Determining the Automorphism Group of a Hyperelliptic Curve

Tanush Shaska*

Department of Mathematics

University of California at Irvine

103 MSTB, Irvine, CA 92697

ABSTRACT

In this note we discuss techniques for determining the automorphism group of a genus g hyperelliptic curve $\mathcal{X}_g$ defined over an algebraically closed field k of characteristic zero. The first technique uses the classical $GL_2(k)$-invariants of binary forms. This is a practical method for curves of small genus, but has limitations as the genus increases, due to the fact that such invariants are not known for large genus.

The second approach, which uses dihedral invariants of hyperelliptic curves, is a very convenient method and works well in all genera. First we define the normal decomposition of a hyperelliptic curve with extra automorphisms. Then dihedral invariants are defined in terms of the coefficients of this normal decomposition. We define such invariants independently of the automorphism group $\mathrm{Aut}(\mathcal{X}_g)$. However, to compute such invariants the curve is required to be in its normal form. This requires solving a nonlinear system of equations.

We find conditions in terms of classical invariants of binary forms for a curve to have reduced automorphism group A_4, S_4, A_5. As far as we are aware, such results have not appeared before in the literature.

Categories and Subject Descriptors

I.1 [**SYMBOLIC AND ALGEBRAIC MANIPULATION**]: ALGORITHMS

General Terms

Algorithms, Theory

Keywords

Hyperelliptic curve, automorphism, moduli space

*Useful suggestions of the anonymous referee are gratefully acknowledged.

1. INTRODUCTION

Let $\mathcal{X}_g$ be an algebraic curve of genus g defined over an algebraically closed field k of characteristic zero. We denote by $\mathrm{Aut}(\mathcal{X}_g)$ the group of analytic (equivalently, algebraic) automorphisms of $\mathcal{X}_g$. Then $\mathrm{Aut}(\mathcal{X}_g)$ acts on the finite set of Weierstrass points of $\mathcal{X}_g$. This action is faithful unless $\mathcal{X}_g$ is hyperelliptic, in which case its kernel is the group of order 2 containing the hyperelliptic involution of $\mathcal{X}_g$. Thus in any case, $\mathrm{Aut}(\mathcal{X}_g)$ is a finite group. This was first proved by Schwartz. In 1893 Hurwitz discovered what is now called the Riemann-Hurwitz formula. From this he derived that

$$|\mathrm{Aut}(\mathcal{X}_g)| \quad \leq \quad 84\ (g-1)$$

which is known as the Hurwitz bound. However, it is not an easy task to compute the automorphism group of a given algebraic curve. Even compiling a list of possible candidates for a small genus g is quite difficult. In [10] we provide an algorithm which computes such lists. We give a complete list for $g = 3$ and list "large" groups for $g \leq 10$. This work is based on previous work of Breuer, among many others; see [10] for a complete list of references.

If $\mathcal{X}_g$ is hyperelliptic then $\mathrm{Aut}(\mathcal{X}_g)$ is a degree 2 central extension of $\mathbb{Z}_n, D_n, A_4, S_4, A_5$. We will explain this briefly in section 2. However, computing $\mathrm{Aut}(\mathcal{X}_g)$ for a given $\mathcal{X}_g$ is still difficult. Even sophisticated computer algebra packages do not have such capabilities for $g \geq 3$. The case $g = 2$ has recently been implemented in Magma [9] and is based on methods used in [15].

In this short note we will focus on determining $\mathrm{Aut}(\mathcal{X}_g)$ for a given genus g hyperelliptic curve $\mathcal{X}_g$. We will not prove any of the results. The interested reader can check [8], [11], [12], [13], [14], or [15] for details. Most of the papers above have focused on studying the locus of all hyperelliptic curves of genus g whose automorphism group contains a subgroup G and inclusions between such loci. In this paper we combine the above results to get a treatment for all hyperelliptic curves in all genera. We generalize the notion of dihedral invariants of hyperelliptic curves with extra involutions discovered in [8] for all hyperelliptic curves with extra automorphisms (cf. Theorem 5.1.). Using these dihedral invariants and classical invariants of binary forms of degree $2g + 2$ we discover some nice necessary conditions for a curve to have reduced automorphism group A_4, S_4, A_5 (cf. section 5).

Notation: We will use the term "curve" to mean a "compact Riemann surface". Throughout this paper $\mathcal{X}_g$ denotes a hyperelliptic curve of genus $g \geq 2$. D_n denotes the dihedral group of order $2n$.

2. PRELIMINARIES

Let k be an algebraically closed field of characteristic zero and $\mathcal{X}_g$ be a genus g hyperelliptic curve given by the equation $Y^2 = F(X)$, where $\deg(F) = 2g+2$. Denote the function field of $\mathcal{X}_g$ by $K := k(X,Y)$. Then, $k(X)$ is the unique degree 2 genus zero subfield of K. K is a quadratic extension field of $k(X)$ ramified exactly at $d = 2g+2$ places $\alpha_1, \dots, \alpha_d$ of $k(X)$. The corresponding places of K are called the *Weierstrass points* of K. Let $\mathcal{P} := \{\alpha_1, \dots, \alpha_d\}$ and $G = Aut(K/k)$. Since $k(X)$ is the only genus 0 subfield of degree 2 of K, then G fixes $k(X)$. Thus, $G_0 := Gal(K/k(X)) = \langle z_0 \rangle$, with $z_0^2 = 1$, is central in G. We call the *reduced automorphism group* of K the group $\bar{G} := G/G_0$. By a theorem of Dickson, $\bar{G}$ is isomorphic to one of the following:

$$\mathbb{Z}_n, D_n, A_4, S_4, A_5,$$

with branching indices of the corresponding cover $\phi : \mathbb{P}^1 \to \mathbb{P}^1/\bar{G}$ given respectively by

$$(n,n), (2,2,n), (2,3,3), (2,4,4), (2,3,5). \tag{1}$$

In [1] all subgroups of G are classified and in [3] all groups that occur as full automorphism groups of hyperelliptic curves are classified. We use the notation of [3] and define V_n, H_n, G_n, U_n, W_2, W_3 as follows:

$$\begin{aligned}
V_n &:= \langle\, x, y \mid x^4, y^n, (xy)^2, (x^{-1}y)^2 \rangle,\\
H_n &:= \langle x, y \mid x^4, y^2x^2, (xy)^n \,\rangle,\\
G_n &:= \langle x, y \mid x^2y^n, y^{2n}, x^{-1}yxy \,\rangle,\\
U_n &:= \langle x, y \mid x^2, y^{2n}, xyxy^{n+1} \rangle,\\
W_2 &:= \langle x, y \mid x^4, y^3, yx^2y^{-1}x^2, (xy)^4 \rangle,\\
W_3 &:= \langle x, y \mid x^4, y^3, x^2(xy)^4, (xy)^8 \rangle
\end{aligned} \tag{2}$$

The following is proven in [3].

THEOREM 2.1. *The automorphism group of a hyperelliptic curve is one of the following D_n, $\mathbb{Z}_n$, V_n, H_n, G_n, U_n, $GL_2(3)$, W_2, W_3.*

The reader should be careful when reading Theorem 3.1., in [3]. It seems as the cases H_1 and G_1 (which are isomorphic to $\mathbb{Z}_4$) must be excluded. For example, for $g = 2$, according to Theorem 3.1., $H_1 \cong \mathbb{Z}_4$ must occur as an automorphism group, but it is well known that this is not the case; see [15] among many others. It is safe to exclude these cases since the group is cyclic and corresponds to case 3 of Table 1.

Also, for $g = 3$ let $N = 3$ in the case 3.d, of Table 2 in [3]. This case is not excluded from Theorem 3.1., (pg. 273). In this case the group is D_3 (dihedral group of order 6) and this group does not occur as an automorphism group of a genus 3 hyperelliptic curve; see [10].

2.1 MODULI SPACES OF COVERS

Let $\phi_0 : \mathcal{X}_g \to \mathbb{P}^1$ be the cover which corresponds to the degree 2 extension $K/k(X)$. Then, $\psi := \phi \circ \phi_0$ has monodromy group $G := \mathrm{Aut}(\mathcal{X}_g)$. From basic covering theory, the group G is embedded in the group S_n, where $n = \deg \psi$. There is an r-tuple $\bar{\sigma} := (\sigma_1, \dots, \sigma_r)$, where $\sigma_i \in S_n$ such that $\sigma_1, \dots, \sigma_r$ generate G and $\sigma_1 \cdots \sigma_r = 1$. The signature of ψ is an r-tuple of conjugacy classes $\mathbf{C} := (C_1, \dots, C_r)$ in S_n such that C_i is the conjugacy class of σ_1. We use the notation n^p to denote the conjugacy class of permutations which are a product of p cycles of length n. Using the signature of $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ given in (1) and the Riemann-Hurwitz formula, one finds out the signature of $\psi : \mathcal{X}_g \to \mathbb{P}^1$ for any given g and G. A natural question is if a given group G occurs as an automorphism group of a curve $\mathcal{X}_g$ with more then one signature $\mathbf{C}$ (cf. Theorem 2.2).

For a fixed $G, \mathbf{C}$ the family of covers $\psi : \mathcal{X}_g \to \mathbb{P}^1$ is a Hurwitz space $\mathcal{H}(G, \mathbf{C})$. This is a quasiprojective variety, not a priori connected. To show irreducibility of $\mathcal{H}(G, \mathbf{C})$ one has to show that there is only one braid orbit in the set of Nielsen classes $Ni(G, \mathbf{C})$.

There is a map

$$\Phi : \mathcal{H}(G, \mathbf{C}) \to \mathcal{H}_g$$

where $\mathcal{H}_g$ is the moduli space of genus g hyperelliptic curves. We denote by $\delta(G, \mathbf{C})$ the dimension in $\mathcal{H}_g$ of $\Phi(\mathcal{H}(G, \mathbf{C}))$. Further $i(G)$ denotes the number of involutions of G.

THEOREM 2.2. *For each $g \geq 2$, the groups G that occur as automorphism groups and their signatures $\mathbf{C}$ are given in Table 1. Moreover; $\mathcal{H}(G, \mathbf{C})$ is an irreducible algebraic variety of dimension $\delta(G, \mathbf{C})$ as given in Table 1.*

Finding algebraic descriptions of Hurwitz spaces is in general a difficult problem. In [14] it is shown that each of the spaces $\mathcal{H}(G, \mathbf{C})$ is a rational variety. Further, the inclusions between such loci are studied.

Let t be the order of an automorphism of an algebraic curve $\mathcal{X}_g$ (not necessary hyperelliptic). Hurwitz [5] showed that $t \leq 10(g-1)$. In 1895, Wiman improved this bound to be $t \leq 2(2g+1)$ and showed that it is the best possible. Thus, if a cyclic group H occurs as an automorphism group then $|H| \leq 2(2g+1)$. Indeed, this bound can be achieved for any genus via a hyperelliptic curve. For example, the curve

$$Y^2 = X(X^{2g+1} - 1)$$

has automorphism group the cyclic group of order $4g+2$. This is the second case in Table 1, when $n = 2g+1$. The family of such curves is 0-dimensional in $\mathcal{H}_g$.

Now we turn our attention to determining if a given curve $\mathcal{X}_g$ belongs to any of the families of Table 1. In other words, find conditions in terms of the coefficients of $\mathcal{X}_g$ such that $\mathcal{X}_g$ belong to a family in Table 1. This would determine the $\mathrm{Aut}(\mathcal{X}_g)$.

3. INVARIANTS OF BINARY FORMS

In this section we define the action of $GL_2(k)$ on binary forms and discuss the basic notions of their invariants. Let $k[X, Z]$ be the polynomial ring in two variables and let V_d denote the $(d+1)$-dimensional subspace of $k[X, Z]$ consisting of homogeneous polynomials.

$$f(X, Z) = a_0X^d + a_1X^{d-1}Z + \dots + a_dZ^d \tag{3}$$

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 $k[X, Z]$ as follows:

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(k), \text{ then } \quad M \begin{pmatrix} X \\ Z \end{pmatrix} = \begin{pmatrix} aX + bZ \\ cX + dZ \end{pmatrix}. \tag{4}$$

This action of $GL_2(k)$ leaves V_d invariant and acts irreducibly on V_d. Let A_0, A_1, ... , A_d be coordinate functions

G	$\bar{G}$	$\delta(G, \mathbf{C})$	$\delta,\ n,\ g$	$\mathbf{C} = (C_1, \dots C_r)$	$\phi : \mathbb{P}^1 \to \mathbb{P}^1$	i(G)
$\mathbb{Z}_2 \oplus \mathbb{Z}_n$		$\frac{2g+2}{n} - 1$	$n < g+1$	$(n^2, n^2, 2^n, \dots, 2^n)$		3
$\mathbb{Z}_{2n}$	$\mathbb{Z}_n$	$\frac{2g+1}{n} - 1$		$(n^2, 2n, 2^n, \dots, 2^n)$	(n, n)	1
$\mathbb{Z}_{2n}$		$\frac{2g}{n} - 1$	$n < g$	$(2n, 2n, 2^n, \dots, 2^n)$		1
$\mathbb{Z}_2 \oplus D_n$		$\frac{g+1}{n}$		$(n^4, 2^{2n}, \dots, 2^{2n})$		2n+3
V_n		$\frac{g+1}{n} - \frac{1}{2}$		$(n^4, 4^n, 2^{2n}, \dots, 2^{2n})$		n+3
D_{2n}	D_n	$\frac{g}{n}$		$((2n)^2, 2^{2n}, \dots, 2^{2n})$	$(2^n, 2^n, n^2)$	n+1
H_n		$\frac{g+1}{n} - 1$	$n < g+1$	$(4^n, 4^n, n^4, 2^{2n} \dots, 2^{2n})$		3
U_n		$\frac{g}{n} - \frac{1}{2}$	$g \neq 2$	$(4^n, (2n)^2, 2^{2n}, \dots, 2^{2n})$		n+1
G_n		$\frac{g}{n} - 1$	$n < g$	$(4^n, 4^n, (2n)^2, 2^{2n}, \dots, 2^{2n})$		1
$\mathbb{Z}_2 \oplus A_4$		$\frac{g+1}{6}$		$(3^8, 3^8, 2^{12}, \dots, 2^{12})$		
$\mathbb{Z}_2 \oplus A_4$		$\frac{g-1}{6}$		$(3^8, 6^4, 2^{12}, \dots, 2^{12})$		7
$\mathbb{Z}_2 \oplus A_4$	A_4	$\frac{g-3}{6}$	$\delta \neq 0$	$(6^4, 6^4, 2^{12}, \dots, 2^{12})$	$(2^6, 3^4, 3^4)$	
$SL_2(3)$		$\frac{g-2}{6}$	$\delta \neq 0$	$(4^6, 3^8, 3^8, 2^{12}, \dots, 2^{12})$		
$SL_2(3)$		$\frac{g-4}{6}$		$(4^6, 3^8, 6^4, 2^{12}, \dots, 2^{12})$		1
$SL_2(3)$		$\frac{g-6}{6}$	$\delta \neq 0$	$(4^6, 6^4, 6^4, 2^{12}, \dots, 2^{12})$		
$\mathbb{Z}_2 \oplus S_4$		$\frac{g+1}{12}$		$(3^{16}, 4^{12}, 2^{24}, \dots, 2^{24})$		
$\mathbb{Z}_2 \oplus S_4$		$\frac{g-3}{12}$		$(6^8, 4^{12}, 2^{24}, \dots, 2^{24})$		19
$GL_2(3)$		$\frac{g-2}{12}$		$(3^{16}, 8^6, 2^{24}, \dots, 2^{24})$		
$GL_2(3)$	S_4	$\frac{g-6}{12}$		$(6^8, 8^6, 2^{24}, \dots, 2^{24})$	$(2^{12}, 3^8, 4^6)$	13
W_2		$\frac{g-5}{12}$		$(4^{12}, 4^{12}, 3^{16}, 2^{24}, \dots, 2^{24})$		7
W_2		$\frac{g-9}{12}$		$(4^{12}, 4^{12}, 6^8, 2^{24}, \dots, 2^{24})$		
W_3		$\frac{g-8}{12}$		$(4^{12}, 3^{16}, 8^6, 2^{24}, \dots, 2^{24})$		1
W_3		$\frac{g-12}{12}$		$(4^{12}, 6^8, 8^6, 2^{24}, \dots, 2^{24})$		
$\mathbb{Z}_2 \oplus A_5$		$\frac{g+1}{30}$		$(3^{40}, 5^{24}, 2^{60}, \dots, 2^{60})$		
$\mathbb{Z}_2 \oplus A_5$		$\frac{g-5}{30}$		$(3^{40}, 10^{12}, 2^{60}, \dots, 2^{60})$		31
$\mathbb{Z}_2 \oplus A_5$		$\frac{g-15}{30}$		$(6^{20}, 10^{12}, 2^{60}, \dots, 2^{60})$		
$\mathbb{Z}_2 \oplus A_5$	A_5	$\frac{g-9}{30}$		$(6^{20}, 5^{24}, 2^{60}, \dots, 2^{60})$	$(2^{30}, 3^{20}, 5^{12})$	
$SL_2(5)$		$\frac{g-14}{30}$		$(4^{30}, 3^{40}, 5^{24}, 2^{60}, \dots, 2^{60})$		
$SL_2(5)$		$\frac{g-20}{30}$		$(4^{30}, 3^{40}, 10^{12}, 2^{60}, \dots, 2^{60})$		1
$SL_2(5)$		$\frac{g-24}{30}$		$(4^{30}, 6^{20}, 5^{24}, 2^{60}, \dots, 2^{60})$		
$SL_2(5)$		$\frac{g-30}{30}$		$(4^{30}, 6^{20}, 10^{12}, 2^{60}, \dots, 2^{60})$		

Table 1: Automorphism groups of hyperelliptic curves

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

$$I^M(f) := I(M(f)) \tag{5}$$

for all $f \in V_d$. Then $I^{MN} = (I^M)^N$ and Eq. (5) defines an action of $GL_2(k)$ on $k[A_0, ..., A_d]$. A homogeneous polynomial $I \in k[A_0, \dots, A_d, X, Z]$ is called a *covariant* of index s if

$$I^M(f) = \delta^s I(f)$$

where $\delta = \det(M)$. The homogeneous degree in $A_1, \dots, A_n$ is called the *degree* of I, and the homogeneous degree in X, Z is called the *order* of I. A covariant of order zero is called *invariant*. An invariant is a $SL_2(k)$-invariant on V_d.

We will use the symbolic method of classical theory to construct covariants of binary forms. Let

$$\begin{aligned} f(X,Z) &:= \sum_{i=0}^{n} \binom{n}{i} a_i X^{n-i} Z^i, \\ g(X,Z) &:= \sum_{i=0}^{m} \binom{m}{i} b_i X^{n-i} Z^i \end{aligned} \tag{6}$$

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

$$(f,g)^r := c_k \cdot \sum_{k=0}^{r} (-1)^k \binom{r}{k} \cdot \frac{\partial^r f}{\partial X^{r-k}\, \partial Y^k} \cdot \frac{\partial^r g}{\partial X^k\, \partial Y^{r-k}} \tag{7}$$

where $c_k = \frac{(m-r)!\,(n-r)!}{n!\,m!}$. It is a homogeneous polynomial in $k[X, Z]$ and therefore a covariant of order $m+n-2r$ and degree 2. In general, the r-transvection of two covariants of order m, n (resp., degree p, q) is a covariant of order $m+n-$

$2r$ (resp., degree $p+q$).

For the rest of this paper $F(X, Z)$ denotes a binary form of order $d := 2g+2$ as below

$$F(X, Z) = \sum_{i=0}^{d} a_i X^i Z^{d-i} = \sum_{i=0}^{d} \binom{n}{i} b_i X^i Z^{n-i} \tag{8}$$

where $b_i = \frac{(n-i)!\, i!}{n!} \cdot a_i$, for $i = 0, \dots, d$. We denote invariants (resp., covariants) of binary forms by I_s (resp., J_s) where the subscript s denotes the degree (resp., the order). We define the following covariants and invariants:

$$\begin{aligned}
I_2 &:= (F, F)^d, \\
J_{4j} &:= (F, F)^{d-2j}, \ j = 1, \dots, g, \\
I_4 &:= (J_4, J_4)^4, \\
I_4' &:= (J_8, J_8)^8, \\
I_6 &:= ((F, J_4)^4, (F, J_4)^4)^{d-4}, \\
I_6' &:= ((F, J_8)^8, (F, J_8)^8)^{d-8}, \\
I_6^{``} &:= ((F, J_{12})^{12}, (F, J_{12})^{12})^{d-12}, \\
I_3 &:= (F, J_d)^d, \\
M &:= ((F, J_4)^4, (F, J_8)^8)^{d-10}, \\
I_{12} &:= (M, M)^8
\end{aligned} \tag{9}$$

$GL_2(k)$-invariants are called *absolute invariants.* We define the following absolute invariants:

$$\begin{aligned}
&i_1 := \frac{I_4'}{I_2^2},\ i_2 := \frac{I_3^2}{I_2^3},\ i_3 := \frac{I_6^{``}}{I_2^3},\ j_1 := \frac{I_6'}{I_3^2}, \\
&j_2 := \frac{I_6}{I_3^2}, s_1 := \frac{I_6^2}{I_{12}},\ s_2 := \frac{(I_6')^2}{I_{12}},\ \mathfrak{v}_1 := \frac{I_6}{I_6^{``}}, \\
&\mathfrak{v}_2 := \frac{(I_4')^3}{I_3^4},\ \mathfrak{v}_3 := \frac{I_6}{I_6'},\ \mathfrak{v}_4 := \frac{(I_6^{``})^2}{I_4^3},\ \mathfrak{v}_5 := \frac{I_6^{``}}{I_6'}
\end{aligned} \tag{10}$$

For a given curve $\mathcal{X}_g$ we denote by $I(\mathcal{X}_g)$ or $i(\mathcal{X}_g)$ the corresponding invariants. Two isomorphic hyperelliptic curves have the same absolute invariants.

Remark 3.1. *It is an open problem to determine the field of invariants of binary form of degree $d \geq 7$.*

4. EQUATIONS OF CURVES

In this section we state the equations of curves in each case of Table 1. For a more detailed treatment of these spaces, including proofs, the reader can check results in [13], [14]. The reader can also check [4] where equations for each family are computed; however the main goal of the book is to study hyperelliptic Riemann surfaces with real structures. In this section G denotes a group as in the first column of Table 1, and $\mathcal{L}_g^G$ the locus of hyperelliptic genus g curves $\mathcal{X}_g$ such that G is embedded in $\mathrm{Aut}(\mathcal{X}_g)$.

4.1 $\overline{\mathrm{Aut}}(\mathcal{X}_g)$ is isomorphic to $\mathbb{Z}_n$

If $\overline{\mathrm{Aut}}(\mathcal{X}_g) \cong \mathbb{Z}_n$ then $\mathcal{X}_g$ belongs to cases 1, 2, 3 in Table 1. These loci were studied in detail in [13]. The family of curves are given below:

$$\begin{aligned}
Y^2 &= X^{nt} + \dots + a_i X^{n(t-i)} + \dots a_{t-1} X^n + 1, \\
Y^2 &= X^{nt} + \dots + a_i X^{n(t-i)} + \dots a_{t-1} X^n + 1, \\
Y^2 &= X\,(X^{nt} + \dots + a_i X^{n(t-i)} + \dots a_{t-1} X^n + 1)
\end{aligned} \tag{11}$$

where t is respectively $\frac{2g+2}{n}, \frac{2g+1}{n}, \frac{2g}{n}$. To classify these curves (up to isomorphism) we need to find invariants of the $GL_2(k)$-action on $k(a_1, \dots, a_{t-1})$. The following

$$u_i := a_1^{t-i}\, a_i \,+\, a_\delta^{t-i}\, a_{t-i}, \quad for \quad 1 \leq i \leq \delta \tag{12}$$

are called *dihedral invariants* for the genus g and the tuple

$$\mathfrak{u} := (u_1, \dots, u_\delta)$$

is called the *tuple of dihedral invariants.* It can be checked that $\mathfrak{u} = 0$ if and only if $a_1 = a_\delta = 0$. In this case replacing a_1, a_δ by $a_2, a_{\delta-1}$ in the formula above would give new invariants. The next theorem shows that the dihedral invariants generate $k(\mathcal{L}_g^G)$.

Theorem 4.1. *$\mathcal{L}_g^G$ is a δ-dimensional rational variety. Moreover, $k(\mathcal{L}_g^G) = k(u_1, \dots, u_\delta)$.*

If $n = 2$ then G is the Klein 4-group. Then $\mathcal{L}_g^G = \mathcal{L}_g$ where $\mathcal{L}_g$ is the locus of hyperelliptic curves with extra involutions, see [8]. A nice necessary and sufficient condition is found in [12] in terms of the dihedral invariants for a curve to have more than three involutions. More precisely, for such curves the relation holds:

$$2^{g-1} u_1^2 - u_g^{g+1} = 0.$$

4.2 $\overline{\mathrm{Aut}}(\mathcal{X}_g)$ is isomorphic to D_n

The dihedral group is generated by

$$D_n = \langle \sigma, \tau |\ \sigma^n = \tau^2 = 1 \rangle$$

such that

$$\sigma(X) = \varepsilon_n\, X, \quad \tau(X) = \frac{1}{X}.$$

Then σ fixes $X = 0, \infty$ and τ fixes $X = \pm 1$ and permutes 0 and ∞. We let

$$G(X) := \prod_{i=1}^{t} (X^{2n} + \lambda_i X^n + 1)$$

Then,

$$\begin{aligned}
G(X) = &X^{2nt} + a_1 X^{2nt-n} + \dots + a_t X^{nt} + \\
&a_{t-1} X^{(n-1)t} + \dots + a_1 X^n + 1
\end{aligned} \tag{13}$$

where $a_i, i = 1, \dots t$ are polynomials in terms of the symmetric polynomials $s_1, \dots, s_t$ of λ_i (i.e., $a_1 = s_1, a_2 = t + s_2, a_3 = (t-1)s_1 + s_3, a_4 := \binom{t}{n/2} + (t-2)s_2 + s_4$, etc.).

Depending on whether $0, \pm 1$, and ∞ are Weierstrass points we get the equations $Y^2 = F(X)$ where

$$\begin{aligned}
F(X) = &G(X), \quad (X^n - 1) \cdot G(X), \\
&X \cdot G(X), \quad (X^{2n} - 1) \cdot G(X) \\
&X\,(X^n - 1) \cdot G(X), \quad X\,(X^{2n} - 1) \cdot G(X)
\end{aligned} \tag{14}$$

where n is respectively as in cases 4-9 of Table 1.

Remark 4.2. *Notice that in all cases n is even; see Theorem 2.1., in [3].*

The case $Y^2 = G(X)$ corresponds to the group $\mathbb{Z}_2 \oplus D_n$. If $n = 2$, then this is a special case of $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_n$. Indeed,

$$2^{g-1} u_1^2 - u_g^{g+1} = 0$$

as expected; see [12] for details. If $n > 2$ then

$$\mathfrak{u} = (u_1, \ldots, u_g) = (0, \ldots, 0)$$

where $\mathfrak{u} = (u_1, \ldots, u_g)$ is as defined in [8].

4.3 $\overline{\textbf{Aut}}(\mathcal{X}_g)$ is isomorphic to A_4

This case is treated in detail in [13]. Let

$$G_i(X) = X^{12} - \lambda_i X^{10} - 33X^8 + 2\lambda_i X^6 - 33X^4 - \lambda_i X^2 + 1, \quad (15)$$

for $\lambda_1^2 + 108 \neq 0$. Denote by

$$G(X) := \prod_{i=1}^{\delta} G_i(X)$$

Then, each family is parameterized as in Table 2. The following lemma gives a necessary condition that a curve has automorphism group $\mathbb{Z}_2 \oplus A_4$ or $SL_2(3)$.

G	δ	Equation $Y^2 =$
$\mathbb{Z}_2 \oplus A_4$	$\frac{g+1}{6}$	$G(X)$
$\mathbb{Z}_2 \oplus A_4$	$\frac{g-1}{6}$	$(X^4 + 2i\sqrt{3}X^2 + 1) \cdot G(X)$
$\mathbb{Z}_2 \oplus A_4$	$\frac{g-3}{6}$	$(X^8 + 14X^4 + 1) \cdot G(X)$
$SL_2(3)$	$\frac{g-2}{6}$	$X(X^4 - 1) \cdot G(X)$
$SL_2(3)$	$\frac{g-4}{6}$	$X(X^4 - 1)(X^4 + 2i\sqrt{3}X^2 + 1) \cdot G(X)$
$SL_2(3)$	$\frac{g-6}{6}$	$X(X^4 - 1)(X^8 + 14X^4 + 1) \cdot G(X)$

Table 2: Hyperelliptic curves with $\overline{\textbf{Aut}}(\mathcal{X}_g) = A_4$

LEMMA 4.3. *Let $\mathcal{X}_g$ be a hyperelliptic curve of genus g with $\overline{Aut}(\mathcal{X}_g) \cong A_4$. Then, $I_4 = 0$. Moreover;*
i) if $g = 4$ then $I_2 = I_4 = I_4' = I_6' = 0$
ii) if $g = 5, 9, 12$ then $I_4 = I_6 = 0$
iii) if $g = 7, 10$ then $I_2 = I_4 = I_4' = I_6'' = 0$
iv) if $g = 8$ then $I_4 = 0$.

4.4 $\overline{\textbf{Aut}}(\mathcal{X}_g)$ is isomorphic to S_4

In this case the reduced automorphism group is generated by

$$\sigma(X) = -\frac{x-1}{x+1}, \quad \tau(X) = iX.$$

We also denote

$$\begin{aligned} G_i(X) :=& X^{24} + \lambda X^{20} + (759 - 4\lambda)X^{16} + 2(3\lambda + \\ & 1288)X^{12} + (759 - 4\lambda)X^8 + \lambda X^4 + 1, \\ R(X) :=& X^{12} - 33X^8 - 33X^4 + 1, \\ S(X) :=& X^8 + 14X^4 + 1, \\ T(X) :=& X^4 - 1. \end{aligned} \quad (16)$$

Let

$$G(X) := \prod_{i=1}^{\delta} G_i(X)$$

where δ is as in Table 1. Then, the equations of the curves in each case are $Y^2 = F(X)$ where F is as below (we suppress X):

$$F = G,\ SG,\ TG,\ STG,\ RG,\ RSG,\ RTG,\ RSTG.$$

Similar conditions in terms of the classical invariants as in the previous case can be obtained in this case also.

LEMMA 4.4. *Let $\mathcal{X}_g$ be a hyperelliptic curve of genus g with $\overline{Aut}(\mathcal{X}_g) \cong S_4$. Then, $I_4 = 0$.*

4.5 $\overline{\textbf{Aut}}(\mathcal{X}_g)$ is isomorphic to A_5

We briefly state the equations here. We denote by $G_i(X)$, $R(X)$, $S(X)$, $T(X)$ the following:

$$\begin{aligned} G_i(X) :=& (\lambda_i - 1)X^{60} - 36\,(19\lambda_i + 29)X^{55} + 6(26239\lambda_i - 42079)X^{50} \\ & - 540(23199\lambda_i - 19343)X^{45} + 105(737719\lambda_i - 953143)X^{40} \\ & - 72(1815127\lambda_i - 145087)X^{35} - 4(8302981\lambda_i + 49913771)X^{30} \\ & + 72(1815127\lambda_i - 145087)X^{25} + 105(737719\lambda_i - 953143)X^{20} \\ & + 540(23199\lambda_i - 19343)X^{15} + 6(26239\lambda_i - 42079)X^{10} \\ & + 36\,(19\lambda_i + 29)X^5 + (\lambda_i - 1) \\ R(X) :=& X^{30} + 522X^{25} - 10005X^{20} - 10005X^{15} - 522X^5 + 1 \\ S(X) :=& X^{20} - 228X^{15} + 494X^{10} + 228X^5 + 1 \\ T(X) :=& X^{10} + 10X - 1. \end{aligned} \quad (17)$$

As above we let

$$G(X) := \prod_{i=1}^{\delta} G_i(X).$$

In the order of Table 1 equations are given as $Y^2 = F(X)$ where $F(X)$ is as given as (we suppress X):

$$F = G,\ SG,\ TG,\ STG,\ RG,\ RSG,\ RTG,\ RSTG$$

These curves can be expressed as $Y^2 = M(X^2)$ or $Y^2 = X \cdot M(X^2)$ where M is a polynomial in X^2. This fact will be used in the next section. The expressions are rather large and we will not state them here. However, we get the following useful fact:

LEMMA 4.5. *Let $\mathcal{X}_g$ be a hyperelliptic curve of genus g with $\overline{Aut}(\mathcal{X}_g) \cong A_5$. Then, $I_4 = I_4' = I_6 = I_6' = I_{12} = 0$.*

5. DETERMINING THE AUTOMORPHISM GROUP OF A GIVEN CURVE

Let $\mathcal{X}_g$ be given. We want to determine $\mathrm{Aut}(\mathcal{X}_g)$. In order to find an algorithm which would work for any g we would have to check whether $\mathcal{X}_g$ can be written in any of the forms above. Thus, we want to find if there is a coordinate change

$$X \to \frac{aX + b}{cX + d}$$

which transforms $\mathcal{X}_g$ to one of the forms of section 4. This would require solving a system of equations for each case and therefore would not be efficient.

5.1 Using classical invariants

For a fixed g we know the dimension δ of the locus $\mathcal{L}_g^G$. We compute enough absolute invariants to generate this locus. Thus, we determine the loci $\mathcal{L}_g^G$ for all G in Table 1 in terms of some invariants $i_1, \ldots i_{\delta+1}$. These loci are computed only once for each g. Then, for a particular curve we simply compute these invariants and check if they generate any of the loci $\mathcal{L}_g^G$. These spaces were computed in detail in [14] for $\bar{G} = A_4$. We will illustrate with $g \leq 12$ and $\bar{G} \cong A_4, S_4, A_5$.

We define $\mathfrak{p}(\mathcal{X}_g)$ as follows:

$$\mathfrak{p}(\mathcal{X}_g) := (\mathfrak{p}_1, \mathfrak{p}_2) = \begin{cases} \mathfrak{v}_1, & \text{if } g = 4, \\ (i_1, i_2), & \text{if } g = 5, 9, \text{ and } I_2 \neq 0 \\ \mathfrak{v}_2, & \text{if } g = 5, 9, \text{ and } I_2 = 0 \\ (j_1, j_2), & \text{if } g = 7, \text{ and } I_3 \neq 0 \\ \mathfrak{v}_3, & \text{if } g = 7, \text{ and } I_3 = 0 \\ (i_1, i_3), & \text{if } g = 8, 12, \text{ and } I_2 \neq 0 \\ \mathfrak{v}_4, & \text{if } g = 8, 12, \text{ and } I_2 = 0 \\ (s_2, s_1), & \text{if } g = 10, \text{ and } I_{12} \neq 0 \\ \mathfrak{v}_5, & \text{if } g = 10, \text{ and } I_{12} = 0 \end{cases}$$

From Lemma 4.3. and results for cases $\bar{G} \cong S_4, A_5$ one can check that $\mathfrak{p}(\mathcal{X}_g)$ is well defined. Moreover, the subvariety $\mathcal{L}_g^G$ is 1-dimensional if $\bar{G}$ is isomorphic to A_4, S_4, A_5. For each parametric curve $\mathcal{X}_g$ of the previous section we compute $\mathfrak{p}(\mathcal{X}_g)$ in terms of the parameter λ. Eliminating λ gives an equation for $\mathcal{L}_g^G$, see [14] for explicit equations.

The following algorithm determines if the automorphism group of a hyperelliptic genus $g \leq 12$ curve is isomorphic to $\mathbb{Z}_2 \oplus A_4, \mathbb{Z}_2 \oplus S_4, \mathbb{Z}_2 \oplus A_5, SL_2(3), SL_2(5), GL_2(3), W_2, W_3$.

Algorithm 1:

Input: A hyperelliptic curve $\mathcal{X}_g : Y^2 = F(X, Z)$.
Output: Determine if the automorphism group $\mathrm{Aut}(\mathcal{X}_g)$ is one of $\mathbb{Z}_2 \oplus A_4$, $\mathbb{Z}_2 \oplus S_4$, $\mathbb{Z}_2 \oplus A_5$, $SL_2(3)$, $SL_2(5)$, $GL_2(3)$, W_2, W_3.

Step1: Compute $I_4(\mathcal{X}_g)$. If $I_4 \neq 0$ then $\mathrm{Aut}(\mathcal{X}_g)$ is not isomorphic to any of $\mathbb{Z}_2 \oplus A_4, \mathbb{Z}_2 \oplus S_4, \mathbb{Z}_2 \oplus A_5, SL_2(3), SL_2(5), GL_2(3), W_2, W_3$. Otherwise go to **Step 2**.
Step 2: Compute $\mathfrak{p}(\mathcal{X}_g)$.
Step 3: Find $\mathcal{L}_g^G$ which is satisfied by $\mathfrak{p}(\mathcal{X}_g)$ (equations are given in [13]). Then, $\mathrm{Aut}(\mathcal{X}_g)$ is isomorphic to G.

The definition of $\mathfrak{p}(\mathcal{X}_g)$ is a little more elaborate for $\bar{G} = \mathbb{Z}_n, D_n$ since the dimension of $\mathcal{L}_g^G$ is > 1. Once the definition of the moduli point is modified and the corresponding $\mathcal{L}_g^G$ are computed the following can be used:

Algorithm 2:

Input: A hyperelliptic curve $\mathcal{X}_g : Y^2 = F(X, Z)$.
Output: The automorphism group $\mathrm{Aut}(\mathcal{X}_g)$.

Step 1: Compute $\mathfrak{p}(\mathcal{X}_g)$.
Step 2: Find $\mathcal{L}_g^G$ which is satisfied by $\mathfrak{p}(\mathcal{X}_g)$. Then, $\mathrm{Aut}(\mathcal{X}_g)$ is isomorphic to G.

The above method of classical invariants is difficult to implement for large g. That's because finding enough absolute invariants is not an easy task for large g. Also the expressions of these invariants and the equations for the loci $\mathcal{L}_g^G$ get very large as g grows. In order to deal with these problems we use the dihedral invariants which will be explained next.

5.2 Using dihedral invariants

In section 4.1., we introduced dihedral invariants for hyperelliptic curves $\mathcal{X}_g$ such that $\mathrm{Aut}(\mathcal{X}_g) \cong \mathbb{Z}_n$. In this section we generalize this approach to all hyperelliptic curves with extra automorphisms. Theorem 5.1., makes this generalization possible.

Let $\mathcal{X}_g$ be an hyperelliptic curve with extra automorphisms. The following lemma gives a general description of how to write an equation for $\mathcal{X}_g$.

Theorem 5.1. *Let $\mathcal{X}_g$ be a hyperelliptic curve with*

$$|Aut(\mathcal{X}_g)| > 2.$$

Then, $\mathcal{X}_g$ can be written as

$$Y^2 = F(X^n), \quad or \quad Y^2 = X \cdot F(X^n), \tag{18}$$

where $n = 2$ or n is odd and divides $2g+2, 2g+1, g$. Moreover, if $n > 2$ then $Aut(\mathcal{X}_g)$ is a cyclic group.

Let $\mathcal{X}_g$ be a hyperelliptic curve with $|\mathrm{Aut}(\mathcal{X}_g)| > 2$ and written as in (18). We call this form a **decomposition** of $\mathcal{X}_g$. Let s be the smallest n that such decomposition is possible. Then,

$$Y^2 = F(X^s), \quad or \quad Y^2 = X \cdot F(X^s) \tag{19}$$

is called the **normal decomposition** or the **normal form** of $\mathcal{X}_g$ and s is called the **degree** of the decomposition. If no such decomposition is possible then we say that $s = 1$. Let $\mathcal{X}_g$ be in its normal decomposition given below:

$$\begin{aligned} Y^2 &= X^{nt} + \dots + a_i X^{n(t-i)} + \dots a_{t-1} X^n + 1, \\ Y^2 &= X \left(X^{nt} + \dots + a_i X^{n(t-i)} + \dots a_{t-1} X^n + 1 \right) \end{aligned} \tag{20}$$

where $nt = 2g+2, 2g+1, 2g$.

We define the following

$$u_i := a_1^{t-i}\, a_i \,+\, a_\delta^{t-i}\, a_{t-i}, \quad for \quad 1 \leq i \leq \delta = t-1, \tag{21}$$

which are called *dihedral invariants* for genus g and the tuple

$$\mathfrak{U}^1 := (u_1, \dots, u_\delta)$$

is called the *tuple of dihedral invariants*. It can be checked that $\mathfrak{u} = 0$ if and only if $a_1 = a_\delta = 0$. Then, let $(a_j, a_{\delta-j+1})$ be the first nonzero tuple. Replacing a_1, a_δ by $a_j, a_{\delta-j+1}$ in the formula above would give new invariants. Thus, we define

$$u_i^j := a_j^{\delta-i+1}\, a_i \,+\, a_{\delta-j}^{\delta-i+1}\, a_{\delta-i+1}, \tag{22}$$

for $1 \leq i \leq \delta$, and $1 \leq j \leq [\frac{\delta+1}{2}]$. Then

$$\mathfrak{U}^j := (u_1^j, \dots, u_m^j) \tag{23}$$

where $m = \delta - 2j$.

Algorithm 3:

Input: A hyperelliptic curve $\mathcal{X}_g : Y^2 = F(X, Z)$.
Output: The automorphism group $\mathrm{Aut}(\mathcal{X}_g)$.

Step 1: Check whether the curve has a normal decomposition. If "Yes" then go to **Step 2** otherwise $\mathrm{Aut}(\mathcal{X}_g) = \mathbb{Z}_2$
Step 2: Compute the degree s of the normal decomposition. If s is odd then $\mathrm{Aut}(\mathcal{X}_g) \cong \mathbb{Z}_{2s}$, otherwise go to **Step 3**.
Step 3: Compute the dihedral invariants $\mathfrak{U}_i^j$ of the normal decomposition. Go to **Step 4**.
Step 4: Find $\mathcal{L}_g^G$ which is satisfied by $\mathfrak{U}_i^j$. Then, $\mathrm{Aut}(\mathcal{X}_g)$ is isomorphic to G.

The above method was used in [15] and [8] to determine the automorphism group of genus 2 and 3. It has the advantages that it can be used for any g no matter how large. A disadvantage is that a nonlinear system of equations must be solved in order to determine the normal decomposition.

EXAMPLE 5.2. *For genus 2, the curve can be written as*

$$Y^2 = X^6 + a_1 X^4 + a_2 X^2 + 1$$

and its the dihedral invariants are

$$u_1 = a_1^3 + a_2^3, \qquad u_2 = 2a_1 a_2,$$

Then,

a) $G \cong V_6$ *if and only if* $(u_1, u_2) = (0, 0)$ *or*

$$(u_1, u_2) = (6750, 450).$$

b) $G \cong GL_2(3)$ *if and only if* $(u_1, u_2) = (-250, 50)$.

c) $G \cong D_6$ *if and only if*

$$u_2^2 - 220u_2 - 16u_1 + 4500 = 0,$$

for $u_2 \neq 18, 140 + 60\sqrt{5}, 50$.

d) $G \cong D_4$ *if and only if*

$$2u_1^2 - u_2^3 = 0,$$

for $u_2 \neq 2, 18, 0, 50, 450$. *Cases* $u_2 = 0, 450, 50$ *are reduced to cases a),and b) respectively, see [15] for details.*

REMARK 5.3. *The notation used in [15] to denote the groups is different.* V_6 *is this case has order 24 and in [15] is identified as* $\mathbb{Z}_3 \rtimes D_4$.

6. CLOSING REMARKS

We briefly described techniques of determining the automorphism group of a hyperelliptic curve. A combination of both methods sometime produces better results. Our goal is to combine these methods and explicitly compute loci $\mathcal{L}_g^G$ for reasonable g (i.e., $g \leq 60$).

There are polynomial time algorithms to compute the decomposition of a polynomial $F(X)$ up to an affine transformation $X \to aX + b$, see [7]. However, this is not sufficient for our purposes since we want to find such decomposition up to a liner fractional transformation $X \to \frac{aX+b}{cX+d}$. If a polynomial time algorithm would be found in this case this would make the second method preferable to the first.

Besides computing the automorphism groups the above techniques can also be used to answer other questions on hyperelliptic curves. For example dihedral invariants can be used to determine the field of moduli of a given curve. The reader can check [12] for details and open questions on the field of moduli and other computational aspects of hyperelliptic curves.

7. REFERENCES

[1] R. BRANDT AND H. STICHTENOTH, Die Automorphismengruppen hyperelliptischer Kurven, *Man. Math* **55** (1986), 83–92.

[2] TH. BREUER, Characters and automorphism groups of compact Riemann surfaces, *London Math. Soc. Lect. Notes* **280**, Cambridge Univ. Press 2000.

[3] E. BUJALANCE, J. GAMBOA, AND G. GROMADZKI, The full automorphism groups of hyperelliptic Riemann surfaces, *Manuscripta Math.* **79** (1993), no. 3-4, 267–282.

[4] E. BUJALANCE, F. J. CIRRE, J. M. GAMBOA, G. GROMADZKI, Symmetry types of hyperelliptic Riemann surfaces. Mm. Soc. Math. Fr. (N.S.), No. 86 (2001).

[5] A. HURWITZ, Über algebraische Gebilde mit eindeutigen Transformationen in sich, *Math. Ann.* **41** (1893), 403–442.

[6] The GAP Group, *GAP – Groups, Algorithms, and Programming*, Version 4.2; 2000. (`http://www.gap-system.org`)

[7] J. GUTIERREZ, A polynomial decomposition algorithm over factorial domains, Comptes Rendues Mathematiques, de Ac. de Sciences, 13 (1991), 81-86.

[8] J. GUTIERREZ AND T. SHASKA, Hyperelliptic curves with extra involutions, 2002 (submitted).

[9] THE MAGMA COMPUTATIONAL ALGEBRA SYSTEM, `http://magma.maths.usyd.edu.au/magma/`

[10] K. MAGAARD, T. SHASKA, S. SHPECTOROV, AND H. VÖLKLEIN, The locus of curves with prescribed automorphism group, *RIMS Kyoto Series*, Communications in Arithmetic Fundamental Groups, ed. H. Nakamura, 2002, 112-141.

[11] T. SHASKA, Genus 2 curves with (3,3)-split Jacobian and large automorphism group, ANTS V (Sydney, 2002), 205-218, Lect. Not. in Comp. Sci., 2369, Springer, Berlin, 2002.

[12] T. SHASKA, Computational Aspects of Hyperelliptic Curves, Computer mathematics (Beijing, 2003), Lecture Notes Ser. Comput., **10**, pg. 248-258, World Sci. Publishing, River Edge, NJ, 2003.

[13] T. SHASKA, Some special families of hyperelliptic curves, *J. Algebra Appl.*, (submitted).

[14] T. SHASKA, Subvarieties of the moduli space of hyperelliptic curves (preprint).

[15] T. SHASKA AND H. VÖLKLEIN, Elliptic subfields and automorphisms of genus two fields, Algebra and Algebraic Geometry with Applications, (West Lafayette, 2000), Lect. Not. in Comp. Sci., Springer, Berlin, 2002 (to appear).