Decomposition of some Jacobian varieties of dimension 3

Lubjana Beshaj and Tony Shaska

Department of Mathematics and Statistics
Oakland University
Rochester, Michigan 48309-4401

Abstract. We discover a family of dimension 3 Jacobian varieties which decompose into three elliptic curves (E, E_1, E_2). Such family does not fall into the well-known cases where such decomposition is induced by the endomorphisms of the Jacobian variety. It is a 2-dimensional subvariety of the hyperelliptic moduli $\mathcal{H}_3$. For any given moduli point $\mathfrak{p} \in \mathcal{H}_3$ we determine explicitly if the corresponding genus 3 curve $\mathcal{X}$ belongs or not to such family. When it does, we can determine explicitly components E, E_1, and E_2 in terms of the absolute invariants $t_1, \dots, t_6$ of binary octavics as in [12].

1 Introduction

There are some problems in classical mathematics which can be solved only through symbolic computational methods. The problem in which this work is focused lies within this category and continues previous work in [3–8, 11, 13, 14]. Whether methods in artificial intelligence, machine learning etc can be improved to generalize such computational methods remains to be seen.

Let $\mathcal{M}_g$ denote the moduli space of genus $g \geq 2$ algebraic curves defined over an algebraically closed field k and $\mathcal{H}_g$ the hyperelliptic submoduli in $\mathcal{M}_g$. The sublocus of genus g hyperelliptic curves with an elliptic involution is a g-dimensional subvariety of $\mathcal{H}_g$. For $g = 2$ this space is denoted by $\mathcal{L}_2$ and studied in [6] and for $g = 3$ is denoted by $\mathcal{S}_2$ and is computed and discussed in detail in [10]. In both cases, a birational parametrization of these spaces is found via *dihedral invariants*; see [6, 12]. We denote the parameters for $\mathcal{L}_2$ by u, v and for $\mathcal{S}_2$ by $\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4$ as in respective papers. Hence, for the case $g = 3$ there is a birational map $\phi : \mathcal{S}_2 \longrightarrow \mathcal{H}_3$ such that $\phi : (\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4) = (t_1, \dots, t_6)$, where $t_1, \dots, t_6$ are the absolute invariants as defined in [12].

The dihedral invariants $\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4$ provide a birational parametrization of the locus $\mathcal{S}_2$. Hence, a generic curve in $\mathcal{S}_2$ is uniquely determined by the corresponding triple $(\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4)$. Let $\mathcal{X}$ be a curve in the locus $\mathcal{S}_2$. Then there is a degree 2 map $f_1 : \mathcal{X} \to E$ for some elliptic curve E. Thus, the Jacobian of $\mathcal{X}$ splits as Jac $(\mathcal{X}) \cong E \times A$, where A is a genus 2 Jacobian. Hence, there is a map $f_2 : \mathcal{X} \to C$ for some genus 2 curve C. The equations of $\mathcal{X}$, E, and C are given in Thm. 2. For any fixed curve $\mathcal{X} \in \mathcal{S}_2$, the subcovers E and C are uniquely determined in terms of the invariants $\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4$.

In section three we give the splitting of the Jacobians for all genus 3 algebraic curves, when this splitting is induced by automorphisms. The proof requires the Poincare duality and some basic group theory.

In this paper, we are mostly interested in the case when the Jacobian of the genus two curve C also splits. The Jacobian of C can split as an (n, n)-structure. The loci of such genus 2 curves with $(3, 3)$-split or $(5, 5)$-split have been studied respectively in [6]. We focus on the case when the Jacobian of C is $(2, 2)$-split, which corresponds to the case when the Klein 4-group $V_4 \hookrightarrow \text{Aut}\,(C)$. Hence, Jac $\mathcal{X}$ splits completely as a product of three elliptic curves. We say that Jac $\mathcal{X}$ is $(2, 4, 4)$-split.

Let the locus of genus 3 hyperelliptic curves whose Jacobian is $(2, 4, 4)$-split be denoted by $\mathcal{T}$. Then, there is a rational map $\psi : \mathcal{T} \to \mathcal{L}_2$ such that $\psi(\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4) = (u, v)$, which has degree 70 and can be explicitly computed, even though the rational expressions of u and v in terms of $\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4$ are quite large.

There are three components of $\mathcal{T}$ which we denote them by $\mathcal{T}_i$, $i = 1, 2, 3$. Two of these components are well known and the correspond to the cases when V_4 is embedded in the reduced automorphism group of $\mathcal{X}$. These cases correspond to the singular locus of $\mathcal{S}_2$ and are precisely the locus $\det(\text{Jac}\,(\phi)) = 0$. This happens for all genus $g \geq 2$ as noted in [6]. The third component $\mathcal{T}_3$ is more interesting to us. It doesn't seem to have any group theoretic reason for this component to be there in the first place. We find the equation of this component it terms of the $\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4$ invariants. It is an equation $F_1(\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4) = 0$ as in Eq. (7). In this locus, the elliptic subfields of the genus two field $k(C)$ can be determined explicitly.

The main goal of this paper is to determine explicitly the family $\mathcal{T}_3$ of genus 3 curves and relations among its elliptic subcovers. We have the maps $\mathcal{T}_3 \xrightarrow{\psi} \mathcal{L}_2 \xrightarrow{\psi_0} k^2$, such that $\psi_0(\psi(\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4)) = (j_1, j_2)$, where $\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4$ satisfy Eq. (7) and u, v are given explicitly by Eq. (6) and Thm. (3) in [6]. The degree deg $\psi_0 = 2$ and deg $\psi = 70$.

Since $\mathcal{T}_3$ is a subvariety of $\mathcal{H}_3$ it would be desirable to express its equation in terms of a coordinate in $\mathcal{H}_3$. One can use the absolute invariants of the genus 3 hyperelliptic curves $t_1, \dots, t_6$ as defined in [12] and the expressions of $\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4$ in terms of these invariants as computed in [10].

Further, we focus our attention to the sublocus $\mathcal{V}$ of $\mathcal{L}_2$ such that the genus 2 field $k(C)$ has isomorphic elliptic subfields. Such locus was discovered in [6] and it is somewhat surprising. It does not rise from a family of genus two curves with a fixed automorphism group as other families, see [6] for details. Using this sublocus of $\mathcal{M}_2$ we discover a rather unusual embedding $\mathcal{M}_1 \hookrightarrow \mathcal{M}_2$ as noted in [6]. Let $\mathfrak{T} \subset \mathcal{T}_3 \subset \mathcal{H}_3$ be the subvariety of $\mathcal{T}_3$ obtained by adding the condition $j_1 = j_2$. Then, $\mathfrak{T}$ is a 1-dimensional variety defined by equations

$$\begin{cases} F_1(\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4) = 0 \\ F_2(\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4) = 0 \end{cases} \tag{1}$$

where F_2 is the discriminant of the quadratic polynomial roots of which are j-invariants j_1 and j_2; cf. Lemma 3. Hence, we have the maps $k \to \mathfrak{T} \hookrightarrow \mathcal{V} \hookrightarrow k$, such that $t \to (\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4) \to (u, v) \to j_1$.

Next we study whether the above maps are invertible. That would provide birational parameterizations for varieties $\mathcal{V}$ and $\mathfrak{T}$. The variety $\mathcal{V}$ is known to have a birational parametrization from Thm. (3) in [6]. The map can be inverted as $j \to (u, v) = \left(9 - \frac{j}{256}, 9\left(6 - \frac{j}{256}\right)\right)$; see [6] for details. The main computational task of this paper is to find a birational parametrization of $\mathfrak{T}$.

Given $(u, v) \in \mathcal{V}$ there is a unique (up to isomorphism) genus 2 curve C corresponding to this point in $\mathcal{V}$. From Lemma 3, every genus 2 curve can be written as in Eq. (11). Hence, there exists a triple $(\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4)$ corresponding to (u, v).

If $j \in \mathbb{Q}$, then the corresponding elliptic curve E_j is defined over $\mathbb{Q}$. From the above expressions we see that $u, v \in \mathbb{Q}$. Then, the corresponding genus two curve C has also minimal field of definition $\mathbb{Q}$. The same holds for $\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4$ and the genus 3 corresponding curve $\mathcal{X}$.

2 Decomposition of Jacobian varieties of dimension 3

Let $\mathcal{X}$ be a genus g algebraic curve with automorphism group $G := \mathrm{Aut}\,(\mathcal{X})$. Let $H \leq G$ such that $H = H_1 \cup \cdots \cup H_t$ where the subgroups $H_i \leq H$ satisfy $H_i \cap H_j = \{1\}$ for all $i \neq j$. Then,

$$\mathrm{Jac}\,^{t-1}(\mathcal{X}) \times \mathrm{Jac}\,^{|H|}(\mathcal{X}/H) \cong \mathrm{Jac}\,^{|H_1|}(\mathcal{X}/H_1) \times \cdots \times \mathrm{Jac}\,^{|H_t|}(\mathcal{X}/H_t)$$

The group H satisfying these conditions is called a group with partition. Elementary abelian p-groups, the projective linear groups $PSL_2(q)$, Frobenius groups, dihedral groups are all groups with partition.

Let $H_1, \dots, H_t \leq G$ be subgroups with $H_i \cdot H_j = H_j \cdot H_i$ for all $i, j \leq t$, and let g_{ij} denote the genus of the quotient curve $\mathcal{X}/(H_i \cdot H_j)$. Then, for $n_1, \dots, n_t \in \mathbb{Z}$ the conditions $\sum n_i n_j g_{ij} = 0$, and $\sum_{j=1}^t n_j g_{ij} = 0$, imply the isogeny relation

$$\prod_{n_i > 0} \mathrm{Jac}\,^{n_i}(\mathcal{X}/H_i) \cong \prod_{n_j < 0} \mathrm{Jac}\,^{|n_j|}(\mathcal{X}/H_j)$$

In particular, if $g_{ij} = 0$ for $2 \leq i < j \leq t$ and if $g = g_{\mathcal{X}/H_2} + \cdots + g_{\mathcal{X}/H_t}$, then

$$\mathrm{Jac}\,(\mathcal{X}) \cong \mathrm{Jac}\,(\mathcal{X}/H_2) \times \cdots \times \mathrm{Jac}\,(\mathcal{X}/H_t)$$

The reader can check [1, 2] for the proof of the above statements.

2.1 Non-hyperelliptic curves

We will use the above facts to decompose the Jacobians of genus 3 non-hyperelliptic curves. $\mathcal{X}$ denotes a genus 3 non-hyperelliptic curve unless otherwise stated and $\mathcal{X}_2$ denotes a genus 2 curve.

The group C_2 Then the curve $\mathcal{X}$ has an elliptic involution $\mathfrak{s} \in \text{Aut}\,(\mathcal{X})$. Hence, there is a Galois covering $\pi \colon \mathcal{X} \to \mathcal{X}/\langle \sigma \rangle =: E$. We can assume that this covering is maximal. The induced map $\pi^* : E \to \text{Jac}\,(\mathcal{X})$ is injective. Then, the kernel projection $\text{Jac}\,(\mathcal{X}) \to E$ is a dimension 2 abelian variety. Hence, there is a genus 2 curve $\mathcal{X}_2$ such that $\text{Jac}\,(\mathcal{X}_2) \cong E \times \text{Jac}\,(\mathcal{X}_2)$.

The Klein 4-group Next, we focus on the automorphism groups G such that $V_4 \hookrightarrow G$. In this case, there are three elliptic involutions in V_4, namely $\sigma, \tau, \sigma\tau$. Obviously they form a partition. Hence, the Jacobian of $\mathcal{X}$ is the product $\text{Jac}\,^2(\mathcal{X}) \cong E_1^2 \times E_2^2 \times E_3^2$ of three elliptic curves. By applying the Poincare duality we get $\text{Jac}\,(\mathcal{X}) \cong E_1 \times E_2 \times E_3$.

The dihedral group D_8 In this case, we have 5 involutions in G in 3 conjugacy classes. No conjugacy class has three involutions. Hence, we can pick three involutions such that two of them are conjugate to each other in G and all three of them generate V_4. Hence, $\text{Jac}\,(\mathcal{X}) \cong E_1^2 \times E_2$, for some elliptic curves E_1, E_2.

The symmetric group S_4 The Jacobian of such curves splits into a product of elliptic curves since $V_4 \hookrightarrow S_4$. Below we give a direct proof of this.

We know that there are 9 involutions in S_4, six of which are transpositions. The other three are product of two 2-cycles and we denote them by $\sigma_1, \sigma_2, \sigma_3$. Let H_1, H_2, H_3 denote the subgroups generated by $\sigma_1, \sigma_2, \sigma_3$. They generate V_4 and are all isomorphic in G. Hence, $\text{Jac}\,(\mathcal{X}) \cong E^3$, for some elliptic curve E.

The symmetric group S_3 We know from above that the Jacobian is a direct product of three elliptic curves. Here we will show that two of those elliptic curves are isomorphic. Let H_1, H_2, H_3 be the subgroups generated by transpositions and H_4 the subgroup of order 3. Then

$$\text{Jac}\,^3(\mathcal{X}) \cong E_1^2 \times E_2^2 \times E_3^2 \times \text{Jac}\,^3(\mathcal{Y})$$

for three elliptic curves E_1, E_2, E_3 fixed by involutions and a curve $\mathcal{Y}$ fixed by the element of order 3. Simply by counting the dimensions we have $\mathcal{Y}$ to be another elliptic curve E_4. Since all the transpositions of S_3 are in the same conjugacy class then E_1, E_2, E_3 are isomorphic. Then by applying the Poincare duality we have that $\text{Jac}\,(X) \cong E^2 \times E'$.

Summarizing, we have the following:

Theorem 1 *Let $\mathcal{X}$ be a genus 3 curve and G its automorphism group. Then,*
a) If $\mathcal{X}$ is hyperelliptic, then the following hold:

i) If G is isomorphic to V_4 or $C_2 \times C_4$, then Jac (X) is isogenous to the product of an elliptic curve E and the Jacobian of a genus 2 curve $\mathcal{X}_2$, namely Jac $(\mathcal{X}) \cong E \times$ Jac $(\mathcal{X}_2)$.

ii) If G is isomorphic to C_2^3 then Jac (X) is isogenous to the product of three elliptic curves, namely Jac $(\mathcal{X}) \cong E_1 \times E_2 \times E_3$.

iii) If G is isomorphic to $D_{12}, C_2 \times S_4$ or any of the groups of order 24 or 32, then Jac (X) is isogenous to the product of three elliptic curves such that two of them are isomorphic, namely Jac $(\mathcal{X}) \cong E_1^2 \times E_2$.

b) If $\mathcal{X}$ is non-hyperelliptic then the following hold:

i) If G is isomorphic to C_2, then Jac (X) is isogenous to the product of an elliptic curve and the Jacobian of some genus 2 curve $\mathcal{X}_2$, namely Jac $(\mathcal{X}) \cong E \times$ Jac $(\mathcal{X}_2)$.

ii) If G is isomorphic to V_4, then Jac (X) is isogenous to the product of three elliptic curves namely Jac $(\mathcal{X}) \cong E_1 \times E_2 \times E_3$.

iii) If G is isomorphic to S_3, D_8 or has order 16 or 48, then Jac (X) is isogenous to the product of three elliptic curves such that two of them are isomorphic to each other, namely Jac $(\mathcal{X}) \cong E_1^2 \times E_2$.

iv) If G is isomorphic to $S_4, L_3(2)$ or $C_2^3 \rtimes S_3$, then Jac (X) is isogenous to the product of three elliptic curves such that all three of them are isomorphic to each other, namely Jac $(\mathcal{X}) \cong E^3$.

Proof. The proof of the hyperelliptic case is similar and we skip the details.

Part b): When G is isomorphic to C_2, V_4, D_8, S_4, S_3 the result follows from the remarks above. The rest of the theorem is an immediate consequence of the list of groups as in the Table 1 of [9]. If $|G| = 16, 48$ then $D_8 \hookrightarrow G$. Then, from the remarks at the beginning of this section the results follows. If G is isomorphic to $L_3(2)$ or $C_4^2 \rtimes S_3$ then $S_4 \hookrightarrow G$. Hence the Jacobian splits as in the case of S_4. This completes the proof.

The above theorem gives the splitting of the Jacobian based on automorphisms. Next we will focus on the $(2, 4, 4)$ splitting for hyperelliptic curves. We will explicitly determine the elliptic components for a given genus 3 curve $\mathcal{X}$.

3 Hyperelliptic curves with extra involutions

Let K be a genus 3 hyperelliptic field over the ground field k. Then K has exactly one genus 0 subfield of degree 2, call it $k(X)$. It is the fixed field of the **hyperelliptic involution** ω_0 in Aut (K). Thus, ω_0 is central in Aut (K), where Aut (K) denotes the group Aut (K/k). It induces a subgroup of Aut $(k(X))$ which is naturally isomorphic to $\overline{\text{Aut}}(K) :=$ Aut $(K)/\langle\omega_0\rangle$. The latter is called the **reduced automorphism group** of K.

An **elliptic involution** of $G =$ Aut (K) is an involution which fixes an elliptic subfield. An involution of $\bar{G} = \overline{\text{Aut}}(K)$ is called **elliptic** if it is the image of an elliptic involution of G. If ω_1 is an elliptic involution in G then $\omega_2 := \omega_0\, \omega_1$ is another involution (not necessarily elliptic). So the non-hyperelliptic involutions come naturally in (unordered) pairs ω_1, ω_2. These pairs correspond bijectively to the Klein 4-groups in G.

Definition 1 *We will consider pairs (K, ε) with K a genus 3 hyperelliptic field and ε an elliptic involution in $\bar{G}$. Two such pairs (K, ε) and (K', ε') are called isomorphic if there is a k-isomorphism $\alpha : K \to K'$ with $\varepsilon' = \alpha\varepsilon\alpha^{-1}$.*

Let ε be an elliptic involution in $\bar{G}$. We can choose the generator X of $\text{Fix}(\omega_0)$ such that $\varepsilon(X) = -X$. Then $K = k(X, Y)$ where X, Y satisfy equation $Y^2 = (X^2 - \alpha_1^2)(X^2 - \alpha_2^2)(X^2 - \alpha_3^2)(X^2 - \alpha_4^2)$, for some $\alpha_i \in k$, $i = 1, \ldots, 4$. Denote by s_1, s_2, s_3, s_4 the symmetric polynomials of $\alpha_1^2, \alpha_2^2, \alpha_3^2, \alpha_4^2$; see [15] for details. Then, we have $Y^2 = X^8 + s_1 X^6 + s_2 X^4 + s_3 X^2 + s_4$, with $s_1, s_2, s_3, s_4 \in k$, $s_4 \neq 0$. Furthermore, $E = k(X^2, Y)$ and $C = k(X^2, YX)$ are the two subfields corresponding to ε of genus 1 and 2 respectively.

Preserving the condition $\varepsilon(X) = -X$ we can further modify X such that $s_4 = 1$. Then, we have the following:

Theorem 2 *Let K be a genus 3 hyperelliptic field and F an elliptic subfield of degree 2.*

i) Then, $K = k(X, Y)$ such that

$$Y^2 = X^8 + aX^6 + bX^4 + cX^2 + 1 \tag{2}$$

for $a, b, c \in k$ such that the discriminant of the right hand side $\Delta(a, b) \neq 0$.

ii) $F = k(U, V)$ where $U = X^2$, and $V = Y$ and

$$V^2 = U^4 + aU^3 + bU^2 + cU + 1 \tag{3}$$

iii) There is a genus 2 subfield $L = k(x, y)$ where $x = X^2$, $y = YX$ and

$$y^2 = x(x^4 + ax^3 + bx^2 + cx + 1) \tag{4}$$

Proof. The proof follows from the above remarks. To show that the genus 2 subfield is generated by X^2, YX it is enough to show that they are fixed by ω_2. In cases ii) and iii) we are again assuming that the discriminant of the right hand side is not zero. □

These conditions determine X up to coordinate change by the group $\langle \tau_1, \tau_2 \rangle$ where $\tau_1 : X \to \zeta_8 X$, $\tau_2 : X \to \frac{1}{X}$, and ζ_8 is a primitive 8-th root of unity in k. Hence, $\tau_1 : (a, b, c) \to \left(\zeta_8^6 a, \zeta_8^4 b, \zeta^2 c\right)$, and $\tau_2 : (a, b, c) \to (c, b, a)$.

Then, $|\tau_1| = 4$ and $|\tau_2| = 2$. The group generated by τ_1 and τ_2 is the dihedral group of order 8. Invariants of this action are

$$\mathfrak{s}_2 = a\,c, \quad \mathfrak{s}_3 = (a^2 + c^2)\,b, \quad \mathfrak{s}_4 = a^4 + c^4. \tag{5}$$

Since the above transformations are automorphisms of the projective line $\mathbb{P}^1(k)$ then the $SL_2(k)$ invariants must be expressed in terms of $\mathfrak{s}_2, \mathfrak{s}_3$, and $\mathfrak{s}_4$.

If $\mathfrak{s}_4 + 2\mathfrak{s}_2^2 = 0$ then this implies that the curve has automorphism group $\mathbb{Z}_2 \times \mathbb{Z}_4$, see [10] for details. From now on we assume that $\mathfrak{s}_4 + 2\mathfrak{s}_2^2 \neq 0$.

The discriminant of the octavic polynomial on the right hand side of Eq. (2) is expressed in terms of $\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4$; see [15] for details. From now forward we will assume that $\Delta(\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4) \neq 0$ since in this case the corresponding triple $(\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4)$ does not correspond to a genus 3 curve. The map $(a, b, c) \mapsto (\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4)$ is a branched Galois covering with group D_4 of the set $\{(\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4) \in k^3 : \Delta(\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4) \neq 0\}$ by the corresponding open subset of (a, b, c)-space. In any case, it is true that if a, b, c and a', b', c' have the same $\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4$-invariants then they are conjugate under $\langle \tau_1, \tau_2 \rangle$.

Lemma 1. *For $(a,b,c) \in k^3$ with $\Delta \neq 0$, equation* (2) *defines a genus 3 hyperelliptic field $K_{a,b,c} = k(X,Y)$. Its reduced automorphism group contains the non-hyperelliptic involution $\varepsilon_{a,b,c} : X \mapsto -X$. Two such pairs $(K_{a,b,c}, \varepsilon_{a,b,c})$ and $(K_{a',b',c'}, \varepsilon_{a',b',c''})$ are isomorphic if and only if $\mathfrak{s}_4 = \mathfrak{s}_4'$, $\quad \mathfrak{s}_3 = \mathfrak{s}_3'$, $\quad$ and $\quad \mathfrak{s}_2 = \mathfrak{s}_2'$, where $\mathfrak{s}_4, \mathfrak{s}_3, \mathfrak{s}_2$ and $\mathfrak{s}_4', \mathfrak{s}_3', \mathfrak{s}_2'$ are associated with a,b,c and a',b',c', respectively, by* (5)*).*

Proof. An isomorphism α between these two pairs yields $K = k(X,Y) = k(X',Y')$ with $k(X) = k(X')$ such that X,Y satisfy (2) and X',Y' satisfy the corresponding equation with a,b,c replaced by a',b',c'. Further, $\varepsilon_{a,b,c}(X') = -X'$. Thus X' is conjugate to X under $\langle \tau_1, \tau_2 \rangle$ by the above remarks. This proves the condition is necessary. It is clearly sufficient. □

Relations among $\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4$ for each G when $V_4 \hookrightarrow G$ are determined in [10].

4 Subcovers of genus 2

Next we study in detail the complement C of E in Jac $(\mathcal{X})$. From the above theorem, C has equation as in Eq. (4). Its absolute invariants i_1, i_2, i_3, as defined in [6], can be expressed in terms of the dihedral invariants $\mathfrak{s}_4, \mathfrak{s}_3, \mathfrak{s}_2$ as follows:

$$i_1 = 144 \frac{M}{D^2} f_1(\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4),\; i_2 = 432 \frac{M^2}{D^3} f_2(\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4),\; i_3 = \frac{243}{16} \frac{M^3}{D^5} f_3(\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4) \qquad (6)$$

where $M = \mathfrak{s}_4 + 2\mathfrak{s}_2^2$ and $D = 16\, s_2{}^3 - 40\, s_2{}^2 + 8\, s_2 s_4 - 3\, s_3{}^2 - 20\, s_4$ and f_1, f_2, f_3 are given in [15]. For the rest of the paper we assume that $D = J_2 \neq 0$.

We consider the case when Jac (C) is $(2,2)$ decomposable. The locus $\mathcal{L}_2$ of such genus two curves is computed in [6] in terms of the invariants i_1, i_2, i_3. Substituting the expressions in Eq. (6) in the equation of $\mathcal{L}_2$ from [6] we have the following:

$$\left(2\,\mathfrak{s}_2{}^2 - \mathfrak{s}_4\right) \cdot \left(2\,\mathfrak{s}_2{}^2 + \mathfrak{s}_4\right) \cdot F_1(\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4) = 0 \qquad (7)$$

where $F_1(\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4)$ is an irreducible polynomial of degree 13, 8, 6 in $\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4$ respectively; see [15].

Let the locus of genus 3 hyperelliptic curves whose Jacobian is $(2,4,4)$-split be denoted by $\mathcal{T}$. There are three components of $\mathcal{T}$ which we denote them by $\mathcal{T}_i$, $i = 1,2,3$ as seen by Eq. (7).

Two of these components are well known and the correspond to the cases when V_4 is embedded in the reduced automorphism group of $\mathcal{X}$. These cases correspond to the singular locus of $\mathcal{S}_2$ and are precisely the locus det (Jac $(\phi)) = 0$, see [6]. This happens for all genus $g \geq 2$ as noted in [6], and shown in [6].

Lemma 2. *Let $\mathcal{X}$ be a genus 3 curve with $(2,2,4)$-split Jacobian. Then, one of the following occurs*

i) $\mathbb{Z}_2^3 \hookrightarrow Aut\ (\mathcal{X})$

ii) $\mathbb{Z}_2 \times \mathbb{Z}_4 \hookrightarrow Aut\ (\mathcal{X})$

iii) $\mathcal{X}$ is in the locus $\mathcal{T}_3$

Proof. The proof is an immediate consequence of Theorem 2 and Eq. (7). □

The third component $\mathcal{T}_3$ is more interesting to us. It is the moduli space of pairs of degree 4 non-Galois covers $\psi_i : \mathcal{X}_3 \to E_i$, $i = 1, 2$.

One of the main goals of this paper is to determine explicitly the family $\mathcal{T}_3$ of genus 3 curves and relations among its elliptic subcovers. We have the maps

$$
\begin{array}{c}
\mathcal{T}_3 \xrightarrow{\psi} \mathcal{L}_2 \xrightarrow{\psi_0} k^2 \\
(\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4) \to (u, v) \to (j_1, j_2)
\end{array}
\tag{8}
$$

where $\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4$ satisfy $F_1(\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4) = 0$ and u, v are given explicitly by Eq. (6) and Thm. (3) in [6].

The expressions of u and v are computed explicitly in terms of $\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4$ by substituting the expressions of Eq. (6) expressions for u and v as rational functions of $i_1, i_2 i_3$ as computed in [6]. As rational functions u and v have degrees 35 and 70 respectively (in terms of $\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4$). The j-invariants j_1 and j_2 will be determined in the next section.

Since $\mathcal{T}_3$ is a subvariety of $\mathcal{H}_3$ it would be desirable to express its equation in terms of a coordinate in $\mathcal{H}_3$. One can use the absolute invariants of the genus 3 hyperelliptic curves $t_1, \dots, t_6$ as defined in [12] and the expressions of $\mathfrak{s}_4, \mathfrak{s}_3, \mathfrak{s}_2$ in terms of these invariants as computed in [10].

Remark 1 *$\mathcal{T}_3$ is a 2-dimensional subvariety of $\mathcal{H}_3$ determined by the equations*

$$
\left\{
\begin{array}{r}
F_1(\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4) = 0 \\
t_i - T_i(\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4), \quad i = 1, \dots, 6
\end{array}
\right.
\tag{9}
$$

where T_i is the function t_i evaluated for the triple $(\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4)$.

The equations of $\mathcal{T}_3$ can be explicitly determined in terms of $t_1, \dots, t_6$ by eliminating $\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_2$ from the above equations. Normally, when we talk about $\mathcal{T}_3$ we will think of it given in terms of $t_1, \dots, t_6$.

Example 1 *Consider the genus 3 curves $\mathcal{X}$ with Aut $(\mathcal{X}) \cong \mathbb{Z}_2^3$. Then, $\mathfrak{s}_4 = 2s_2^2$ and*

$$
\begin{aligned}
u =& \frac{1}{P} \left(-9\, {s_3}^2 + 120\, s_2 s_3 - 400\, {s_2}^2 + 16\, {s_2}^3 \right) \\
v =& -\frac{2}{P^2} \left(432\, s_2 {s_3}^3 - 27\, {s_3}^4 - 1440\, {s_2}^2 {s_3}^2 - 6400\, {s_2}^3 s_3 + 32000\, {s_2}^4 + 288\, {s_2}^3 {s_3}^2 \right. \\
& \left. - 5376\, {s_2}^4 s_3 + 23040\, {s_2}^5 + 256\, {s_2}^6 \right)
\end{aligned}
$$

where $P = -s_3^2 - 8\, s_2 s_3 - 16\, s_2^2 + 16\, s_2^3$.

For the rest of this section we will see if we can invert the map ψ.

Proposition 1 *Let $(u, v) \in k^2$ such that*

$$
(u^2 - 4v + 18u - 27)(v^2 - 4u^3)(4v - u^2 + 110u - 1125) \neq 0.
$$

Then, the curve of genus 2 defined over k given by

$$y^2 = a_0 x^6 + a_1 x^5 + a_2 x^4 + a_3 x^3 + t a_2 x^2 + t^2 a_1 x + t^3 a_0, \tag{10}$$

corresponds to the moduli point $(u, v) \in \mathcal{L}_2 \hookrightarrow \mathcal{M}_2$, where one of the following holds:

i) If $u \neq 0$, then $t = v^2 - 4u^3$, $a_0 = v^2 + u^2 v - 2u^3$, $a_1 = 2(u^2 + 3v)(v^2 - 4u^3)$, $a_2 = (15v^2 - u^2 v - 30u^3)(v^2 - 4u^3)$, and $a_3 = 4(5v - u^2)(v^2 - 4u^3)^2$.

ii) If $u = 0$, then $t = 1$, $a_0 = 1 + 2v$, $a_1 = 2(3 - 4v)$, $a_2 = 15 + 14v$, $a_3 = 4(5 - 4v)$.

Hence, corresponding to the pair (u, v) there is a unique genus 2 curve $C_{u,v}$. The following Lemma addresses the rest of our question.

Lemma 3. *i) Any genus two curve C defined over an algebraically closed field k can be written as*

$$y^2 = x(x^4 + ax^3 + bx^2 + cx + 1) \tag{11}$$

for some $a, b, c \in k$ such that $\Delta(a, b, c) \neq 0$.

ii) Let C be a genus 2 curve with equation as in Eq. (11)*. Then, there exists a genus 3 curve $\mathcal{X}$ with equation $Y^2 = X^8 + aX^6 + bX^4 + CX^2 + 1$ and a degree 2 map $f : \mathcal{X} \to C$ such that $x = X^2$ and $y = YX$.*

Proof. i) Let C be a genus 2 curve defined over k. Then, the equation of C is given by $y^2 = \Pi_{i=1}^{6}(x - \alpha_i)$, where α_i are all distinct for all $i = 1 \dots 6$. Since k is algebraically closed, then we can pick a change of transformation in $\mathbb{P}^1(k)$ such that $\alpha_1 \to 0$ and $\alpha_2 \to \infty$. We can also pick a coordinate such that $\alpha_3 \cdots a_6 = 1$. Then, the curve C has equation as claimed. The condition that $\Delta(a, b, c) \neq 0$ simply assures that not two roots of the sextic coalesce.

ii) This genus 3 curve is a covering of C from Thm. 2. □

Hence, the curve $C_{u,v}$ can be written as in Eq. (11). This would mean that we can explicitly compute $\mathfrak{s}_4, \mathfrak{s}_3, \mathfrak{s}_2$ in terms of u and v. Finding a general formula for $(\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4)$ in terms of (u, v) is computationally difficult. Under some additional restrictions this ca be done, as we will see in the next section.

5 Elliptic subfields

In this section we will determine the elliptic subcovers of the genus 3 curves $\mathcal{X} \in \mathcal{T}_3$. We will describe how this can be explicitly done, but will skip displaying the computations here. A point $\mathfrak{p} = (t_1, \dots, t_6) \in \mathcal{T}_3$ satisfies equations Eq. (9). Our goal is to determine the j-invariants of E, E_1, E_2 in terms of $t_1, \dots t_6$. The j-invariant of E is

$$j = 256 \, \frac{\left(-\mathfrak{s}_3{}^2 - 12\,\mathfrak{s}_4 - 24\,\mathfrak{s}_2{}^2 + 3\,\mathfrak{s}_2\mathfrak{s}_4 + 6\,\mathfrak{s}_2{}^3\right)^3}{(\mathfrak{s}_4 + 2\,\mathfrak{s}_2{}^2)} f(\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4), \tag{12}$$

where $f(\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4)$ can be found in [15].

We denote the degree 2 elliptic subcovers of C by E_1 and E_2 and their j-invariants by j_1 and j_2. These j invariants are the roots of the quadratic

$$j^2 + 256\,\frac{2u^3 - 54u^2 + 9uv - v^2 + 27v}{u^2 + 18u - 4v - 27}\,j + 65536\,\frac{u^2 + 9u - 3v}{(u^2 + 18u - 4v - 27)^2}, \tag{13}$$

see Eq. (4) in [6].

Since these j-invariants are determined explicitly in terms of u and v, then via the map $\psi : \mathcal{T}_3 \to \mathcal{L}_2$ we express such coefficients in terms of $\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4$. Moreover, the maps

$$\begin{aligned} &\mathcal{T}_3 \to k^3 \setminus \{\Delta(\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4) = 0\} \to k^2 \setminus \{\Delta_{u,v} = 0\} \to k^2 \\ &(t_1, \dots, t_6) \to (\mathfrak{s}_4, \mathfrak{s}_3, \mathfrak{s}_2) \xrightarrow{\psi} (u, v) \to (j_1, j_2) \end{aligned} \tag{14}$$

are all explicitly determined.

Example 2 *Let be given a 6-tuple*

$$(t_1, \dots, t_6) = \left(\frac{8767521}{6224272}, \frac{152464}{5329}, \frac{8116}{3431}, -\frac{3343532}{695617}, -\frac{91532}{148117}, -\frac{50448727768}{28398241} \right)$$

which satisfies the Eq. (17) in [12]. *Then, this tuple corresponds to a genus 3 hyperelliptic curve, more precisely the curve $\mathcal{X}$ with equation*

$$Y^2 = X^8 + X^6 + X^4 + X^2 + 1$$

Then, the corresponding invariants are $\mathfrak{s}_2 = 1$, $\mathfrak{s}_3 = 2$, $s_4 = 2$. The genus 2 subcover has invariants $i_1 = -\frac{48}{5}$, $i_2 = \frac{432}{5}$, $i_3 = \frac{1}{400}$ and the corresponding dihedral invariants are $u = 9$ and $v = -\frac{754}{5}$. The j-invariants of the three elliptic subcover are $j = 2048$ $j_1 = \frac{32768}{5} + \frac{2}{5}\sqrt{268435081}$ and $j_2 = \frac{32768}{5} - \frac{2}{5}\sqrt{268435081}$.

Next we will study the subvariety of $\mathcal{T}_3$, such that E_1 is isomorphic to E_2.

5.1 Isomorphic elliptic subfields

The two elliptic curves E_1 and E_2 are isomorphic when their j-invariants are equal, which happens when the discriminant of the quadratic in Eq. (13) is zero. From Remark (1) in [6] this occurs if and only if

$$(v^2 - 4u^3)(v - 9u + 27) = 0$$

The first condition is equivalent to $D_8 \hookrightarrow Aut(C)$. The later condition gives $u = 9 - \frac{\lambda}{256}$ and $v = 9\left(6 - \frac{\lambda}{256}\right)$, where $\lambda := j_1 = j_2$. Both of these loci can be explicitly computed given enough computing power.

Substituting u and v in terms of $\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4$ in the equation $v - 9u + 27 = 0$, we get an equation of degree 68, 42, and 29 in $\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4$ respectively. We denote it by

$$F_2(\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4) = 0 \tag{15}$$

and do not display it here because of its size. This equation and the Eq. (7) define the locus $\mathfrak{T}$ in terms of $\mathfrak{s}_4, \mathfrak{s}_3, \mathfrak{s}_2$.

Lemma 4. *The algebraic variety $\mathfrak{T}$ is a 1-dimensional subvariety, it has 5 genus 0 components as in Eq.* (16)*. Every point $(\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4) \in \mathfrak{T}$ correspond to a genus 3 hyperelliptic curve with* $(2, 4, 4)$*-split Jacobian such that the degree 4 elliptic subcovers are isomorphic to each other.*

Proof. From the equations above we can eliminate $\mathfrak{s}_3$ via resultants and get the following. In this case we get

$$(2\mathfrak{s}_2^2 - \mathfrak{s}_4)^{16}(\mathfrak{s}_4 + 2\mathfrak{s}_2^2)^{172}\, g_1^{12}\, g_2^{12}\, g_3^{10}\, g_4^8\, g_5 = 0 \tag{16}$$

where g_5 can be found in [15] and $g_1, \dots, g_4$ are

$$\begin{aligned}
g_1 =& \, s_4 + 2\, {s_2}^2 - 100\, s_2 + 625 \\
g_2 =& -27\, s_4 + {s_2}^3 + 6\, {s_2}^2 + 768\, s_2 - 4096 \\
g_3 =& -16777216 + 5242880\, s_2 - 450560\, {s_2}^2 + 7680\, {s_2}^3 - 340\, {s_2}^4 + 8\, {s_2}^5 - 102400\, s_4 \\
& + 16640\, s_2 s_4 - 220\, {s_2}^2 s_4 + 4\, s_4 {s_2}^3 - 125\, {s_4}^2 \\
g_4 =& \, 3515625 - 937500\, s_2 + 62500\, {s_2}^2 + 64\, {s_2}^4 + 15000\, s_4 - 2000\, s_2 s_4
\end{aligned}$$

Since $(2\mathfrak{s}_4 - \mathfrak{s}_2^2)(2\mathfrak{s}_4 + \mathfrak{s}_2^2) \neq 0$, as noted before. All other components are genus zero curves. □

The equation of $\mathfrak{T}$ can be expressed in the absolute invariants $t_1, \dots, t_6$ by eliminating $\mathfrak{s}_4, \mathfrak{s}_3, \mathfrak{s}_2$ from expressions in Eq. (6). Such expressions are large and we do not display them here.

Let be given a parameterization of $\mathfrak{T}$. Then we have the following maps

$$\begin{aligned}
k &\to \mathfrak{T} \to L_2 \to k \\
t &\to (\mathfrak{s}_4(t), \mathfrak{s}_3(t), \mathfrak{s}_2(t)) \to (u(t), v(t)) \to j(t)
\end{aligned} \tag{17}$$

This map gives us the possibility to construct a family of curves defined over $\mathbb{Q}$ such that all their subcovers, namely C, E, E_1, and E_2 are also defined over $\mathbb{Q}$. For example, for $t \in \mathbb{Q}$ we have the corresponding $\mathfrak{s}_4, \mathfrak{s}_3, \mathfrak{s}_3 \in \mathbb{Q}$. Hence, there is a genus 3 curve $\mathcal{X}$ defined over $\mathbb{Q}$. The invariants u, v are rational functions of $\mathfrak{s}_4, \mathfrak{s}_3, \mathfrak{s}_2$ and therefore of t. Thus, $u, v \in \mathbb{Q}$. Form Prop. 1 there is a genus 2 curve C such that C is defined over $\mathbb{Q}$. Moreover, the j-invariants for all elliptic subcovers are rational functions in $\mathfrak{s}_4, \mathfrak{s}_3, \mathfrak{s}_2$ and therefore in t. Hence, E, E_1, E_2 are also defined over $\mathbb{Q}$.

Theorem 3 *Let $\mathcal{X}$ be a curve in $\mathfrak{T}$ and $\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4$ its corresponding dihedral invariants. Then*

$$Jac\ (\mathcal{X}) \cong E \times E' \times E'$$

where E and E' are elliptic curves with j-invariants $j(E)$ as in Eq. (12) *and $j(E')$ as*

$$j' = -128\, \frac{2\, u^3 - 54\, u^2 + 9\, uv - v^2 + 27\, v}{u^2 + 18\, u - 4\, v - 27},$$

where u and v are given as rational functions of i_1, i_2, i_3 as in [6]*. Moreover, there is only a finite number of genus 3 curves $\mathcal{X}$ such that $E \cong E'$.*

Proof. The equation of $j(E)$ was computed in Eq. (12). Since the other two elliptic subcovers have the same j-invariants then this invariant is given by the double root of the quadratic in Eq. (13). Thus,

$$j' = -128 \frac{2\,u^3 - 54\,u^2 + 9\,uv - v^2 + 27\,v}{u^2 + 18\,u - 4\,v - 27}$$

Substituting the values for u and v we get the expression as claimed.

We have $E \cong E'$ if and only if $j = j'$. This gives a third equation $G(\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4) = 0$ as claimed in the theorem. By Bezut's theorem, the number of solutions of the system of equations $F_i(\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4) = 0$, for $i = 1, 2$ and $G(\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4) = 0$ is finite. □

References

[1] Robert D. M. Accola, *Two theorems on Riemann surfaces with noncyclic automorphism groups.* Proc. Amer. Math. Soc. **25** (1970), 598–602.

[2] ———, *Riemann surfaces with automorphism groups admitting partitions*, Proc. Amer. Math. Soc. **21** (1969), 477–482.

[3] L. Beshaj, *Singular locus on the space of genus 2 curves with decomposable Jacobians*, Albanian J. Math. **4** (2010), no. 4, 147–160.

[4] L. Beshaj and F. Thompson, *Equations for superelliptic curves over their minimal field of definition*, arXiv:1405.4556v1.

[5] L. Beshaj, T. Shaska, and C. Shor, *On Jacobians of curves with superelliptic components*, arXiv:1310.7241v3.

[6] L. Beshaj and T. Shaska, *The arithmetic of genus two curves*, Information security, coding theory and related combinatorics, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur. vol. 29, IOS, Amsterdam, 2011, pp. 59–98.

[7] ———, *Heights of algebraic curves*, The arithmetic of hyperelliptic curves, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur. IOS, Amsterdam, 2014, pp. to appear.

[8] ———, *Algebraic curves with minimal height*, work in progress.

[9] J. Gutierrez and T. Shaska, *Hyperelliptic curves with extra involutions*, LMS J. Comput. Math. **8** (2005), 102–115.

[10] T. Shaska and F. Thompson, *Bielliptic curves of genus 3 in the hyperelliptic moduli*, Appl. Algebra Engrg. Comm. Comput. **24** (2013), no. 5, 387–412.

[11] T. Shaska and C. Shor, *The 2-Weierstrass points of genus 3 hyperelliptic curves with extra automorphisms*, arXiv:1307.8177v2.

[12] T. Shaska, *Some Remarks on the Hyperelliptic Moduli of Genus 3*, Comm. Algebra **42** (2014), no. 9, 4110–4130.

[13] ———, *Genus two curves covering elliptic curves: a computational approach*, Computational aspects of algebraic curves, Lecture Notes Ser. Comput. vol. 13, World Sci. Publ., Hackensack, NJ, 2005, pp. 206–231.

[14] ———, *Families of genus 2 curves with many elliptic subcovers*, arXiv:1209.0434v1.

[15] ———, *Genus 3 hyperelliptic curves with (2, 4, 4) decomposable Jacobians*, arXiv:1306.5284.