SOME REMARKS ON THE HYPERELLIPTIC MODULI OF GENUS 3

T. SHASKA

This paper is dedicated to my father and my best teacher Bedri Shaska on the occasion of his 78th birthday

Abstract. In 1967, Shioda [20] determined the ring of invariants of binary octavics and their syzygies using the symbolic method. We discover that the syzygies determined in [20] are incorrect. In this paper, we compute the correct equations among the invariants of the binary octavics and give necessary and sufficient conditions for two genus 3 hyperelliptic curves to be isomorphic over an algebraically closed field k, char $k \neq 2, 3, 5, 7$. For the first time, an explicit equation of the hyperelliptic moduli for genus 3 is computed in terms of absolute invariants.

1. Introduction

Let k be an algebraically closed field. A binary form of degree d is a homogeneous polynomial $f(X, Y)$ of degree d in two variables over k. Let V_d be the k-vector space of binary forms of degree d. The group $GL_2(k)$ of invertible 2×2 matrices over k acts on V_d by coordinate change. Many problems in algebra involve properties of binary forms which are invariant under these coordinate changes. In particular, any hyperelliptic genus g curve over k has a projective equation of the form $Z^2Y^{2g} = f(X, Y)$, where f is a binary form of degree $d = 2g + 2$ and non-zero discriminant. Two such curves are isomorphic if and only if the corresponding binary forms are conjugate under $GL_2(k)$. Therefore the moduli space $\mathcal{H}_g$ of hyperelliptic genus g curves is the affine variety whose coordinate ring is the ring of $GL_2(k)$-invariants in the coordinate ring of the set of elements of V_d with non-zero discriminant. It is well known that the moduli spaces $\mathcal{H}_g$ of hyperelliptic curves of genus g, $g \neq 4$, are all rational varieties, i.e. isomorphic to a purely transcendental extension field $k(t_1, \ldots, t_r)$; see Igusa [10], Katsylo [11].

Generators for this and similar invariant rings in lower degree were constructed by Clebsch, Bolza and others in the last century using complicated symbolic calculations. For the case of sextics, Igusa [10] extended this to algebraically closed fields of any characteristic using difficult techniques of algebraic geometry. For a modern treatment of the degree six case see [12].

The case of binary octavics has been first studied during the 19th century by von Gall [21, 22] and Alagna [1, 2]. Shioda in his thesis [20] determined the structure of the ring of invariants $\mathcal{R}_8$, which turns out to be generated by nine $SL(2, k)$-invariants $J_2, \cdots, J_{10}$ satisfying five algebraic relations. He computed explicitly these five syzygies, and determined the corresponding syzygy-sequence and therefore the structure of the ring $\mathcal{R}_8$; see Shioda [20].

This paper started as a project to implement an algorithm which determines if two genus 3 hyperelliptic curves are isomorphic over $\mathbb{C}$. According to Shioda [20, Thm. 5]; two genus 3 hyperelliptic curves are isomorphic if and only if the corresponding 9-tuples $(J_2, \ldots, J_{10})$ are equivalent, satisfying five syzygies

$$R_i(J_2, \ldots, J_{10}) = 0,$$

for $i = 1, \ldots, 5$ and non-zero discriminant $\Delta \neq 0$. While trying to implement the syzygies $R_i(J_2, \ldots, J_{10}) = 0$, for $i = 1, \ldots, 5$ we discovered that they are not satisfied for a generic octavic. Hence, such algebraic relations in terms of $J_2, \ldots, J_{10}$ are incorrect as stated in [20]; cf Example 1.

Indeed, if you take any random binary octavics then its invariants will not satisfy the Shioda's relations. Since the results in [20] do not hold, then one needs to determine explicitly the algebraic relations between the invariants in order to have an explicit description of the ring of invariants $\mathcal{R}_8$ and its field of fractions $\mathcal{S}_8$. This will be our goal for the rest of this paper.

In section 2, we give some basic preliminaries on invariants of binary forms. In section 3, we define the main invariants of binary octavics via transvectants. The definitions are the same as used by classical invariant theorists,

2000 *Mathematics Subject Classification.* Primary 54C40, 14E20; Secondary 46E25, 20C20.
Key words and phrases. invariants, binary forms, genus 3, algebraic curves.

however, we scale by a constant factor in order to work with primitive polynomials with integer coefficients. We show an example of a binary form which does not satisfy the syzygies as claimed in [20]; see Example 1. Furthermore, we determine the algebraic relations between the invariants $J_2, \ldots, J_{10}$. Such algebraic relations determine the ring of invariants $\mathcal{R}_8$.

From the basic $SL(2,k)$-invariants $J_2, \ldots, J_8$ we define six $GL(2,k)$-invariants

$$t_1 := \frac{J_3^2}{J_2^3}, \quad t_2 := \frac{J_4}{J_2^2}, \quad t_3 := \frac{J_5}{J_2 \cdot J_3}, \quad t_4 := \frac{J_6}{J_2 \cdot J_4}, \quad t_5 := \frac{J_7}{J_2 \cdot J_5}, \quad t_6 := \frac{J_8}{J_2^4},$$

which we call absolute invariants. There is an algebraic relation

$$T(t_1, \ldots, t_6) = 0$$

that such invariants satisfy, computed for the first time. Shioda in his paper talked about this relation but never attempted to compute it. It has total degree 14, degrees 5, 10, 6, 6, 5, 5 in $t_1, \ldots, t_6$ respectively, and has 25 464 monomials. The field of invariants $\mathcal{S}_8$ of binary octavics is $\mathcal{S}_8 = k(t_1, \ldots, t_6)$, where $t_1, \ldots, t_6$ satisfy the equation $T(t_1, \ldots, t_6) = 0$. Hence, we have an explicit description of the hyperelliptic moduli $\mathcal{H}_3$. A birational parametrization of this variety seems out of reach computationally.

All of our results are implemented in a Maple package and made available at [19]. Such results will be helpful in the arithmetic of genus 3 hyperelliptic curves. The computation of Eq. (17) makes now possible to describe the subloci of $\mathcal{H}_3$ in terms of the $t_1, \ldots, t_6$ invariants and other problems on genus 3 hyperelliptic curves as described in [3, 4, 6, 7, 13, 15–18] among others.

2. Preliminaries on invariants of binary forms

In this section we define the action of $GL_2(k)$ on the space of binary forms and discuss the basic notions of their invariants. Most of this section is a summary of section 2 in [12]. Throughout this section k denotes an algebraically closed field.

2.1. **Action of $GL_2(k)$ on binary forms.** Let $k[X,Y]$ be the polynomial ring in two variables and let V_d denote the $(d+1)$-dimensional subspace of $k[X,Y]$ consisting of homogeneous polynomials.

$$f(X,Y) = a_0X^d + a_1X^{d-1}Y + \cdots + a_dY^d \tag{1}$$

of degree d. Elements in V_d are called **binary forms** of degree d. We let $GL_2(k)$ act as a group of automorphisms on $k[X,Y]$ as follows: if

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(k)$$

then

$$g \begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} aX + bY \\ cX + dY \end{pmatrix} \tag{2}$$

This action of $GL_2(k)$ leaves V_d invariant and **acts irreducibly** on V_d.

Remark 1. *It is well known that $SL_2(k)$ leaves a bilinear form (unique up to scalar multiples) on V_d invariant. This form is symmetric if d is even and skew symmetric if d is odd.*

Let A_0, A_1, …, A_d be coordinate functions on V_d. Then the coordinate ring of V_d can be identified with $k[A_0, \ldots, A_d]$. For $I \in k[A_0, \ldots, A_d]$ and $g \in GL_2(k)$, define $I^g \in k[A_0, \ldots, A_d]$ as follows

$$I^g(f) = I(g(f)) \tag{3}$$

for all $f \in V_d$. Then $I^{gh} = (I^g)^h$ and (3) defines an action of $GL_2(k)$ on $k[A_0, \ldots, A_d]$.

Definition 1. *Let $\mathcal{R}_d$ be the ring of $SL_2(k)$ invariants in $k[A_0, \ldots, A_d]$, i.e., the ring of all $I \in k[A_0, \ldots, A_d]$ with $I^g = I$ for all $g \in SL_2(k)$.*

Note that if I is an invariant, so are all its homogeneous components. So $\mathcal{R}_d$ is graded by the usual degree function on $k[A_0, \ldots, A_d]$.

Since k is algebraically closed, the binary form $f(X,Y)$ in Eq. (1) can be factored as

$$f(X,Y) = (y_1X - x_1Y)\cdots(y_dX - x_dY) = \prod_{1\le i\le d} det\begin{pmatrix} X & x_i \\ Y & y_i \end{pmatrix} \tag{4}$$

The points with homogeneous coordinates $(x_i, y_i) \in \mathbb{P}^1$ are called the **roots of the binary form** in Eq. (1). Thus for $g \in GL_2(k)$ we have

$$g(f(X,Y)) = (det(g))^d(y_1^{'}X - x_1^{'}Y)\cdots(y_d^{'}X - x_d^{'}Y).$$

where

$$\begin{pmatrix} x_i^{'} \\ y_i^{'} \end{pmatrix} = g^{-1}\begin{pmatrix} x_i \\ y_i \end{pmatrix} \tag{5}$$

Definition 2. *The **nullcone** $\mathcal{N}_d$ of V_d is the zero set of all homogeneous elements in $\mathcal{R}_d$ of positive degree*

The notion of *nullcone* was first used by Hilbert; see [9]. Next we define the *Reynold's operator* on $k[A_0,\ldots,A_d]$.

Lemma 1. *Let $char(k) = 0$ and Ω_s be the subspace of $k[A_0,\ldots,A_d]$ consisting of homogeneous elements of degree s. Then there is a k-linear map*

$$R : k[A_0,\ldots,A_d] \to \mathcal{R}_d$$

with the following properties:
(a) $R(\Omega_s) \subseteq \Omega_s$ for all s
(b) $R(I) = I$ for all $I \in \mathcal{R}_d$
(c) $R(g(f)) = R(f)$ for all $f \in k[A_0,\ldots,A_d]$

Proof. Ω_s is a polynomial module of degree s for $SL_2(k)$. Since $SL_2(k)$ is linearly reductive in $char(k) = 0$, there exists a $SL_2(k)$-invariant subspace Λ_s of Ω_s such that $\Omega_s = (\Omega_s \cap \mathcal{R}_d) \bigoplus \Lambda_s$. Define

$$R : k[A_0,\ldots,A_d] \to \mathcal{R}_d$$

such that $R(\Lambda_s) = 0$ and $R_{|\Omega_s\cap\mathcal{R}_d} = id$. Then R is k-linear and the rest of the proof is clear from the definition of R.

□

The map R is called the **Reynold's operator**.

Lemma 2. *Suppose $char(k) = 0$. Then every maximal ideal in $\mathcal{R}_d$ is contained in a maximal ideal of $k[A_0,\ldots,A_d]$.*

Proof. If $\mathcal{I}$ is a maximal ideal in $\mathcal{R}_d$ which generates the unit ideal of $k[A_0,\ldots,A_d]$, then there exist m_1, m_2, $\ldots$,$m_t \in \mathcal{I}$ and f_1, f_2, $\ldots$,$f_t \in k[A_0,\ldots,A_d]$ such that

$$1 = m_1f_1 + \cdots + m_tf_t$$

Applying the Reynold's operator to the above equation we get

$$1 = m_1R(f_1) + \cdots + m_tR(f_t)$$

But $R(f_i) \in \mathcal{R}_d$ for all i. This implies $1 \in \mathcal{I}$, a contradiction. □

Theorem 1. *[Hilbert's Finiteness Theorem] Suppose $char(k) = 0$. Then $\mathcal{R}_d$ is finitely generated over k.*

See [12] for details. If k is of arbitrary characteristic, then $SL_2(k)$ is geometrically reductive, which is a weakening of linear reductivity; see Haboush [8]. It suffices to prove Hilbert's finiteness theorem in any characteristic; see Nagata [14]. The following theorem is also due to Hilbert [9]; see [12] for details of the proof.

Theorem 2. *Let I_1, I_2, $\ldots$, I_s be homogeneous elements in $\mathcal{R}_d$ whose common zero set equals the null cone $\mathcal{N}_d$. Then $\mathcal{R}_d$ is finitely generated as a module over $k[I_1,\ldots,I_s]$.*

2.2. **Hyperelliptic curves of genus 3.** In this section we want to use the projective equivalence of binary octavics in order two give conditions that two hyperelliptic curves of genus 3 are isomorphic.

Denote a binary form of order $2g+2$ by

$$f(X,Y) = \sum_{i=0}^{2g+2} a_i X^i\, Y^{2g+2-i}$$

To each $f(X,Y)$ with no multiple roots we associate the non-singular hyperelliptic curve C_f with affine equation $Z^2 = f(X,1)$. Every hyperelliptic curve of genus g is obtained this way.

Two hyperelliptic curves C_f and C_h are birationally equivalent if and only if $f(X,Y)$ and $h(X,Y)$ are projectively equivalent, i.e., there exists a $\tau \in SL_2(k)$ and $\lambda \in k \setminus \{0\}$ such that $f^\tau = \lambda \cdot h$.

Let Δ_f denote the discriminant of the polynomial $f(X,1)$. It is an invariant of degree $2(2g+1)$. When $g=3$ then the discriminant has degree 14 and is given as a polynomial in $J_2, \ldots, J_8$.

3. Projective invariance of binary octavics.

Throughout this section char $(k) \neq 2, 3, 5, 7$.

3.1. **Covariants and invariants of binary octavics.** We will use the symbolic method of classical theory to construct covariants of binary octavics. They were first constructed by van Gall who showed that there are 70 such covariants; see von Gall [21]. First we recall some facts about the symbolic notation. Let

$$f(X,Y) := \sum_{i=0}^{n} \binom{n}{i} a_i X^{n-i}\, Y^i, \quad \textit{and} \quad g(X,Y) := \sum_{i=0}^{m} \binom{m}{i} b_i X^{n-i}\, Y^i$$

be binary forms of degree n and m respectively. We define the *r-transvection*

$$(f,g)^r := \frac{(m-r)!\,(n-r)!}{n!\,m!} \sum_{k=0}^{r} (-1)^k \binom{r}{k} \cdot \frac{\partial^r f}{\partial X^{r-k}\,\partial Y^k} \cdot \frac{\partial^r g}{\partial X^k\,\partial Y^{r-k}},$$

see Grace and Young [5] for details.

The following result gives relations among the invariants of binary forms and it is known as the Gordon's formula. It is the basis for most of the classical papers on invariant theory.

Theorem 3 (Gordon)**.** *Let ϕ_i, $i = 0,1,2$ be covariants of order m_i and e_i be three non-negative integers such that $e_i + e_j \leq m_k$ for distinct i,j,k. The following is true:*

$$\sum_i \frac{C_i^{e_1} \cdot C_i^{m_1-e_0-e_2}}{C_i^{m_0+m_1+1-2e_2-i}} \left((\phi_0\,\phi_1)^{e_2+1}, \phi_2\right)^{e_0+e_1-i} = \sum_i \frac{C_i^{e_2} \cdot C_i^{m_2-e_0-e_1}}{C_i^{m_0+m_2+1-2e_1-i}} \left((\phi_0\,\phi_2)^{e_1+1}, \phi_1\right)^{e_0+e_2-i},$$

where $e_0 = 0$ or $e_1 + e_2 = m_0$.

This result has been used by many XIX century mathematicians to compute algebraic relations among invariants, most notably by Bolza for binary sextics and by Alagna for binary octavics. It provides algebraic relations among the invariants in a very similar manner that the Frobenious identities do for theta functions of hyperelliptic curves. Whether there exists some explicit relation among both formulas seems to be unknown.

For the rest of this paper $f(X,Y)$ denotes a binary octavic as below:

$$f(X,Y) = \sum_{i=0}^{8} a_i X^i Y^{8-i} = \sum_{i=0}^{8} \binom{n}{i} b_i X^i Y^{n-i} \tag{6}$$

where $b_i = \frac{(n-i)!\;i!}{n!} \cdot a_i$, for $i = 0, \ldots, 8$. We define the following covariants:

$$\begin{aligned} &g = (f,f)^4, \quad k = (f,f)^6, \quad h = (k,k)^2, \quad m = (f,k)^4, \\ &n = (f,h)^4, \quad p = (g,k)^4, \quad q = (g,h)^4. \end{aligned} \tag{7}$$

Then, the following

$$
\begin{aligned}
&J_2 = 2^2\cdot 5\cdot 7\cdot (f,f)^8, && J_3 = \frac{1}{3}\cdot 2^4\cdot 5^2\cdot 7^3\cdot (f,g)^8,\\
&J_4 = 2^9\cdot 3\cdot 7^4\cdot (k,k)^4, && J_5 = 2^9\cdot 5\cdot 7^5\cdot (m,k)^4,\\
&J_6 = 2^{14}\cdot 3^2\cdot 7^6\cdot (k,h)^4, && J_7 = 2^{14}\cdot 3\cdot 5\cdot 7^7\cdot (m,h)^4,\\
&J_8 = 2^{17}\cdot 3\cdot 5^2\cdot 7^9\cdot (p,h)^4, && J_9 = 2^{19}\cdot 3^2\cdot 5\cdot 7^9\cdot (n,h)^4,\\
&J_{10} = 2^{22}\cdot 3^2\cdot 5^2\cdot 7^{11}(q,h)^4
\end{aligned}
\tag{8}
$$

are $SL_2(k)$- invariants. Notice that we are scaling such invariants up to multiplication by a constant for computational purposes only. We display only the first two of such invariants to avoid any confusion in the definitions

$$
\begin{aligned}
J_2 =& 280\, a_8a_0 - 35\, a_7a_1 + 10\, a_6a_2 - 5\, a_5a_3 + 2\, {a_4}^2\\
J_3 =& 1050\, a_8{a_2}^2 + 1050\, {a_6}^2a_0 + 75\, a_6{a_3}^2 + 75\, {a_5}^2a_2 + 12\, {a_4}^3 + 3920\, a_8a_4a_0\\
&- 2450\, a_8a_3a_1 + 735\, a_7a_4a_1 - 2450\, a_7a_5a_0 - 175\, a_7a_3a_2 - 110\, a_6a_4a_2\\
&- 175\, a_6a_5a_1 - 45\, a_5a_4a_3
\end{aligned}
$$

In other words, we take the numerator of the corresponding transvectants since we prefer to work over $\mathbb{Z}$ instead of $\mathbb{Q}$ and then take the primitive part of each invariant. Hence, we have $J_i \in \mathbb{Z}[a_0,\dots,a_8]$, for $i = 2,\dots,8$ and J_i's are primitive polynomials. In [20] such scaling is not done and these invariants are homogenous polynomials with coefficients in $\mathbb{Q}[a_0,\dots,a_8]$ and not primitive.

Lemma 3. *For each binary octavic $f(X,Y)$, its invariants defined in Eq.(8) are primitive homogeneous polynomials $J_i \in \mathbb{Z}[a_0,\dots,a_8]$ of degree i, for $i = 2,\dots,10$. Let $f' = g(f)$, where*

$$g = \begin{pmatrix} a & b\\ c & d\end{pmatrix} \in GL_2(k),$$

and denote the corresponding $J_2,\dots,J_{10}$ of f' by $J_2',\dots,J_{10}'$. Then,

$$J_i' = (\Delta^4)^i\, J_i$$

where $\Delta = ad - bc$ and $i = 2,\dots,10$.

Proof. The first claim is immediate from the definition of the covariants and invariants. Let f and f' be two binary octavics as in the hypothesis. One can check the result computationally. □

Remark 2. *There are 68 invariants defined this way as discovered by van Gall [21,22] in 1880. Indeed, van Gall claimed 70 such invariants, but as discovered in XX-century there are only 68 of them. Perhaps, one that needs to be mentioned is J_{14} which is the discriminant of the binary octavic.*

In a couple of papers in 1892 and 1896 R. Alagna determined the algebraic relations among such invariants; see [1,2] for details. All these works have computational mistakes and are almost impossible to check.

Next we want to show that the ring of invariants $\mathcal{R}_8$ is finitely generated as a module over $k[J_2,\dots,J_7]$. First we need some auxiliary lemmas.

Lemma 4. *If $J_i = 0$, for $i = 2,\dots 7$, then the $f(X,Y)$ has a multiple root.*

Proof. Compute $J_i = 0$, for $i = 2,\dots 7$. These equations imply that

$$Res(f(X,1), f'(X,1), X) = 0,$$

where f' is the derivative of f. This proves the lemma. □

Theorem 4. *The following hold true for any octavic.*

i) An octavic has a root of multiplicity exactly four if and only if the basic invariants take the form

$$
\begin{aligned}
&J_2 = 2\cdot r^2, \quad J_3 = 2^2\cdot 3\cdot r^3, \quad J_4 = 2^6\cdot r^4, \quad J_5 = 2^6\cdot r^5,\\
&J_6 = 2^9\cdot r^6, \quad J_7 = 2^9\cdot r^7, \quad J_8 = 2^{11}\cdot 3^2\cdot r^8,
\end{aligned}
\tag{9}
$$

for some $r \neq 0$. Moreover, if the octavic has equation

$$f(x,y) = x^4(ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4),$$

then $r = e$.

ii) An octavic has a root of multiplicity 5 if and only if

$$J_i = 0, \quad for \quad i = 2, \ldots, 8.$$

Proof. i) Let

$$f(X,Y) = a_0X^8 + a_7X^7Y + \cdots + a_8Y^8$$

be an octavic with a root of multiplicity four. Let this root be at $(1,0)$. Then,

$$f(X,Y) = (a_4X^4 + a_3X^3Y + a_2X^2Y^2 + a_1XY^3 + a_0Y^4)X^4$$

Thus, for $r = a_4$, J_i for $i = 2, \ldots, 8$ are as claimed.

Conversely assume that Eq. (9) holds. Then, we have a multiple root. We assume the multiple root is at $(1,0)$. If this is the only root then $r = 0$. Thus, there is at least one more root. We assume the other root is $(0,1)$. Then the octavic takes the form

$$f(X,Y) = a_2X^6Y^2 + a_3X^5Y^3 + a_4X^4Y^4 + a_5X^3Y^5 + a_6X^2Y^6 + a_7XY^7 \tag{10}$$

and (9) becomes a system of six equations. We eliminate a_2, a_3 to get that $a_5 = 0$ or $a_4 = r$. If $a_4 = r$ and $a_5 \neq 0$ then $a_2 = a_3 = 0$ and $(1,0)$ is a root of multiplicity four. If $a_5 = 0$ then from the system we get $a_2 = 0$ or $a_6 = 0$. In both cases we have a root of multiplicity four. □

ii) Suppose $(1,0)$ is a root of multiplicity 5. Then, as in previous lemma we can take $a_8 = a_7 = a_6 = a_5 = a_4 = 0$. Then by a lemma of Hilbert [9] or by simple computation we have these invariants $J_i = 0$, for $i = 2, \ldots, 7$.

For the converse, since $J_{14} = 0$, there is a multiple root. If there is no root other than the multiple root, we are done. Otherwise, let the multiple root be at (1,0) and the other root be at (0, 1). Since $SL_2(k)$ acts 3-transitively on the points of the projective space, then as in the previous lemma the octavic becomes

$$f(X,Y) = a_2X^6Y^2 + a_3X^5Y^3 + a_4X^4Y^4 + a_5X^3Y^5 + a_6X^2Y^6 + a_7XY^7 \tag{11}$$

Compute all $J_2, \ldots J_7$. From the corresponding system of equations we can eliminate a_2, a_3, a_7. We have a few cases:

$$a_4\left(-2\,a_4\,a_6 + a_5^2\right)\left(-34\,a_4\,a_6 + 15\,a_5^2\right)\left(5476\,a_6^2a_4^2 + 2025\,a_5^4 - 6780\,a_4\,a_5^2a_6\right) = 0$$

Careful analysis of each case leads to the existence of a root of multiplicity 5. The proof is computational and we skip the details. □

Remark 3. *An alternative proof of the above can provided using the k-th subresultants of f and its derivatives. Two forms have k roots in common if and only if the first k subresultants vanish. This is equivalent to $J_2 = \cdots = J_7 = 0$.*

3.2. **The Null Cone of V_8 and Algebraic Dependencies.**

Theorem 5. *$\mathcal{R}_8$ is finitely generated as a module over $k[J_2, \ldots, J_7]$.*

Proof. By Theorem 2 we only have to prove $\mathcal{N}_8 = V(J_2, \ldots, J_7)$. For $\lambda \in k^*$, set

$$g(\lambda) := \begin{pmatrix} \lambda^{-1} & 0 \\ 0 & \lambda \end{pmatrix}$$

Suppose $J_2, \ldots, J_7$ vanish on an octavic $f \in V_8$. Then we know from Theorem 4 that f has a root of multiplicity at least 5. Let this multiple root be $(1,0)$. Then f is of the form

$$f(X,Y) = (a_5X^3 + a_6X^2Y + a_7XY^2 + a_8Y^3)\,Y^5$$

If $I \in \mathcal{R}_8$ is homogeneous of degree $s > 0$, then

$$I(f^{g(\lambda)}) = \lambda^{2s} I(a_5X^3Y^5 + \lambda^2 a_6X^2Y^6 + \lambda^3 a_7XY^7 + \lambda^4 a_8Y^8)$$

Thus $I(f^{g(\lambda)})$ is a polynomial in λ with no constant term. But since I is an $SL_2(k)$-invariant, we have $I(f^{g(\lambda)}) = I(f)$ for all λ. Thus $I(f) = 0$. Then, $\mathcal{N}_8 = V(J_2, J_3, J_4, J_5, J_6, J_7)$. This completes the proof.

□

The above lemma is proven by Shioda in a more computational way using the symbolic method; see below for more details.

Corollary 1. *$J_2, \ldots, J_7$ are algebraically independent over k because $\mathcal{R}_8$ is the coordinate ring of the 5-dimensional variety $V_8//SL_2(k)$.*

3.2.1. *Shioda's computations.* The algebraic relations between $J_2, \ldots, J_{10}$ were computed by Shioda in [20] using the symbolic method. However, we could not confirm the correctness of such results with our computations. For a binary octavic

$$f(X,Y) = \sum_{i=0}^{8} a_i X^i Y^{8-i},$$

Shioda invariants are defined as

$$\begin{aligned}
J_2 =& 2\,a_8a_0 - 16\,a_7a_1 + 56\,a_6a_2 - 112\,a_5a_3 + 70\,{a_4}^2\\
J_3 =& \frac{9}{392}\,a_8{a_2}^2 + \frac{9}{392}\,{a_6}^2a_0 + \frac{9}{5488}\,a_6{a_3}^2 + \frac{9}{5488}\,{a_5}^2a_2 + \frac{9}{560}\,a_7a_4a_1 - \frac{3}{56}\,a_7a_5a_0\\
&- \frac{3}{784}\,a_7a_3a_2 - \frac{33}{13720}\,a_6a_4a_2 - \frac{3}{784}\,a_6a_5a_1 - \frac{27}{27440}\,a_5a_4a_3 + \frac{3}{35}\,a_8a_4a_0\\
&- \frac{3}{56}\,a_8a_3a_1 + \frac{9}{34300}\,{a_4}^3
\end{aligned}$$

Notice that that definition of J_2 looks different from that of Shioda [20, page 1037], but that is because there J_2 is evaluated for

$$f(X,Y) = \sum_{i=0}^{8} \binom{8}{i} a_i X^i Y^{8-i}.$$

Now we are ready to show that the syzygies in [20, Th. 5] are not correct. Below is an example of a genus 3 hyperelliptic curve with invariants which do not satisfy Shioda relations.

Example 1. *Let a genus 3 hyperelliptic curve be given by the equation*

$$y^2 = x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

Then, its invariants are

$$\begin{aligned}
&J_2 = \frac{9}{5},\ J_3 = \frac{81}{2450},\ J_4 = \frac{837}{1568},\ J_5 = \frac{2187}{109760},\ J_6 = -\frac{6885}{43904},\\
&J_7 = -\frac{3645}{1229312},\ J_8 = -\frac{410427}{17210368},\ J_9 = \frac{234009}{172103680},\ J_{10} = \frac{5972697}{860518400}
\end{aligned}$$

Then evaluating all expressions as in Shioda's paper we have

$$\begin{aligned}
&A_6 == -\frac{3645}{9604}, && A_7 = \frac{130491}{439040}, && A_8 = -\frac{15261615}{87808},\\
&B_7 = \frac{130491}{351232}, && B_9 = \frac{1414989}{172103680}, && B_8 = \frac{143437311}{21512960},\\
&C_9 = \frac{809753208633}{376476800000}, && C_{10} = -\frac{51828148570131}{150590720000},\\
&D_{10} = -\frac{19194738471171}{385512243200}, && A_{16} = -\frac{1097050897751848407621}{925614895923200000}.
\end{aligned}$$

Substituting all these values in the first equation of [20, Thm. 5] *we get the value*

$$-\frac{546607935510034107123}{462807447961600000} \neq 0.$$

This implies that the relations determined by Shioda are not correct.

Indeed, if you take any random binary octavics then its invariants will not satisfy the Shioda's relations. Since the results in [20] do not hold, then one needs to determine explicitly the algebraic relations between the invariants in order to have an explicit description of the ring of invariants $\mathcal{R}_8$ and its field of fractions $\mathcal{S}_8$. This will be our goal for the rest of this paper.

3.2.2. *Algebraic dependencies among the invariants.* In this section we will determine algebraic relations among the invariants $J_2, \ldots, J_8$. We will use computational algebra techniques such as elimination by resultants, Groebner bases, etc. Any computer algebra package can be used to reproduce our results. Once obtained, these results can be easily verified. All our results are organized in a Maple package and will be freely made available at [19].

Without loss of generality we can assume that the generic binary octavic is given by

$$\begin{aligned} f(X,1) &= X(X-1)(X^5 - s_1X^4 + s_2X^3 - s_3X^2 + s_4X - s_5) \\ &= X^7 - (s_1+1)X^6 + (s_2+s_1)X^5 - (s_3+s_2)X^4 + (s_4+s_3)X^3 - (s_4+s_5)X^2 + s_5X \end{aligned} \tag{12}$$

Denote by

$$a := s_1 + s_2,\ b := s_2 + s_3,\ c := s_3 + s_4,\ d := s_4 + s_5,\ s := s_5.$$

Then we have

$$f(X,1) = X^7 + (-1 + b - s + d - c - a)X^6 + aX^5 - bX^4 + cX^3 - dX^2 + sX$$

We first compute the $J_2, \ldots, J_{10}$ for $f(X,1)$.

$$\begin{aligned} J_2(f) =& -35\,s + 10\,d - 10\,db + 10\,ds - 10\,d^2 + 10\,dc + 10\,da - 5\,ac + 2\,b^2 \\ J_3(f) =& -75\,c^2 + 75\,c^2b - 75\,c^2s + 75\,c^2d - 75\,c^3 - 75\,c^2a - 75\,d\,a^2 - 12\,b^3 + 110\,db \\ & - 110\,db^2 + 110\,dbs - 110\,d^2b + 110\,dbc + 110\,dba + 175\,as - 175\,asb + 175\,as^2 \\ & - 175\,asd + 175\,asc + 175\ a^2s - 735\,bs + 175\,dc + 45\,cba, \end{aligned}$$

$J_4, \ldots, J_8$ are larger expressions and we do not display them.

Our goal is to express J_8, J_9, J_{10} in terms of $J_2, \ldots, J_7$. Indeed, from Thm. 5 it is enough to express J_8 in terms of $J_2, \ldots, J_7$. Since in [20] the syzygies include expressing J_9 and J_{10} in terms of $J_2, \ldots, J_7$ we will comment on how that can be done also.

We have the following system of equations

$$\begin{cases} F_2 := J_2 - J_2(a,b,c,d,s) = 0 \\ F_3 := J_3 - J_3(a,b,c,d,s) = 0 \\ F_4 := J_4 - J_4(a,b,c,d,s) = 0 \\ F_5 := J_5 - J_5(a,b,c,d,s) = 0 \\ F_6 := J_6 - J_6(a,b,c,d,s) = 0 \\ F_7 := J_7 - J_7(a,b,c,d,s) = 0 \\ F_8 := J_8 - J_8(a,b,c,d,s) = 0 \end{cases} \tag{13}$$

We compute the equation of J_8 in terms of $J_2, \ldots, J_7$ using the following technique. Take the resultant with respect to a of the polynomials F_i, F_8, for $i = 2, \ldots 7$. Let $G_i := Res(F_i, F_8, a)$, for $i = 2, \ldots 7$. For each resultant we want to factor the result and take the primitive part. It is exactly this part that is important and it is not usually done by implementations of Grobener basis algorithms. In many cases the resultant will be factored to a power or will have factors which imply that $J_{14} = 0$. Since we are computing in an integral domain, we cancel such factors.

We continue now with the system $G_i := Res(F_i, F_8, a)$, for $i = 2, \ldots 7$ and compute the resultants $H_i := Res(G_i, G_7, b)$ for $i = 2, \ldots 6$. Hence, we are left 5 equations and transcendentals c, d, s. Continuing this process we get a degree 8 equation of J_8 in terms of the other $J_2, \ldots, J_7$, as expected by Shioda; see [20, pg. 1044]. Its leading monomial has coefficient $2^2 \cdot 3^{20} \cdot 5^{12}$. Since we are assuming that the characteristic of the field is $\neq 2, 3, 5, 7$ then we can divide by this coefficient. Hence, denote the minimal quintic by

$$J_8^5 + c_4 J_8^4 + \cdots + c_1 J_8 + c_0 = 0.$$

Since this equation is a homogenous equation of degree 40 in $J_2, \ldots, J_8$, then all other coefficients of J_8 are homogenous polynomials in $J_2, \ldots, J_7$ of degree 8, 16, 24, 32, 40 respectively. We denote the primitive part of each of these coefficients by $I_8, I_{16}, I_{24}, I_{32}, I_{40}$.

For now on we use the following notation

$$J_2 := a, \quad J_3 := b, \quad J_4 := c, \quad J_5 := d, \quad J_6 := e, \quad J_7 := f,$$

to display the expressions of $I_8, I_{16}, I_{24}, I_{32}, I_{40}$.

$$
\begin{aligned}
I_8 &= -2^7 7^5 a^4 + 2^2 5^3 7^3 3 a^2 c + 2^6 3^3 7^2 a b^2 + 2^3 5^4 7^2 a e - 2^2 3^5 5^2 7 b d - 3^3 5^4 17 c^2 \\
I_{16} &= 2^2 3^7 5^5 7^5 a^3 d^2 + 2^2 3^8 5^6 7 \cdot 11 b c^2 d + 2^3 5^8 7^4 a^2 e^2 - 2 \cdot 3^7 5^6 7^3 a b c f + 2^9 3^6 7^4 a^2 b^4 \\
&\quad - 3 \cdot 2^3 5^5 7^6 \cdot 31 a^3 c e - 2^2 3^8 5^6 7^3 a c d^2 + 2^3 3^4 5^5 7^2 11^2 b^2 c e - 2 \cdot 3^3 5^7 7^3 13 a^2 c^3 - 57173 5^5 4^7 2 a b^2 c^2 \\
&\quad + 2^6 3^6 5^3 7^5 a^3 b f + 2^2 3^8 5^5 7^4 a^2 d f + 2^7 3^5 5^2 7^6 a^4 b d - 3^8 5^7 7^3 a f^2 - 2^3 3^{10} 5^4 7^2 b^2 d^2 - 2^5 3^7 5^2 7^2 19 b^4 c \\
&\quad - 2^2 3^7 5^7 7^2 d^2 e + 2^{11} 7^{10} a^8 + 2^6 3^4 5^2 7^5 43 a^3 b^2 c - 2^8 5^4 7^7 a^5 e - 2^2 3^6 5^5 7^4 11 a^2 b c d + 2^7 3^3 5^4 7^4 a^2 b^2 e \\
&\quad + 2^3 3^3 5^4 7^5 491 a^4 c^2 - 2^6 3^8 5^2 7^3 a b^3 d - 2^5 3^9 5^3 7^2 b^3 f - 2^3 3^5 5^6 7^3 a b d e - 2^2 3^6 5^7 7^2 b e f - 2^{11} 3^3 7^7 a^5 b^2 \\
&\quad + 2^2 3^2 5^7 7^2 601 a c^2 e - 2^{10} 3^2 5^2 7^8 a^6 c + 3^5 5^9 19 c^4 + 2^2 3^9 5^7 7^2 17 c d f - 2 \cdot 5^9 7^2 c e^2
\end{aligned}
$$

The invariant I_{32} is an equation of degree 14, 8, 8, 4, 5, 4 in a, b, c, d, e, f respectively. We denote it as $I_{32} = \sum_{i=0}^{14} b_i J_2$ and display its coefficients as follows:

$$
\begin{aligned}
b_{14} &= -2^{24} \cdot 3 \cdot 7^{18} \cdot c \\
b_{13} &= 2^{21} \cdot 5 \cdot 7^{17} \cdot 41 \cdot e \\
b_{12} &= 2^{20} \cdot 3^4 \cdot 5^2 \cdot 7^{16} \cdot c^2 \\
b_{11} &= 2^{16} \cdot 3 \cdot 7^{15} \cdot c \left(13824 b^2 - 140125 e\right) \\
b_{10} &= 2^{14} \cdot 5 \cdot 7^{14} \cdot \left(-466560 b c d - 874800 d f - 283392 b^2 e - 246375 c^3 + 401750 e^2\right) \\
b_9 &= 2^{14} \cdot 3^2 \cdot 5^2 \cdot 7^{12} \left(370440 d b e - 90720 b c f - 157248 b^2 c^2 - 510300 c d^2 + 1055875 e c^2 + 595350 f^2\right) \\
b_8 &= 2^{11} 3^3 7^{10} (988722000 b^2 c e + 1190700000 b c^2 d + 3051168750 c d f + 1190700000 d^2 e - 48771072 b^4 c \\
&\quad - 1189015625 e^2 c - 100453125 c^4)
\end{aligned}
$$

Next we describe I_{40}. It is a degree 17 polynomial in J_2 and we denote it by $I_{40} = \sum_{i_0}^{17} A_i J_2^i$. Then, we have

$$
\begin{aligned}
A_{17} &= 2^{33} \cdot 7^{22} \\
A_{16} &= 2^{28} \cdot 3^2 \cdot 5 \cdot 7^{21} \cdot c^2 \\
A_{15} &= 2^{28} \cdot 3 \cdot 5^4 \cdot 7^{20} \cdot c e \\
A_{14} &= 2^{22} \cdot 5 \cdot 7^{18} \left(193536 b^2 e - 223425 c^3 - 266875 e^2\right) \\
A_{13} &= 2^{24} \cdot 3^4 \cdot 5^2 \cdot 7^{17} \left(-168 b^2 c^2 - 1975 c^2 e - 1890 f^2 - 1680 b d e + 504 b c f\right) \\
A_{12} &= 2^{18} \cdot 3 \cdot 5^3 \cdot 7^{16} \left(4898880 c d f - 6531840 d^2 e + 2668750 c e^2 + 924075 c^4 + 326592 b c^2 d - 1935360 b^2 c e\right) \\
A_{11} &= 2^{19} \cdot 5 \cdot 7^{15} \left(1020600000 b c d e + 96519600 b^2 c^3 - 172226250 c^2 d^2 - 41803776 b^4 e + 143184375 c^3 e \right. \\
&\quad \left. + 115290000 b^2 e^2 + 602791875 f^2 c - 71225000 e^3 - 306180000 b c^2 f + 1262992500 d e f\right)
\end{aligned}
$$

The other coefficients are displayed in the Appendix of the extended paper in [19]. The solution to the following problem would provide a more elegant treatment of these results.

Problem 1. *Express all invariants $I_8, I_{16}, I_{24}, I_{32}, I_{40}$ in terms of the transvectants of the binary octavics.*

We summarize the above in the following theorem.

Theorem 6. *The invariants $J_2, \ldots, J_8$ satisfy the following equation*

$$
J_8^5 + \frac{I_8}{3^4 \cdot 5^3} J_8^4 + 2 \cdot \frac{I_{16}}{3^8 \cdot 5^6} J_8^3 + \frac{I_{24}}{2 \cdot 3^{12} \cdot 5^6} J_8^2 + \frac{I_{32}}{3^{16} \cdot 5^{10}} J_8 + \frac{I_{40}}{2^2 \cdot 3^{20} \cdot 5^{12}} = 0, \tag{14}
$$

Proof. To prove that this relation holds we take a generic octavic

$$
f(x, z) = \sum_{i=1}^{8} a_i x^i z^{8-i}.
$$

Compute the invariants $J_2, \ldots, J_8$ and substitute them in the Eq. (14). We see that the equation is satisfied. This completes the proof.

□

Remark 4. *i) In terms of the coefficients of the binary octavic the above equation is a degree 40 homogenous equation.*

ii) The equation has degrees in J_i, $i = 2, \ldots, 8$, respectively 17, 10, 10, 6, 6, 5, 5.

iii) Similar relations as that in previous Theorem can be determined for J_9 and J_{10} in terms of $J_2, \ldots, J_7$. However, such relations, as expected, are too long to display.

iv) In [20] *it is commented that the field of fractions of $\mathcal{R}$ is determined by a degree 5 equation*

$$J_8^5 + a_1 J_8^4 + \ldots \alpha_5 = 0,$$

where $a_1, \ldots, a_5$ are homogenous elements in $\mathbb{Q}[J_2, \ldots, J_7]$ but are not computed; see page 1043. That equation is precisely Eq. (14)*.*

v) All coefficients of these equation can be expressed in terms of the transvectants of binary octavics.

vi) The reader can check the correctness of the above equation in [19]

Lemma 5. *The following hold true for any octavic.*

i) If an octavic has a root of multiplicity exactly four then

$$\begin{aligned} I_8 &= 2^{11} \cdot 3^6 \cdot 5^4 \cdot r^8, \quad I_{16} = 2^{22} \cdot 3^{12} \cdot 5^7 \, r^{16}, \quad I_{24} = 2^{35} \cdot 3^{18} \cdot 5^7 \, r^{24}, \\ I_{32} &= 2^{44} \cdot 3^{24} \cdot 5^{11} \, r^{32}, \quad I_{40} = 2^{57} \cdot 3^{30} \cdot 5^{12} \, r^{40}, \end{aligned} \tag{15}$$

for some $r \neq 0$. Moreover, if the octavic has equation

$$f(x, y) = x^4(ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4),$$

then $r = e$.

ii) If an octavic has a root of multiplicity 5 then

$$I_{8i} = 0, \; for \;\; i = 1, \ldots, 5.$$

Proof. i) The proof follows Theorem 4 part i) or by direct computation.

ii) Since all I_{8i} for $i = 1, \ldots, 5$ are all homogenous polynomials in terms of $J_2, \ldots, J_7$ this is an immediate consequence of Theorem 4. □

Corollary 2. *If $J_4 = J_5 = J_6 = J_7 = 0$, then $I_{24} = I_{32} = I_{40} = 0$. In this case, the Eq.* (14) *becomes*

$$J_8 \left(-10125 J_8 + 1075648 J_2^4 - 42336 J_3^2 \, J_2\right) = 0$$

The equation Eq. (14) corrects the result of [20, Thm. 1]. To compute the other syzygies we follow a similar technique replacing J_8 by J_9 or J_{10}. Indeed, both such cases are a bit easier from the computational point of view. For our purposes of determining the field of invariants $\mathcal{S}_8$ the Eq. (14) is enough.

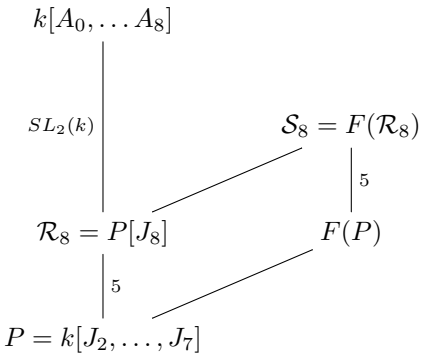

FIGURE 1. The ring of invariants $\mathcal{R}_8$ and its field of fractions

Example 2. *Let C be the generic genus 3 hyperelliptic curve with automorphism group $\mathrm{Aut}(C) \cong \mathbb{Z}_2 \times D_8$. Then C has equation*

$$C: \ y^2 = x^8 + \lambda\, x^4 + 1$$

Then, invariants I_{8i}, $i = 1, \dots 5$ of the corresponding binary form are given below.

$$\begin{aligned}
I_8 =& -2^{11} \cdot 3^4 \cdot 5^4 \ \left(9\,\lambda^2 - 2450\right) (\lambda - 14)^3 \, (\lambda + 14)^3 \\
I_{16} =& 2^{22} \cdot 3^9 \cdot 5^7 \ \left(9\,\lambda^2 + 980\right) \left(3\,\lambda^2 - 1960\right) (\lambda - 14)^6 \, (\lambda + 14)^6 \\
I_{24} =& -2^{35} \cdot 3^{12} \cdot 5^7 \ \left(9\,\lambda^2 - 9310\right) \left(9\,\lambda^2 + 980\right)^2 (\lambda - 14)^9 \, (\lambda + 14)^9 \\
I_{32} =& 2^{44} \cdot 3^{16} \cdot 5^{11} \ \left(9\,\lambda^2 - 12740\right) \left(9\,\lambda^2 + 980\right)^3 (\lambda - 14)^{12} \, (\lambda + 14)^{12} \\
I_{40} =& -2^{57} \cdot 3^{21} \cdot 5^{12} \ \left(3\,\lambda^2 - 5390\right) \left(9\,\lambda^2 + 980\right)^4 (\lambda - 14)^{15} \, (\lambda + 14)^{15}
\end{aligned}$$

If $\lambda^2 = 14$ then $I_{8i} = 0$, for $i = 1, \dots, 5$ and $J_i = 0$ for $i = 4, \dots, 8$. This corresponds to the single curve with automorphism group $\mathrm{Aut}(C) \cong \mathbb{Z}_2 \times S_4$.

Theorem 7. *Two genus 3 hyperelliptic curves C and C' in Weierstrass form, given by equations*

$$C : Z^2 = f(X, Y) \text{ and } C' : z^2 = g(X, Y)$$

are isomorphic over k if and only if there exists some $\lambda \in k \setminus \{0\}$ such that

$$J_i(C) = \lambda^i J_i(C'), \text{ for } \ i = 2, \dots, 7,$$

and $J_2, \dots J_8$ satisfy the Eq. (14)*. Moreover, the automorphism is given by*

$$\begin{aligned}
C &\to C' \\
\begin{bmatrix} X \\ Y \end{bmatrix} &\to M \cdot \begin{bmatrix} X \\ Y \end{bmatrix}
\end{aligned}$$

where $M \in GL_2(k)$ and $\lambda = (\det M)^4$.

Proof. The proof follows directly from the properties of invariants and Lemma 3. □

The above theorem gives a necessary and sufficient condition for two hyperelliptic curves to be isomorphic. However, $GL(2, k)$-invariants are preferred for identifying the isomorphism classes of curves. In order to find such invariants we need to determine the field of fractions of $\mathcal{R}_8 = k[J_2, \dots, J_7, J_8]$.

3.3. **On the invariant field of $GL_2(k)$.** Let us assume that J_2, J_3, J_4, J_5 are all nonzero. Define the invariants

$$t_1 := \frac{J_3^2}{J_2^3}, \quad t_2 := \frac{J_4}{J_2^2}, \quad t_3 := \frac{J_5}{J_2 \cdot J_3}, \quad t_4 := \frac{J_6}{J_2 \cdot J_4}, \quad t_5 := \frac{J_7}{J_2 \cdot J_5}, \quad t_6 := \frac{J_8}{J_2^4}. \tag{16}$$

Such invariants have the same degree in numerator and denominator, therefore they are $GL(2, k)$-invariants. Hence, $t_1, \dots, t_6 \in \mathcal{S}_8$. For analogy with the genus 2 case, we call them **absolute invariants**. For any two isomorphic genus 3 hyperelliptic curves C and C' we have $t_j(C) = t_j(C')$, for $j = 1, \dots, 6$. We would prefer an if and only if statement.

By substituting in Eq.(14) get an affine equation of the hyperelliptic moduli of genus 3 as

$$T(t_1, \dots, t_6) = 0 \tag{17}$$

This is an algebraic variety of dimension 5. It has degrees in $t_1, \dots, t_6$ respectively as 5, 10, 6, 6, 5, 5 and it has 25 464 terms. We denote this variety by $\mathcal{T}_3$. The equation of $\mathcal{T}_3$ is explicitly computed and very useful in the arithmetic of genus 3 curves. The reader can check it at [19].

Then we have the following theorem.

Theorem 8. *The field of invariants of binary octavics is $\mathcal{S}_8 = k(t_1, \dots, t_6)$, where $t_1, \dots, t_6$ satisfy the equation* (17)*.*

Proof. The proof of the theorem follows directly from Thm. 5 in Shioda. However, since that is based on Thm. 1 which contains syzygies which are incorrect, we provide a direct proof for this result.

We denote the roots of the octavic $f(X,Y)$ by (α_i, β_i). Every $g \in GL_2(k)$ which fixes $f(X,Y)$ permutes these roots. Thus there is an S_8 action on $\{\alpha_0, \ldots, \alpha_7\}$. The fixed field is the invariant field of $GL_2(k)$ which we denote by $\mathcal{S}_8$. We can fix $\alpha_5 = 0$, $\alpha_6 = 1$, and $\alpha_7 = \infty$. Let $s_1, \ldots, s_5$ denote the symmetric polynomials of $\alpha_0, \ldots, \alpha_4$. Then $[k(\alpha_0, \ldots, \alpha_4) : k(s_1, \ldots, s_5)] = 120$. Thus, $[k(s_1, \ldots, s_5) : \mathcal{S}_8] = 6 \cdot 7 \cdot 8 = 336$.

$$
\begin{array}{c}
k(\alpha_0, \ldots, \alpha_4) \\
\Big| \ 120 \\
k(s_1, \ldots, s_5) \\
\Big| \ 336 \\
\mathcal{S}_8 \\
\Big| \\
k(t_1, \ldots, t_6) \\
\Big| \ 5 \\
k(t_1, \ldots, t_5)
\end{array}
$$

Our goal is to determine $\mathcal{S}_8$.

Since $t_1, \ldots, t_6$ are $GL(2,k)$-invariants then $k(t_1, \ldots, t_6) \subset \mathcal{S}_8$. We know that $[k(t_1, \ldots, t_6) : k(t_1, \ldots, t_5)] = 5$, since the degree in t_6 of the irreducible polynomial from Eq. (17) is 5. If we show that $[k(s_1, \ldots, s_5) : k(t_1, \ldots, t_5)] = 5 \cdot 336$, or equivalently $[k(s_1, \ldots, s_5) : k(t_1, \ldots, t_6)] = 336$ then we are done.

The proof is computational. Compute $t_1, \ldots, t_5$ in terms of $s_1, \ldots, s_5$. This is computationally easy and we do not display these expressions here. By Bezout's theorem we know that the degree $d = [k(s_1, \ldots, s_5) : k(t_1, \ldots, t_5)]$ is $d \leq 6 \cdot 4 \cdot 5 \cdot 6 \cdot 7$, because the degrees of $i_1, \ldots, i_5$ are respectively 6, 4, 5, 6, 7. There is at least one more solution at infinity. Moreover, d must be divisible by $5 \cdot 336$. Hence, $d = 5 \cdot 336$ or $d = 2 \cdot 5 \cdot 336$.

From the system of equations we eliminate first s_5. Continuing via the resultants we eliminate also s_1 and s_4. We are left with two equations of degree 36 and 56. From Bezout's theorem, the degree $d \leq 36 \cdot 56$ and divisible by 1680. Hence $d = 1680$ and the proof is complete.

□

Corollary 3. *Two hyperelliptic genus 3 curves with nonzero invariants J_2, J_3, J_4, J_5 are isomorphic if and only if they correspond to the same point on the algebraic variety $\mathcal{T}_3$.*

Proof. The proof is an immediate consequence of the previous Theorem.

□

Since the moduli space of hyperelliptic curves is a rational variety then $\mathcal{T}_3$ must have a birational parametrization. Finding such parametrization via an equation of this size is very difficult.

3.4. **Cases when $t_1, \ldots, t_6$ are not defined.** To describe the moduli points in cases when absolute invariants are not defined is not difficult. In this case, one has to treat each case separately when any of the invariants $J_2, \ldots J_5$ are zero.

Indeed, we can define invariants depending of which of the invariants is nonzero. If $J_2 \neq 0$, then we define

$$i_1 = \frac{J_3^2}{J_2^3}, \quad i_2 = \frac{J_4}{J_2^2}, \quad i_3 = \frac{J_5^2}{J_2^5}, \quad i_4 = \frac{J_6}{J_2^3}, \quad i_5 = \frac{J_7^2}{J_2^7}, \quad i_6 = \frac{J_8}{J_2^4}$$

If $J_2 = 0$ then we pick the smallest degree invariant among $J_3, \ldots, J_7$ which is not zero. This is possible because if $J_2 = \cdots = J_7 = 0$, then from Lemma 4 the binary octavic has a double root, hence we don't have a genus 3 curve. For example, if $J_3 \neq 0$, then we define

$$i_1 = \frac{J_2^3}{J_3^2}, \quad i_2 = \frac{J_4}{J_3 \cdot J_4}, \quad i_3 = \frac{J_8}{J_3 \cdot J_5}, \quad i_4 = \frac{J_4^3}{J_3^4}, \quad i_5 = \frac{J_5^3}{J_3^5},$$

Such invariants have high degree in some cases and therefore are not suitable for computations. Hence, we prefer invariants $t_1, \ldots, t_6$ defined in Eq. (16).

In the next example we see what happens in the case when all $J_2 = J_3 = J_4 = J_5 = 0$. We see that we get a genus 0 curve in the hyperelliptic moduli $\mathcal{H}_3$.

Example 3. *Let us assume that* $J_2 = J_3 = J_4 = J_5 = 0$. *In this case* I_8 *and* $I_8 = I_{16} = 0$ *and*

$$\begin{aligned} I_{24} &= -2679687500000u^4, \\ I_{32} &= -32049481201171875 00\, u^3\, v^2, \\ I_{40} &= -30665344231796264648437 5\, u^2\, v^4 \end{aligned}$$

where $u, v \in k[a, b, c, d, e]$. *Moreover,*

$$(25I_{24}\, I_{40} - 2I_{32}^2)(25I_{24}\, I_{40} + 2I_{32}^2) = 0$$

In this case, the Eq. (14) *becomes*

$$2125764\, J_8^5 - 343000000\, J_6^4\, J_8^2 + 16206750000\, J_6^3\, J_7^2\, J_8 - 191442234375\, J_6^2\, J_7^4 = 0$$

By defining

$$\tau_1 := \frac{J_7^6}{J_6^7}, \quad \tau_2 = \frac{J_8^3}{J_6^4},$$

the Eq. (14) *becomes*

$$\begin{aligned} &-10642111561612617187500000000000\, \tau_1\, \tau_2 + 40353607000000000000000000\, {\tau_2}^2 \\ &+4649919888623184000000\, {\tau_2}^4 - 9606056659007943744\, {\tau_2}^5 - 75028202650800000000000\, {\tau_2}^3 \\ &+70163826055133644948081970214843 75\, {\tau_1}^2 - 19786546042268119734375000000\, \tau_1\, {\tau_2}^2 = 0 \end{aligned}$$

This is a genus 0 curve that can be parametrized as follows

$$\tau_1 = 2^{46}\, 3^6\, 5^{60}\, 7^{36} \cdot \frac{\left(t + 2^{11}\, 3^9\, 5^{18}\, 7^{12}\right)^2}{t^5}, \qquad \tau_2 = \frac{2^4\, 5^6\, 7^3}{3^{12}} \cdot \frac{\left(t + 2^{11}\, 3^9\, 5^{18}\, 7^{12}\right)^2}{t^2}$$

It is possible in this case to express the equation of the curve in terms of the parameter t.

3.5. **A computational package for genus 3 hyperelliptic curves.** All the computational results described in this paper are implemented in a Maple package which is made freely available at [19]. This package among other things computes the following:

i) Invariants J_i for $i = 1, \ldots, 10$. Their formulas are given in terms of the coefficients of a generic octavic

$$f(X, Y) = \sum_{i=1}^{8} a_i\, X^i Y^{8-i}$$

and can be evaluated on any given octavic.

ii) Invariants I_{5i}, for $i = 1, \ldots, 5$. Their formulas are given in terms of $J_2, \ldots, J_7$ and can be evaluated on any octavic.

iii) The equation (14) in terms of the invariants $J_2, \ldots, J_8$.

iv) The equation (17) in terms of invariants $i_1, \ldots, i_6$.

Some problems which we are further studying are finding a minimal model of a genus 3 curve over its minimal field of definition, determining an algorithm which determines when the field of moduli is a field of definition, and describing the loci of curves with fixed automorphism group in terms of invariants $t_1, \ldots, t_6$. For some of these problems and new addtional features on computational aspects of genus 3 hyperelliptic curves the reader can check [19].

An extended version of these paper with all equations displayed in its Appendix is posted in [19].

Acknowledgments: We want to thank the anonymous referee for useful suggestions on improving this paper.

References

[1] R. Alagna, *Le relazioni fra gl'invarianti d'una forma qualunque d'ottavo ordine*, Rendiconti del Circolo Matematico di Palermo **6** (1892), no. 1, 77–99 (Italian).

[2] ———, *Le relazioni fra gl'invarianti d'una forma qualunque d'ottavo ordine*, Rendiconti del Circolo Matematico di Palermo **10** (1896), no. 1, 41–74 (Italian).

[3] Lubjana Beshaj, Valmira Hoxha, and Tony Shaska, *On superelliptic curves of level n and their quotients*, Albanian J. Math. **5** (2011), no. 3, 115–137.

[4] A. Elezi and T. Shaska, *Quantum codes from superelliptic curves*, Albanian J. Math. **5** (2011), no. 4, 175 - 191.

[5] J. H. Grace and A. Young, *The algebra of invariants*, Cambridge Library Collection, Cambridge University Press, Cambridge, 2010. Reprint of the 1903 original.

[6] J. Gutierrez, D. Sevilla, and T. Shaska, *Hyperelliptic curves of genus 3 with prescribed automorphism group*, Computational aspects of algebraic curves, Lecture Notes Ser. Comput., vol. 13, World Sci. Publ., Hackensack, NJ, 2005, pp. 109–123.

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

[8] W. Haboush, *Reductive groups are geometrically reductive*, Ann. of Math. **102** (1975), 68-83.

[9] D. Hilbert, *Theory of algebraic invariants*, Cambridge University Press, Cambridge, 1993. Translated from the German and with a preface by Reinhard C. Laubenbacher; Edited and with an introduction by Bernd Sturmfels.

[10] Jun-ichi Igusa, *Arithmetic variety of moduli for genus two*, Ann. of Math. (2) **72** (1960), 612–649.

[11] P. Katsylo, *Rationality of the moduli variety of curves of genus* 3, Comment. Math. Helv. **71** (1996), no. 4, 507–524.

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

[13] Kay Magaard, Helmut Völklein, and Götz Wiesend, *The combinatorics of degenerate covers and an application for general curves of genus 3*, Albanian J. Math. **2** (2008), no. 3, 145–158. MR2495806 (2009k:14053)

[14] M. Nagata, *Invariants of a group in an affine ring*, J. Math, Kyoto Univ. **3** (1964), 369-377.

[15] E. Previato, T. Shaska, and G. S. Wijesiri, *Thetanulls of cyclic curves of small genus*, Albanian J. Math. **1** (2007), no. 4, 253–270.

[16] R. Sanjeewa and T. Shaska, *Determining equations of families of cyclic curves*, Albanian J. Math. **2** (2008), no. 3, 199–213.

[17] R. Sanjeewa, *Automorphism groups of cyclic curves defined over finite fields of any characteristics*, Albanian J. Math. **3** (2009), no. 4, 131–160.

[18] T. Shaska, *Some open problems in computational algebraic geometry*, Albanian J. Math. **1** (2007), no. 4, 297–319.

[19] ———, *Some remarks on the hyperelliptic moduli of genus 3*, arXiv:1209.1237 [math.AG].

[20] Tetsuji Shioda, *On the graded ring of invariants of binary octavics*, Amer. J. Math. **89** (1967), 1022–1046.

[21] Von Gall, *Ueber das vollständige System einer binären Form achter Ordnung*, Math. Ann. **17** (1880), no. 1, 139–152 (German).

[22] ———, *Das vollständige Formensystem einer binären Form achter Ordnung*, Math. Ann. **17** (1880), no. 1, 31–51 (German).

Department of Mathematics & Statistics, Oakland University, Rochester, MI, 48309.
E-mail address: shaska@oakland.edu