{\sqrt{(x-1)(x+3-2\sqrt{2})(x+3+2\sqrt{2})}}} \approx 0.7071\mathrm{i} \approx \frac{\sqrt{2}}{2}\mathrm{i}.$$

We conclude that $\tau' = \frac{\sqrt{2}\mathrm{i}}{2}, \tau = 1 + \frac{\sqrt{2}\mathrm{i}}{2}$. Plugging them in the formula we derived for Z results in $Z = \begin{bmatrix} \frac{1+\sqrt{2}\mathrm{i}}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1+\sqrt{2}\mathrm{i}}{2} \end{bmatrix}$ as a normalized period matrix of the Bolza curve.

4. **Covers with a unique ramification point**

Let $f : C \to E = \{y^2 = x(x-1)(x-\lambda)\}$ be a degree-n morphism from the hyperelliptic curve C of genus $g > 1$ onto the elliptic curve E with exactly one ramification point, namely p. The Riemann-Hurwitz formula indicates that the multiplicity of p is $2g-1$. We may assume that $f(p)$ is the point at infinity and $p \mapsto \infty$ under the ramified 2-fold cover $C \to \mathbb{CP}^1$.[5] Furthermore, suppose that f respects the hyperelliptic involutions. So once more we have a commutative diagram:

$(\star\ \star\ \star\star)$

$$\begin{array}{ccc} C & \xrightarrow{f} & E \\ \downarrow & & \downarrow{\scriptstyle (x,y)\mapsto x} \\ \mathbb{CP}^1 & \xrightarrow{h} & \mathbb{CP}^1 \end{array}$$

By diagram chasing, the degree-n map $h : \mathbb{CP}^1 \to \mathbb{CP}^1$ takes the value ∞ at the point ∞ with multiplicity $2g-1$ and all of its other ramification points are of multiplicity two. Moreover, its critical values are among those of the right column, i.e. $0, 1, \lambda, \infty$, and the number of its non-critical points over these

[5] In what follows, ∞ is a critical value of $C \to \mathbb{CP}^1$ and hence p must be a Weierstrass point of the curve C. This is justified by looking at the divisor of $f^*\omega$ for an arbitrary $0 \neq \omega \in \Omega^1(E)$ which is $(2g-2)p$. Hence this non-zero holomorphic 1-form on the genus-g curve C vanishes at p with multiplicity $2g - 2 \geq g$. Extending $f^*\omega$ to a basis for the g-dimensional space $\Omega^1(C)$, it follows that the Wronskian of this basis vanishes at p and thus p is a Weierstrass point.

four values coincides with the number of critical values of the left column other than ∞ which is $2g+1$. This implies that there are exactly $\frac{4n-(2g+1)-(2g-1)}{2} = 2(n-g)$ points of multiplicity two in $h^{-1}(\{0,1,\lambda,\infty\})$. In summary, the only constraints on h are:

- The function $h : \mathbb{CP}^1 \to \mathbb{CP}^1$ is of degree n and maps ∞ to ∞ with multiplicity $2g-1$. All other ramification points of h are of multiplicity two.
- The branch values of h belong to the set $\{0,1,\lambda,\infty\}$.
- Let l_i denote the number of ramification points of multiplicity two above $i \in \{0,1,\lambda,\infty\}$. Then $l_0, l_1, l_\lambda \leq \lfloor \frac{n}{2} \rfloor$, $l_\infty \leq \lfloor \frac{n+1}{2} \rfloor - g$ and $l_0 + l_1 + l_\lambda + l_\infty = 2(n-g)$.[6]

Such a function always determines a degree-n cover $f : C \to E$ with the desired property: these conditions imply that the number of non-critical points of h over the set $\{0,1,\lambda,\infty\}$ is $2g+1$. Denoting them by $\lambda_i\,(1 \leq i \leq 2g+1)$, $\frac{h(x)(h(x)-1)(h(x)-\lambda)}{\prod_{i=1}^{2g+1}(x-\lambda_i)}$ lies in $\mathbb{C}(x)^2$ and taking $g(x)$ to be one of its square roots, $(x,y) \mapsto (h(x), yg(x))$ is an explicit formula of a degree-n morphism from the hyperelliptic curve $C = \{y^2 = \prod_{i=1}^{2g+1}(x-\lambda_i)\}$ of genus g onto the elliptic curve $E = \{y^2 = x(x-1)(x-\lambda)\}$ whose only ramification point is the point at infinity.

Assuming

$$h(x) = \frac{k\prod_{i=1}^{l_0}(x-\alpha_i)^2 . \prod_{j=1}^{n-2l_0}(x-\alpha'_j)}{\prod_{i=1}^{l_\infty}(x-\beta_i)^2 . \prod_{j=1}^{n-2l_\infty-2g+1}(x-\beta'_j)},$$

one may obtain these functions by solving systems of equations similar to those of Theorem 2.7. Equations come from equating coefficients of the identities in (4.1) and unknowns are pairwise distinct complex numbers α_i's, α'_j's, β_i's, β'_j's, γ_i's, γ'_j's, δ_i's, δ'_j's along with $\lambda \in \mathbb{C} - \{0,1\}$ and $k \neq 0$.

$$\begin{cases} k\prod_{i=1}^{l_0}(x-\alpha_i)^2 . \prod_{j=1}^{n-2l_0}(x-\alpha'_j) - \prod_{i=1}^{l_\infty}(x-\beta_i)^2 . \prod_{j=1}^{n-2l_\infty-2g+1}(x-\beta'_j) \\ = k\prod_{i=1}^{l_1}(x-\gamma_i)^2 . \prod_{j=1}^{n-2l_1}(x-\gamma'_j), \\ k\prod_{i=1}^{l_0}(x-\alpha_i)^2 . \prod_{j=1}^{n-2l_0}(x-\alpha'_j) - \lambda\prod_{i=1}^{l_\infty}(x-\beta_i)^2 . \prod_{j=1}^{n-2l_\infty-2g+1}(x-\beta'_j) \\ = k\prod_{i=1}^{l_\lambda}(x-\delta_i)^2 . \prod_{j=1}^{n-2l_\lambda}(x-\delta'_j). \end{cases} \tag{4.1}$$

[6] Note that in the main example of [12] where $n=5$, $g=2$ and $\lambda=-1$, l_∞ vanishes whereas all the other parameters l_0, l_1, l_λ are 2

The geometric point of view enables us to formulate a necessary and sufficient combinatorial condition for the existence of a solution to this complicated algebraic system: thinking of the monodromy of h, the only constraint on l_i's is the existence of permutations $\tau_1, \tau_2, \tau_\lambda, \tau_\infty \in \mathrm{S}_n$ with $\tau_0\tau_1\tau_\lambda\tau_\infty = \mathrm{id}$ that generate a transitive subgroup of S_n and furthermore τ_∞ is a product of l_∞ transpositions and a $2g-1$-cycle which are disjoint while any other τ_i decomposes to l_i disjoint transpositions. The number of equations is $2n$ while there are $2n+3$ unknowns. But since the only point of the domain fixed in our discussion was ∞, there are two degrees of freedom left which indicates that number of unknowns can be reduced to $2n+1$. So in the case that the combinatorial condition is satisfied, we expect to get a 1-parameter family $\left\{f_t : C_t \to E_{\lambda(t)}\right\}_t$ of totally ramified maps as solutions to this system. Considering the action of $\mathrm{Gal}\left(\frac{\mathbb{C}}{\mathbb{Q}(\lambda)}\right)$ on solutions $h : \mathbb{CP}^1 \to \mathbb{CP}^1$ (where λ is fixed) shows that any such a meromorphic function, and hence any cover of the elliptic curve E_λ with a unique ramification point has a model over the field $\overline{\mathbb{Q}(\lambda)}$. In particular, setting two of unknowns to be $0, 1$, solutions of (4.1) are defined over a finite extension of $\mathbb{Q}(\lambda)$.

Next, we try to construct examples of such h's. First, assuming that the function h is also Belyi, that is $l_\lambda = 0$, in the corresponding dessin all vertices are of degree at most 2 except the one corresponding to the face associated with the pole ∞ which is of degree $2g-1$. The only dessin on the Riemann sphere with these properties is the path with $n = 2g-1$ edges. It is a standard fact that the dessin of $x \mapsto \frac{T_m(x)+1}{2}$, where $T_m(x)$ is the mth Chebyshev polynomial, is the path with m edges. So we derive the following proposition. Compare with [11, Theorem 3.2].

Proposition 4.1. *For any $g > 1$ and $t \neq \pm 1$ the genus-g curve $y^2 = (x^2-1)(T_{2g-1}(x) - t)$ admits a morphism of degree $2g-1$ to the elliptic curve $y^2 = (x^2-1)(x-t)$ given by*

$$(x, y) \mapsto \left(T_{2g-1}(x), 2^{2g-2} y \prod_{k=1}^{2g-2} \left(x - \cos\frac{\pi k}{2g-1}\right)\right).$$

The unique ramification point of this map is the point at infinity.

Let us finish this section with another special case where $n = 4, g = 2$. The only possible choice for l_i's is $l_\infty = 0$ and among l_0, l_1, l_λ, one of them is 2 and the remaining parameters are 1, say $l_0 = 2, l_1 = l_\lambda = 1$. Consequently, the degree-4 meromorphic function $h : \mathbb{CP}^1 \to \mathbb{CP}^1$ take ∞ to ∞ with multiplicity three and possesses two points of multiplicity two above 0 which, by a linear change of coordinates, may be assumed to be $0, 1$. This amounts to $h(x) = \frac{k(x^2-x)^2}{x-t}$ ($t \neq 0, 1$). Moreover, h has a single point of multiplicity two above either of values 1 or λ. Thus, the numerators of $h(x)-1$ and $h(x)-\lambda$ have multiple roots. But μ is a multiple root of either of polynomials $k(x^2-x)^2-(x-t)$ or $k(x^2-x)^2-\lambda(x-t)$

only if $\frac{\mu^2-\mu}{2(2\mu-1)} = \mu - t$. This shows that the multiple roots $\mu_1(t)$, $\mu_2(t)$ of previous polynomials are the roots of $3\mu^2 - (4t+1)\mu + 2t = 0$. Plugging $\mu_1(t)$ in the first polynomial results in a description $k = k(t)$ of k in terms of t and the fact that $\mu = \mu_2(t)$ satisfies the equation $k(t)(\mu^2-\mu)^2 - \lambda(\mu - t) = 0$ yields an expression in the form of $\lambda(t)$ for λ. To obtain the hyperelliptic equation for C, one should compute the degree $2g+1 = 5$ polynomial whose roots are non-critical points of $h(x) = \frac{k(t)(x^2-x)^2}{x-t}$ above $0, 1, \lambda(t), \infty$. Over ∞ we only have t while over critical values 1, $\lambda(t)$ the roots are those of the quadratic polynomials:

$$\frac{k(t)(x^2-x)^2 - (x-t)}{(x-\mu_1(t))^2} = k(t)\left(x^2 + (2\mu_1(t)-2)x + \frac{t}{k(t)\mu_1(t)^2}\right),$$
$$\frac{k(t)(x^2-x)^2 - \lambda(t)(x-t)}{(x-\mu_2(t))^2} = k(t)\left(x^2 + (2\mu_2(t)-2)x + \frac{t\lambda(t)}{k(t)\mu_2(t)^2}\right).$$

We deduce that:

Proposition 4.2. *For any $\beta \in \mathbb{C} - \{0,1\}$, the following is an equation for a 4-fold branched cover of an elliptic curve by a curve of genus 2 with precisely one ramification point which is the point at infinity.*

$$\begin{cases} \left\{y^2 = (x-t)\left(x^2 + (2\mu_1(t)-2)x + \frac{t}{k(t)\mu_1(t)^2}\right)\left(x^2 + (2\mu_2(t)-2)x + \frac{t\lambda(t)}{k(t)\mu_2(t)^2}\right)\right\} \\ \to \left\{y^2 = x(x-1)(x-\lambda(t))\right\} \\ (x,y) \mapsto \left(\frac{k(t)(x^2-x)^2}{x-t}, \frac{k(t)^{\frac{3}{2}}(x^2-x)(3x^2-(4t+1)x+2t)}{3(x-t)^2}y\right) \end{cases},$$

where $\mu_1(t)$, $\mu_2(t)$ are the roots of $3\mu^2 - (4t+1)\mu + 2t = 0$ and

$$k(t) = \frac{\mu_1(t) - t}{(\mu_1(t)^2 - \mu_1(t))^2}, \quad \lambda(t) = \frac{k(t)(\mu_2(t)^2 - \mu_2(t))^2}{\mu_2(t) - t}.$$

5. An example of a non-hyperelliptic case

In all of examples worked out so far, *descending* calculations to a simpler curve and then to a system of equations was done by factoring through hyperelliptic involutions. But this idea can still be pursued when we have other normal forms for the family of curves in hand. We devote this last brief section to an example of this kind.

A Riemann surface C of genus 3 is either hyperelliptic and thus determined by a non-degenerate binary octavic, or, is non-hyperelliptic and therefore the canonical embedding maps it to a smooth plane curve of degree 4 such that isomorphism translates to projective equivalence of plane quartics. So one can study the moduli spaces of hyperelliptic and non-hyperelliptic Riemann surfaces of genus 3 by computing invariants for binary octavics and ternary quartics, respectively. See [14] and [4] for such treatments.

We are going to look at a Riemann surface C of genus 3 and a morphism

$f : C \to \mathbb{CP}^1$ of degree 3 (which is the gonality in this genus). Having the positions of critical values and the monodromy in hand, can one *descend* writing an equation for f to solving some system of equations?

Since C has a Weierstrass point, we may assume that f has a ramification point of multiplicity three. Denoting the set of ramification values whose fibers has a ramification point of multiplicity two (respectively, three) by $\{p_1, \dots, p_u\}$ (respectively, $\{q_1, \dots, q_v\}$), possible choices for (u, v) are $(8, 1)$, $(6, 2)$, $(4, 3)$, $(2, 4)$, $(0, 5)$. The monodromy (which determines the isomorphism class of $f : C \to \mathbb{CP}^1$ once the set of branch values $\{p_1, \dots, p_u, q_1, \dots, q_v\}$ is fixed) is specified by a u-tuple $\theta^u = (\theta_1, \dots, \theta_u)$ of transpositions and a v-tuple $\tau^v = (\tau_1, \dots, \tau_v)$ of 3-cycles where components come from S_3 and satisfy $\theta_1 \dots \theta_u \tau_1 \dots \tau_v = \mathrm{id}$. Let us denote the Hurwitz space of isomorphism classes of degree-3 maps $f : C \to \mathbb{CP}^1$ of monodromy type (θ^u, τ^v) with the ordering $(p_1, \dots, p_u, q_1, \dots, q_v)$ on their branch values by $\mathcal{H}_{(\theta^u, \tau^v)}$. By the same geometric point of view that the isomorphism class of f (in particular, the complex structure of C) is uniquely determined by the position of branch values and the monodromy, we can describe these spaces as quotients of an affine open set by the action of some finite group, just like what we did for moduli spaces $\mathcal{M}_{1,1}$ and $\mathcal{M}_2$ in (2.1) and (3.1). Here, one should think of any $\mathcal{H}_{(\theta^u, \tau^v)}$ as ordered pairs $((p_1, \dots, p_u), (q_1, \dots, q_v)) \in (\mathbb{CP}^1)^u \times (\mathbb{CP}^1)^v - \Delta$ (Δ: the divisor of points with repeated components) modulo the component-wise action of the Möbius transformations group. We can rigidify these sets by assuming $0, 1, \infty$ are among these $u + v$ points and then one gets action of a finite group on some domain in $\mathbb{C}^{u+v-3}$. Again, by invoking the invariant theory of finite groups, computing invariants for this action gives us the coordinate ring of the affine variety $\mathcal{H}_{(\theta^u, \tau^v)}$ (and perhaps its equations if one can calculate the syzygies). These actions are summarized in Table 1. Indeed, there are cases where, precisely like the action of S_5 in Remark 3.1, the action can be projectivized to a linear action on a polynomial ring generated by pseudo-reflections and so computing invariants is not difficult because the Chevalley-Shephard-Todd theorem implies that there are no syzygies.

The space $\mathcal{H}_{(\theta^u, \tau^v)}$ is of dimension $u + v - 3$ and so is of "full moduli dimension", i.e. the same dimension as that of the moduli space $\mathcal{M}_3$, when $(u, v) = (8, 1)$. Let us address our computational problem in this generic case: having sets $\{p_1, \dots, p_8\}$, $\{q_1\}$ in hand, can one specify an equation for a degree-3 $f : C \to \mathbb{CP}^1$ whose ramification points are precisely a point of multiplicity three above q_1 and one point of multiplicity two above each p_i? Kill three degrees of freedom by setting $q_1 = \infty$, $p_7 = 0, p_8 = 1$. The paper [13] contains an equation for a non-hyperelliptic genus-3 curve that depends on $\dim \mathcal{M}_3 = 6$ parameters and is equipped with a degree-3 meromorphic function with a triple

pole. This is given by a smooth curve of degree 4 in $\mathbb{CP}^2$ with the affine equation:

$$y^3(x+a)+y^2(bx+c)+y(dx^2+ex)+x^3+fx^2+x=0, \tag{5.1}$$

and with the meromorphic function $(x,y)\mapsto x$ which for generic values of a,b,c,d,e,f has a unique point of multiplicity three (a triple pole) at one of points at infinity. The discriminant of (5.1), regarded as an element of $\mathbb{C}[a,b,c,d,e,f,x][y]$, is:

$$\begin{aligned}&(bx+c)^2(dx^2+ex)^2-4(x+a)(dx^2+ex)^3-4(bx+c)^3(x^3+fx^2+x)\\&-27(x+a)^2(x^3+fx^2+x)^2+18(x+a)(bx+c)(dx^2+ex)(x^3+fx^2+x).\end{aligned}$$

This expression, considered as an element of $\mathbb{C}[a,b,c,d,e,f][x]$, is of degree 8 and with the leading coefficient -27. Equating this with the known polynomial $-27x(x-1)\prod_{i=1}^{6}(x-p_i)$ of x and then solving for a,b,c,d,e,f yields the desired example. Once more we *descend* to a system obtained from equality of two polynomials.

TABLE 1. Realizing the Hurwitz space $\mathcal{H}_{\theta^u,\tau^v}$ as $(\mathbb{C}-\{0,1\})^{u+v-3}-\Delta$ modulo a finite group that is the subgroup of those elements $\beta\in\mathrm{Aut}\left(\mathbb{CP}^1\right)$ for which $A\cap\{0,1,\infty\}=\beta(A)\cap\{0,1,\infty\}$ for any of subsets A appeared in the second column. In each row, σ_i comes from some suitable transposition in the S_n-component and γ is induced by the generator of the $\mathbb{Z}_2$-component. In the first, second and fourth rows, the action of S_n can be projectivized to an action which satisfies the conditions of Chevalley-Shephard-Todd theorem.

(u,v)	branch points	group	generators of the action
$(8,1)$	$\{0,1,z_1,\dots,z_6\},\{\infty\}$	S_8	$\begin{cases}\sigma_i:(z_1,\dots,z_6)\mapsto\left(\frac{z_1}{z_i},\dots,\frac{z_{i-1}}{z_i},\frac{1}{z_i},\frac{z_{i+1}}{z_i},\dots,\frac{z_6}{z_i}\right)\\ \sigma_7:(z_1,\dots,z_6)\mapsto(1-z_1,\dots,1-z_6)\end{cases}$
$(6,2)$	$\{1,z_1,\dots,z_5\},\{0,\infty\}$	$\mathrm{S}_6\times\mathbb{Z}_2$	$\begin{cases}\sigma_i:(z_1,\dots,z_5)\mapsto\left(\frac{z_1}{z_i},\dots,\frac{z_{i-1}}{z_i},\frac{1}{z_i},\frac{z_{i+1}}{z_i},\dots,\frac{z_5}{z_i}\right)\\ \gamma:(z_1,\dots,z_5)\mapsto\left(\frac{1}{z_1},\dots,\frac{1}{z_5}\right)\end{cases}$
$(4,3)$	$\{z_1,\dots,z_4\},\{0,1,\infty\}$	S_3	$\begin{cases}\sigma_1:(z_1,\dots,z_4)\mapsto\left(\frac{1}{z_1},\dots,\frac{1}{z_4}\right)\\ \sigma_2:(z_1,\dots,z_4)\mapsto(1-z_1,\dots,1-z_4)\end{cases}$
$(2,4)$	$\{0,\infty\},\{1,z_1,z_2,z_3\}$	$\mathrm{S}_4\times\mathbb{Z}_2$	$\begin{cases}\sigma_i:(z_1,z_2,z_3)\mapsto\left(\frac{z_1}{z_i},\dots,\frac{z_{i-1}}{z_i},\frac{1}{z_i},\frac{z_{i+1}}{z_i},\dots,\frac{z_3}{z_i}\right)\\ \gamma:(z_1,z_2,z_3)\mapsto\left(\frac{1}{z_1},\frac{1}{z_2},\frac{1}{z_3}\right)\end{cases}$
$(0,5)$	$\emptyset,\{0,1,\infty,z_1,z_2\}$	S_5	$\begin{cases}\sigma_1:(z_1,z_2)\mapsto\left(\frac{1}{z_1},\frac{z_2}{z_1}\right)\\ \sigma_2:(z_1,z_2)\mapsto\left(\frac{z_1}{z_2},\frac{1}{z_2}\right)\\ \sigma_3:(z_1,z_2)\mapsto\left(\frac{1}{z_1},\frac{1}{z_2}\right)\\ \sigma_4:(z_1,z_2)\mapsto(1-z_1,1-z_2)\end{cases}$

Acknowledgements

This work is part of author's Ph.D. thesis at Sharif University of Technology under co-advising of H. Fanai and M. Shahshahani.

References

[1] C. Birkenhake and H. Lange, Complex Abelian Varieties, Grundlehren Math. Wiss. 302, Springer-Verlag, 2nd edition, Berlin-Heidelberg, 2004.

[2] O. Bolza, On binary sextics with linear transformations into themselves, *Amer. J. Math.* **10** (1887), no. 1, 47–70.

[3] H. Cohen, A Course in Computational Algebraic Number Theory, Grad. Texts in Math. 138, Springer-Verlag, Berlin-Heidelberg, 1993.

[4] J. Dixmier, On the projective invariants of quartic plane curves, *Adv. Math.* **64** (1987), no. 3, 279–304.

[5] E. Girondo and G. González-Diez, On complex curves and complex surfaces defined over number fields, in: Teichmüller Theory and Moduli Problem, pp. 247–280, Ramanujan Math. Soc. Lect. Notes Ser. 10, Ramanujan Math. Soc. Mysore, 2010.

[6] J.I. Igusa, Arithmetic variety of moduli for genus two, *Ann. of Math. (2)* **72** (1960), no. 3, 612–649.

[7] J.I. Igusa, On Siegel modular forms of genus two, *Amer. J. Math.* **84** (1962), no. 1, 175–200.

[8] A. Kamalinejad and M. Shahshahani, On computations with dessins d'enfants, *Math. Comp.* **86** (2017), no. 303, 419–436.

[9] V. Krishnamoorthy, T. Shaska and H. Völklein, Invariants of binary forms, in: Progress in Galois Theory, pp. 101–122, Dev. Math. 12, Springer, New York, 2005.

[10] J. Milnor, Dynamics in One Complex Variable, Ann. of Math. Stud. 160, Princeton Univ. Press, 3rd edition, Princeton, 2006.

[11] S. Rubinstein-Salzedo, Covers of elliptic curves with unique, totally ramified branch points, *Math. Nachr.* **286** (2013), no. 14-15, 1530–1536.

[12] S. Rubinstein-Salzedo, Period computations for covers of elliptic curves, *Math. Comp.* **83** (2014), no. 289, 2455–2470.

[13] T. Shaska and J. Thompson, On the generic curve of genus 3, in: Affine Algebraic Geometry, pp. 233–243, Contemp. Math. 369, Amer. Math. Soc. Providence, RI, 2005.

[14] T. Shioda, On the graded ring of invariants of binary octavics, *Amer. J. Math.* **89** (1967), no. 4, 1022–1046.

[15] T. Shioda and N. Mitani, Singular abelian surfaces and binary quadratic forms, in: Classification of Algebraic Varieties and Compact Complex Manifolds, pp. 259–287, Lecture Notes in Math. 412, Springer, Berlin, 1974.

[16] B. Sturmfels, Algorithms in Invariant Theory, Texts Monogr. Symbol. Comput., Springer-Verlag, 2nd edition, Wien, 2008.

(Khashayar Filom) Department of Mathematical Sciences, Sharif University of Technology, Tehran, Iran.

E-mail address: filom@mehr.sharif.ir