ALBANIAN JOURNAL
OF MATHEMATICS
Volume 1, Number 4, Pages 297–319
ISSN 1930-1235: (2007)

SOME OPEN PROBLEMS IN COMPUTATIONAL ALGEBRAIC GEOMETRY

TANUSH SHASKA

To my wonderful children
Rachel, Adrianna, Eva, and Besianna.

Abstract. The development of computational techniques in the last decade has made possible to attack some classical problems of algebraic geometry from a computational viewpoint. In this survey, we briefly describe some open problems of computational algebraic geometry which can be approached from such viewpoint. Some of the problems we discuss are the decomposition of Jacobians of genus two curves, automorphisms groups of algebraic curves and the corresponding loci in the moduli space of algebraic curves $\mathcal{M}_g$, inclusions among such loci, decomposition of Jacobians of algebraic curves with automorphisms, invariants of binary forms and the hyperelliptic moduli, theta functions of curves with automorphisms, etc. We decompose Jacobians of genus 3 curves with automorphisms and determine the inclusions among the loci for algebraic curves with automorphisms of genus 3 and 4.

Contents

Key words and phrases. computational algebraic geometry, algebraic curves, automorphisms, Hurwitz spaces.

1. Introduction

Computational algebraic geometry is a very active and rapidly growing field, with many applications to other areas of mathematics, computer science, and engineering. In this survey, we will focus on some open problems of algebraic geometry which can be approached by a computational viewpoint.

The first version of this paper appeared in 2003 in the ACM, *SIGSAM Bulletin*, *Comm. Comp. Alg.*, see [26]. It was a list of problems on algebraic curves. Some of those problems were solved and many papers were written based on that modest paper. Since then I have updated the list with new problems and have included problems on higher dimensional varieties.

In the first part, we focus on algebraic curves and revisit some of the problems of the 2003 list. We report on some progress made on some of the problems and work done in other problems. Most notably, there are many papers generated on the field of moduli versus the field of definition problem.

This survey is organized in two parts. In Part 1 we survey some open problems, related to algebraic curves, which can be attacked using computational techniques. In Part 2 we discuss a couple of problems about higher dimensional varieties. When we say computational techniques we don't necessarily mean only Groebener basis and elimination techniques. Instead our understanding of computational geometry includes computational group theory, numerical methods using homotopy techniques, complex integration, combinatorial methods, etc.

Part 1 contains sections 2-7. In the second section we describe genus 2 curves with split Jacobians. There are many papers written on these topic going back to Legendre and Jacobi in the context of elliptic integrals. The problem we suggest is to compute the moduli space of covers of degree 5, 7 from a genus 2 curve to an elliptic curve. This problem is completely computational and could lead to some better understanding of some conjectures on elliptic curves; see Frey [9].

In section three, we discuss the automorphism groups of algebraic curves. There has been some important progress on this topic lately, however much more can be done. Extending some of the results to positive characteristic would be important. Further we suggest computing the equations of Hurwitz curves of genus 14 and 17.

In section 4 we study automorphism groups of algebraic curves defined over fields of positive characteristics. Determining such groups has theoretical applications as well as applications in coding theory, cryptography, etc. While a complete answer to this problem might still be out of reach, it seems that it is possible to determine such groups and equations of curves for special classes of curves.

In section 5 we study the decomposition of Jacobians of curves via the automorphisms of curves. We completely deal with the case $g = 3$. As far as we are aware this is the first time this result appears in the literature. Since now we have full

knowledge of the list of automorphism groups for any genus it seems possible (and reasonable) that such decomposition be determined for reasonably small genus (say $g \leq 10$).

In section 6, we go back to the problem of invariants of binary forms. The reader might find interesting the fact that we believe that the result of Shioda is not correct.

Denote by $S(n, r)$ the graded ring of invariants of homogeneous polynomials of order r in n variables over C. Shioda determines the structure of $S(2, 8)$, which turns out to be generated by nine invariants $J_2, \cdots, J_{10}$ satisfying five relations; see [35, On the graded ring of invariants of binary octavics. Amer. J. Math. 89 1967 1022–1046.]. He also computes explicitly five independent syzygies, and determines the corresponding syzygy-sequence. We believe such relations are not correct and should be determined using computational algebra tools.

In section 7 we introduce the problem of determining relations among theta functions for algebraic curves with automorphisms. This is a long project of the author and his collaborators; see for example [22] for more details. There is some progress on this topic lately, by some attempts to generalize Thomae's formula for cyclic curves; see [22] for references. Such formula, when known, expresses branch points of the cover $\mathcal{X} \to \mathbb{P}^1$ in terms of theta functions. Since such branch points for cyclic curves are easily determined then it becomes a problem of computational algebra to determine such relations.

Part 2 contains two sections. The problems stated here are of particular interest to the author. No effort is made to have a comprehensive list of problems in higher dimensional varieties. The first problem is to determine the degree of a rational map and the second problem is that of parameterizing surfaces.

Most of the problems suggested in this survey and software programs connected to them can be found in [8]. We have tried to make available most of the computer files where the computations are performed at:

http://algcurves.albmath.org/

Throughout this paper it is assumed that the reader is familiar with computer algebra packages as GAP [10] and the library of small groups in GAP.

Notation: Throughout this paper an "algebraic curve" means the isomorphism class of the curve defined over an algebraically closed field, unless otherwise stated.

Part 1. **Algebraic curves**

Algebraic curves are one of the oldest and most studied branches of algebraic geometry and indeed one of the most studied areas of mathematics. They provide some of the most exciting problems of classical mathematics. Meanwhile, they have found applications in many different areas of science and technology, such as computer vision, coding theory, cryptography, quantum information, biomathematics, etc. However, amazingly enough, there are some vary basic questions about algebraic curves of deep theoretical interest which still elude the community of experts in this area of research. We briefly describe a few problems of interest which can be studied using computational techniques.

2. Genus 2 curves with (n,n)-split Jacobian

In this section we focus on genus 2 curves whose Jacobians are isogenous to a product of elliptic curves. These curves have been studied extensively in the 19-th century in the context of elliptic integrals by Legendre, Jacobi, Clebsch, Hermite, Goursat, Brioschi, and Bolza et al. In the late 20th century Frey and Kani, Kuhn, Gaudry and Schost, Shaska and Voelklein, and many others have studied these curves further. They are of interest for the arithmetic of genus 2 curves as well as elliptic curves. For a complete survey on this topic see [32, 3] where [32] focuses on the computational aspects and [3] on connections of such coverings to the elliptic integral, mathematical physics, etc.

Let C be a curve of genus 2 and $\psi_1 : C \longrightarrow E$ a map of degree n, from C to an elliptic curve E, both curves defined over $\mathbb{C}$. The degree n cover $\phi : C \to E$ induces a degree n cover $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ such that the following diagram commutes

$$\begin{array}{ccc} C & \xrightarrow{\pi_C} & \mathbb{P}^1 \\ {\scriptstyle\psi}\downarrow & & \downarrow{\scriptstyle\phi} \\ E & \xrightarrow{\pi_E} & \mathbb{P}^1 \end{array}$$

Figure 1. The basic setup

Here $\pi_C : C \to \mathbb{P}^1$ and $\pi_E : E \to \mathbb{P}^1$ are the natural degree 2 covers. Let r be the number of branch points of the cover $\phi : \mathbb{P}^1 \to \mathbb{P}^1$. Then $r = 4$ or $r = 5$, with $r = 5$ being the generic case and $r = 4$ occurring for a certain 1-dimensional sub-locus of $\mathcal{L}_n$. We refer to the case $r = 5$ (resp., $r = 4$) as the **non-degenerate case**, resp., the **degenerate case**; see [25, Thm 3.1].

If $\psi_1 : C \longrightarrow E_1$ is maximal[1] (i.e., does not factor non-trivially) then there exists a maximal map $\psi_2 : C \longrightarrow E_2$, of degree n, to some elliptic curve E_2 such that there is an isogeny of degree n^2 from the Jacobian J_C to $E_1 \times E_2$. We say that J_C is (n,n)-decomposable. If the degree n is odd the pair (ψ_2, E_2) is canonically determined; see [25] for details.

We denote the moduli space of such degree n coverings $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ by $\mathcal{L}_n$. It can be viewed also as the Hurwitz space of covers $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ with ramification determined as in [25]. For our purposes, $\mathcal{L}_n$ will simply be the locus of genus 2 curves whose Jacobian is (n,n)-isogenous to a product of two elliptic curves.

The case $n = 2$ is a special case since the coverings $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ are Galois. The locus $\mathcal{L}_2$ of these genus 2 curves is a 2-dimensional subvariety of the moduli space $\mathcal{M}_2$ and is studied in detail in [34]. An equation for $\mathcal{L}_2$ is already in the work of Clebsch and Bolza. In [34] we found a birational parametrization of $\mathcal{L}_2$ by affine 2-space to study the relation between the j-invariants of the degree 2 elliptic subfields. We found a 1-dimensional family of genus 2 curves having exactly two isomorphic elliptic subfields of degree 2; this family is parameterized by the j-invariant of these subfields.

[1]Some authors would call such a map **minimal covering.**

2.1. **Covers of odd degree.** If $n > 2$, the surface $\mathcal{L}_n$ is less understood. The case $n = 3$ was initially studied by Kuhn [15] where some computations for $n = 3$ were performed. The computation of the equation of $\mathcal{L}_3$ was a major computational effort. Computational algebra techniques (i.e., Groebner basis, Buchberger algorithm) and computational algebra packages (i.e, Maple, GAP) were used. Let $K = \mathbb{C}(C)$ be genus 2 function fields of C. The ellipic subcovers E_1, E_2 correspond to degree 3 elliptic subfields of K. The number of $Aut(K)$-classes of such subfields of fixed K is 0, 1, 2 or 4; see [29] for details. Also, an equation for the locus of such C in the moduli space of genus 2 curves is computed. It was the first time to explicitly compute such spaces and the results were obtained with the help of computer algebra.

The case $n = 5$ is studied in detail in [19]. This extends earlier work for $n = 2, 3$ in Shaska [25], [29], and Shaska/Völklein [34]. The cover $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ has one of the ramification structures given in Table 1. This data lists the ramification indices > 1 over the branch points. E.g., in the last case there is one branch point that has exactly one ramified point over it, of index 3, and each of the other 3 branch points has exactly two ramified points over it, of index 2. The reader should check [25] for ramification structures of arbitrary degree.

non-degenerate:		$\big((2)^2, (2)^2, (2)^2, (2), (2)\big)$
degenerate:		
	I)	$\big((2)^2, (2)^2, (4), (2)\big)$
	II)	$\big((2)^2, (2)^2, (2)\cdot(3), (2)\big)$
	III)	$\big((2)^2, (2)^2, (2)^2, (3)\big)$

TABLE 1. ramification structure of ϕ

The main feature that distinguishes the case $n = 5$ from all other values $n > 5$ is that the cover ϕ does not determine $\psi : C \to E$ uniquely, but there is essentially **two** choices of ψ for a given ϕ. These two choices correspond to the two branch points of ϕ of ramification structure (2) (notation as in Table 1) – anyone of these two branch points can be chosen to ramify in E while the other doesn't. This phenomenon implies that the function field of $\mathcal{L}_5$ is a quadratic extension of the function field of the Hurwitz space parameterizing the covers ϕ.

The spaces $\mathcal{L}_n$ were studied by many authors in different contexts. The new results obtained in [29, 19] were the result of applying successfully computational tools and computer algebra. Continuing on the work of the above papers, we suggest the following problem:

Problem 1. Determine the locus $\mathcal{L}_n$ in $\mathcal{M}_2$ for $n = 7$. Further, determine the relation between the elliptic curves E_1 and E_2 in each case.

Using techniques from [34, 29] this becomes simply a computational problem. However, determining such loci requires the use of a Groebner basis algorithm. Computationally this seems to be difficult for $n = 7$. Notice that $n = 7$ is the first generic case of the problem since all degenerate cases occur.

2.2. **Covers of even degree.** The case when n is even is less studied. In this case there are several possible ramifications that can occur for the covering $\phi : \mathbb{P}^1 \to \mathbb{P}^1$; see [25] for the following theorem.

Theorem 2. *If n is an even number then the generic case for $\psi : C \longrightarrow E$ induce the following three cases for $\phi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$:*

I.: $\Big((2)^{\frac{n-2}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n}{2}}, (2)\Big)$

II.: $\Big((2)^{\frac{n-4}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}, (2)\Big)$

III.: $\Big((2)^{\frac{n-6}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}, (2)\Big)$

Each of the above cases has the following degenerations (two of the branch points collapse to one)

I.: (1) $\Big((2)^{\frac{n}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n}{2}}\Big)$

(2) $\Big((2)^{\frac{n-2}{2}}, (2)^{\frac{n-2}{2}}, (4)(2)^{\frac{n-6}{2}}, (2)^{\frac{n}{2}}\Big)$

(3) $\Big((2)^{\frac{n-2}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n-2}{2}}, (4)(2)^{\frac{n-4}{2}}\Big)$

(4) $\Big((3)(2)^{\frac{n-4}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n}{2}}\Big)$

II.: (1) $\Big((2)^{\frac{n-2}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}\Big)$

(2) $\Big((2)^{\frac{n-4}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}\Big)$

(3) $\Big((4)(2)^{\frac{n-8}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}\Big)$

(4) $\Big((2)^{\frac{n-4}{2}}, (4)(2)^{\frac{n-6}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}\Big)$

(5) $\Big((2)^{\frac{n-4}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n-4}{2}}, (2)^{\frac{n}{2}}\Big)$

(6) $\Big((3)(2)^{\frac{n-6}{2}}, (2)^{\frac{n-2}{2}}, (4)(2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}\Big)$

(7) $\Big((2)^{\frac{n-4}{2}}, (3)(2)^{\frac{n-4}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}\Big)$

III.: (1) $\Big((2)^{\frac{n-4}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}, (4)(2)^{\frac{n}{2}}\Big)$

(2) $\Big((2)^{\frac{n-6}{2}}, (4)(2)^{\frac{n-4}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}\Big)$

(3) $\Big((2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}, (4)(2)^{\frac{n-10}{2}}\Big)$

(4) $\Big((3)(2)^{\frac{n-8}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}\Big)$

The following problem is a natural extension of the techniques used in the odd degree case to the even degree.

Problem 3. Determine the loci $\mathcal{L}_n$ in $\mathcal{M}_2$ for $n = 4, 6$. Further, determine the relation between the elliptic curves E_1 and E_2 in each case.

We expect that the computation of such loci computationally to be easier than in the cases $n = 5$. The ramification structure in the case $n = 4$ is:

non-degenerate:		$\big((2)^2, (2), (2), (2), (2)\big)$
degenerate:		
	i)	$\big((2)^2, (2), (2), (2)^2\big)$
	ii)	$\big((2), (2), (2), (4), \ \big)$

TABLE 2. Ramification structures of ϕ for $n = 4$

Note that when n is even the choice of E_2, on contrary to the odd case, is not canonical. The reader who would like a more detailed survey on this topic should check [32, 3].

3. The automorphism group of algebraic curves

Computation of automorphism groups of compact Riemann surfaces is a classical problem that goes back to Schwartz, Hurwitz, Klein, Wiman and many others. Hurwitz showed that the order of the automorphism group of a compact Riemann surface of genus g is at most $84(g-1)$, which is known as the Hurwitz bound. Klein was mostly interested with the real counterpart of the problem, hence the term "compact Klein surfaces". Wiman studied automorphism groups of hyperelliptic curves and orders of single automorphisms.

The 20th century produced a huge amount of literature on the subject. Baily [6] gave an analytical proof of a theorem of Hurwitz: if $g \geq 2$, there exists a curve of genus g with non-trivial automorphisms. In other papers was treated the number of automorphisms of a Riemann surface; see Accola [2], Maclachlan [16], [17] among others. Accola [1] gives a formula relating the genus of a Riemann surface with the subgroups of the automorphism group; known as Accola's theorem. Harvey studied cyclic groups and Lehner and Newman maximal groups that occur as automorphism groups of Riemann surfaces.

A group of automorphisms of a compact Riemann surface X of genus g can be faithfully represented via its action on the Abelian differentials on X as a subgroup of $GL(g, \mathbf{C})$. There were many efforts to classify the subgroups G of $GL(g, \mathbf{C})$ that so arise, via the cyclic subgroups of G and conditions on the matrix elements of G. In a series of papers, I. Kuribayashi, A. Kuribayashi, and Kimura compute the lists of subgroups which arise this way for $g = 3, 4$, and 5.

By covering space theory, a finite group G acts (faithfully) on a genus g curve if and only if it has a genus g generating system. Using this purely group-theoretic condition, Breuer [7] classified all groups that act on a curve of genus ≤ 48. This was a major computational effort using the computer algebra system GAP. It greatly improved on several papers dealing with small genus, by various authors.

Of course, for each group in Breuer's list, all subgroups are also in the list. This raises the question how to pick out those groups that occur as the **full automorphism group** of a genus g curve.

Let G be a finite group, and $g \geq 2$. In [18] is studied the locus of genus g curves that admit a G-action of given type, and inclusions between such loci. We use this to study the locus of genus g curves with prescribed automorphism group G. We completely classify these loci for $g = 3$ (including equations for the corresponding curves), and for $g \leq 10$ we classify those loci corresponding to "large" G. Furthermore, such work has been continued by K. Magaard who has given complete answers for the list of groups (in characteristic 0) of algebraic curves of any genus g.

3.1. Inclusion among the loci of curves with prescribed automorphism group.

Let H and G be groups which occur as automorphism groups of genus g algebraic curves such that $H < G$. If the cover $\mathcal{X} \to \mathcal{X}^H$ is obtained as a degeneration (collapsing of branch points) of the cover $\mathcal{X} \to \mathcal{X}^G$ then the locus $\mathcal{M}(g, H)$ (locus of curves in $\mathcal{M}_g$ with automorphism group H) is a sublocus of

$\mathcal{M}(g, G)$. We are avoiding signatures here, assuming that the reader is aware of the details of moduli spaces of covers and Hurwitz spaces; for details see [18].

Problem 4. Determine the inclusion among the loci $\mathcal{M}(g, G)$ for algebraic curves defined over $\mathbb{C}$ and genus $g \leq 10$.

The case of genus 2 is well known and can be found in [34] among others. Here we briefly describe the cases $g = 3, 4$.

3.1.1. *Genus 3.* Automorphism groups of genus 3 algebraic curves are well known. Furthermore, the subvarieties of $\mathcal{M}_3$ determined by group actions and inclusions among such loci are studied in detail; see [28, 27, 30, 12, 5] among others. There are 21 groups that occur as automorphism groups of genus 3 curves. Only two groups occur with two different signatures, namely $\mathbb{Z}_2$ and V_4. Such signatures distinguish between the hyperelliptic and non-hyperelliptic case. Hence, overall we have 23 cases, twelve of which belong to the non-hyperelliptic curves and the other eleven belong to the hyperelliptic locus.

Throughout this section we use the GAP identity of the library of small groups to identify the groups. We display the list of groups in Table 1 and Table 2. The equation of the family of curves, the signature, the number of involutions N_i and the number of conjugacy classes of involutions N_c are also displayed.

	Aut $(\mathcal{X}_g)$	$\overline{\text{Aut}}(\mathcal{X}_g)$	δ	equation $y^2 = f(x)$	Id.
1	$\mathbb{Z}_2$	$\{1\}$	5	$x(x-1)(x^5 + ax^4 + bx^3 + cx^2 + dx + e)$	$(2, 1)$
2	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\mathbb{Z}_2$	3	$x^8 + a_3x^6 + a_2x^4 + a_1x^2 + 1$	$(4, 2)$
3	$\mathbb{Z}_4$	$\mathbb{Z}_2$	2	$x(x^2 - 1)(x^4 + ax^2 + b)$	$(4, 1)$
4	$\mathbb{Z}_{14}$	$\mathbb{Z}_7$	0	$x^7 - 1$	$(14, 2)$
5	$\mathbb{Z}_2^3$	D_4	2	$(x^4 + ax^2 + 1)(x^4 + bx^2 + 1)$	$(8, 5)$
6	$\mathbb{Z}_2 \times D_8$	D_8	1	$x^8 + ax^4 + 1$	$(16, 11)$
7	$\mathbb{Z}_2 \times \mathbb{Z}_4$	D_4	1	$(x^4 - 1)(x^4 + ax^2 + 1)$	$(8, 2)$
8	D_{12}	D_6	1	$x(x^6 + ax^3 + 1)$	$(12, 4)$
9	U_6	D_{12}	0	$x(x^6 - 1)$	$(24, 5)$
10	V_8	D_{16}	0	$x^8 - 1$	$(32, 9)$
11	$\mathbb{Z}_2 \times S_4$	S_4	0	$x^8 + 14x^2 + 1$	$(48, 48)$

TABLE 3. Aut (X_3) for hyperelliptic X_3

Hyperelliptic curves: Let $\mathcal{X}_g$ be a genus g hyperelliptic curve, $G :=$ Aut $(\mathcal{X}_g)$ the automorphism group, and $\sigma \in G$ its hyperelliptic involution. Then σ is in the center of G. The group $\overline{\text{Aut}}(\mathcal{X}_g) := G/\langle\sigma\rangle$ is called the *reduced automorphism group* of $\mathcal{X}_g$. It is a finite group of $PGL(2, \mathbb{C})$. Thus, $\overline{\text{Aut}}(\mathcal{X}_g)$ is isomorphic to a cyclic group, dihedral group, S_4, A_4, or A_5. Then, Aut $(\mathcal{X})g)$ is a degree 2 central extension of $\overline{\text{Aut}}(\mathcal{X}_g)$. Using these facts, for each $g \geq 2$ one determines the list of automorphism groups that occur, their signatures, and the parametric equation of corresponding curve. Moreover the inclusion among the loci $\mathcal{H}(G, C)$ is also known; see [27, 28, 11, 31, 11, 33, 24, 12] for details. Below we display the list of automorphism groups, the reduced automorphism group, a parametric equation of the curve, and the dimension of the corresponding locus. For the signature in each case

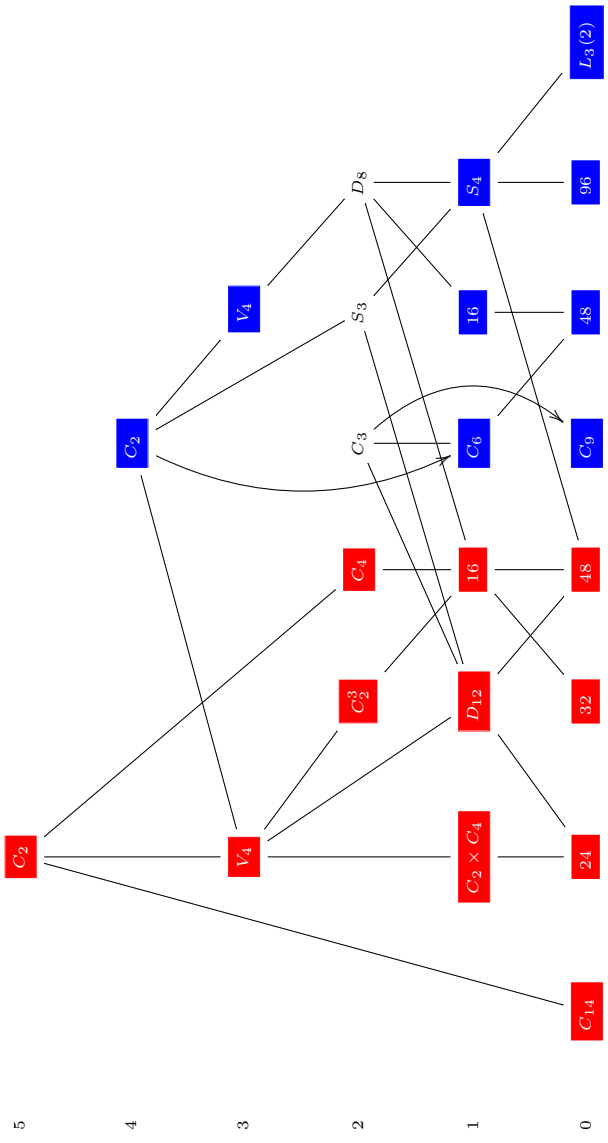
and other details the reader can check [12]. The subvarieties of $\mathcal{H}_3$ corresponding to each locus in the table are studied in details in [12]. In this paper we skip the details for the hyperelliptic moduli.

Non-hyperelliptic curves: A genus 3 non-hyperelliptic curve $\mathcal{X}$ is a ternary quartic. The group of automorphisms Aut $(\mathcal{X})$ is a finite group of order ≤ 168 with notably the Klein curve having automorphism group the simple group of order 168. The list of groups that occur as full automorphism groups of genus 3 curves are given in the table below. Each group is identified also with the Gap identity number. This number uniquely (up to isomorphism) determines the group in the library of small groups in GAP; see [10].

#	G	sig.	genus g_0	dim. δ	Id	N_i	N_c
1	V_4	(2^6)	0	3	(4,2)	3	3
2	D_8	(2^5)	0	2	(8,3)	5	3
3	S_4	$(2^3, 3)$	0	1	(24,12)	9	2
4	$C_4^2 \rtimes S_3$	$(2, 3, 8)$	0	0	(96,64)	15	2
5	16	$(2^3, 4)$	0	1	(16,13)	7	4
6	48	$(2, 3, 12)$	0	0	(48,33)	7	2
7	C_3	(3^5)	0	2	(3,1)	0	0
8	C_6	$(2, 3, 3, 6)$	0	1	(6,2)	1	1
9	C_9	$(3, 9, 9)$	0	0	(9,1)	0	0
10	$L_3(2)$	$(2, 3, 7)$	0	0	(168,42)	21	1
11	S_3	$(2^4, 3)$	0	2	(6,1)	3	1
12	C_2	(2^4)	1	4	(2,1)	1	1

TABLE 4. Automorphism groups of genus 3 non-hyperelliptic curves

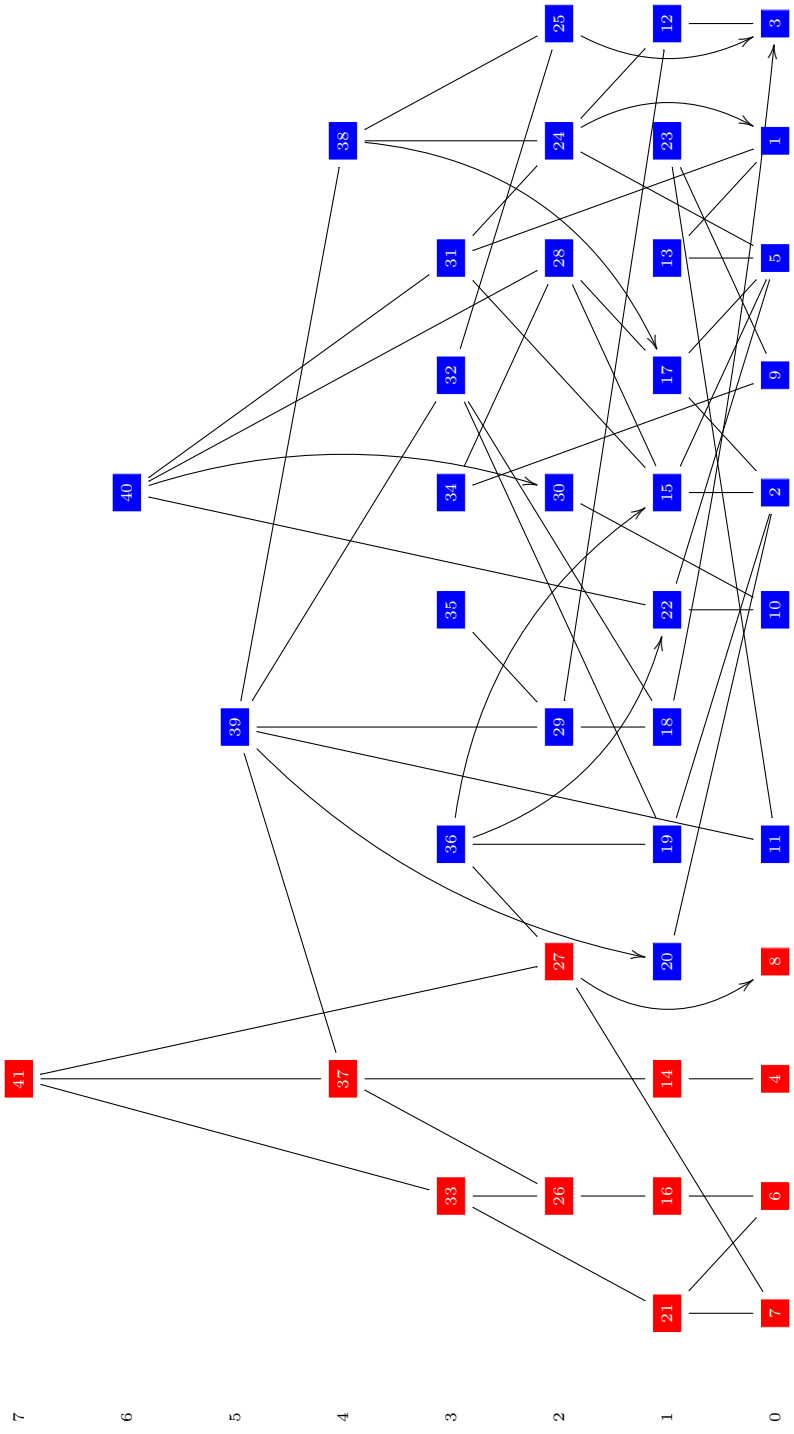
Each of these cases is an irreducible locus in $\mathcal{M}_3$. It is reasonable to know the inclusions between such loci. Such inclusions could help in determining all the cases. We display such inclusions in the following diagram.


$L_3(2)$
S_4
96
D_8
V_4
16
48
S_3
C_2
C_6
C_9
C_3
C_4
16
48
C_2^3
D_{12}
32
C_2
V_4
$C_2 \times C_4$
24
C_{14}
5
4
3
2
1
0

3.1.2. *Genus 4.* In the case of genus $g = 4$ we get the following groups and their corresponding signatures. The Table is provided by K. Magaard.

#	dim	G	ID	sig	type	subs
1	0	S_5	(120,34)	0-$(2,4,5)$	1	
2	0	$C_3 \times S_4$	(72,42)	0-$(2,3,12)$	3	
3	0		(72,40)	0-$(2,4,6)$	4	
4	0	V_{10}	(40,8)	0-$(2,4,10)$	7	
5	0	$C_6 \times S_3$	(36,12)	0-$(2,6,6)$	10	
6	0	U_8	(32,19)	0-$(2,4,16)$	16	
7	0	$SL_2(3)$	(24,3)	0-$(3,4,6)$	20	
8	0	C_{18}	(18,2)	0-$(2,9,18)$	27	
9	0	C_{15}	(15,1)	0-$(3,5,15)$	38	
10	0	C_{12}	(12,2)	0-$(4,6,12)$	45	
11	0	C_{10}	(10,2)	0-$(5,10,10)$	51	
12	1	S_3^2	(36,10)	0-$(2,2,2,3)$	12	3
13	1	S_4	(24,12)	0-$(2,2,2,4)$	18	1, 2
14	1	$C_2 \times D_5$	(20,4)	0-$(2,2,2,5)$	21	4
15	1	$C_3 \times S_3$	(18,3)	0-$(2,2,3,3)$	30	2, 5
16	1	D_8	(16,7)	0-$(2,2,2,8)$	35	6
17	1	$C_2 \times C_6$	(12,5)	0-$(2,2,3,6)$	46	2, 5
18	1	$C_2 \times S_3$	(12,4)	0-$(2,2,3,6)$	41	3
19	1	A_4	(12,3)	0-$(2,3,3,3)$	43	2
20	1	D_{10}	(10,1)	0-$(2,2,5,5)$	49	1
21	1	Q_8	(8,4)	0-$(2,4,4,4)$	59	6, 7
22	1	C_6	(6,2)	0-$(2,6,6,6)$	66	5, 10
23	1	C_5	(5,1)	0-$(5,5,5,5)$	69	9, 11
24	2	D_6	(12,4)	0-(2^5)	40	1, 5, 12
25	2	D_4	(8,3)	0-$(2^4,4)$	57	3, 13
26	2	D_4	(8,3)	0-$(2^4,4)$	56	4, 16
27	2	C_6	(6,2)	0-$(2^3,3,6)$	64	7, 8
28	2	C_6	(6,2)	0-$(2^2,3^3)$	65	15, 17
29	2	S_3	(6,1)	0-$(2^2,3^3)$	62	12, 18
30	2	C_4	(4,1)	0-$(2,4^4)$	77	10
31	3	S_3	(6,1)	0-(2^6)	61	13, 15, 24
32	3	V_4	(4,2)	1-$(2,2,2)$	72	18, 19, 25
33	3	C_4	(4,1)	0-$(2^4,4^2)$	76	21, 26
34	3	C_3	(3,1)	0-(3^6)	80	9, 28
35	3	C_3	(3,1)	0-(3^6)	81	29
36	3	C_3	(3,1)	1-$(3,3,3)$	79	15, 19, 22, 27
37	4	V_4	(4,2)	0-(2^7)	73	14, 26
38	4	V_4	(4,2)	0-(2^7)	74	17, 24, 25
39	5	C_2	(2,1)	2-$(2,2)$	82	11, 20, 29, 32, 37, 38
40	6	C_2	(2,1)	1-(2^6)	83	22, 28, 30, 31, 38
41	7	C_2	(2,1)	0-(2^{10})	84	27, 33, 37

TABLE 5. Hurwitz loci of genus 4 curves


25
12
3
38
24
23
1
31
28
13
5
32
17
9
40
34
30
15
2
35
22
10
39
29
18
36
19
11
27
20
8
41
37
14
4
33
26
16
6
21
7
7
6
5
4
3
2
1
0

In the above diagram are given inclusions among the loci of genus 4 curves. K. Magaard and S. Shpectorov have implemented programs that could compute such inclusions among loci for any reasonable genus.

Problem 5. Determine the inclusions among the loci for all $g \leq 48$

Problem 6. For any group G and a given signature σ such that G occurs as automorphism group of some genus g curve, find the corresponding equation for the curve.

Such problem is open even for small genus. For genus 3 such equations are determined in [18]. However, for $g > 3$ we are unaware of a complete list of equations.

3.2. **Hurwitz curves.** A Hurwitz curve is a genus g curve, defined over an algebraically closed field of characteristic zero, which has $84(g-1)$ automorphisms. A group G that can be realized as an automorphism group of a Hurwitz curve is called a Hurwitz group. There are a lot of papers by group-theoretists on Hurwitz groups, surveyed by Conder. It follows from Hurwitz's presentation that a Hurwitz group is perfect. Thus every quotient is again a Hurwitz group, and if such a quotient is minimal then it is a non-abelian simple group. Several infinite series of simple Hurwitz groups have been found by Conder, Malle, Kuribayashi, Zalessky, Zimmermann and others. In 2001, Wilson showed the monster is a Hurwitz group; see [18] for a complete list of references.

Klein's quartic is the only Hurwitz curve of genus $g \leq 3$. Fricke showed that the next Hurwitz group occurs for $g = 7$ and has order 504. Its group is $SL(2, 8)$, and an equation for it was computed by Macbeath in 1965. Klein's quartic and Macbeath's curve are the only Hurwitz curves whose equations are known. Further Hurwitz curves occur for $g = 14$ and $g = 17$ (and for no other values of $g \leq 19$). It is natural, to try to write equations for these Hurwitz curves of genus 14, 17.

Problem 7. Compute equations for the Hurwitz curves of genus 14, and possibly 17.

4. The automorphism groups of algebraic curves in positive characteristic

The Hurwitz bound is not valid in prime characteristic. Roquette (1970) found that the estimate

$$|G| \leq 84(g-1),$$

on the order of the automorphism group G, holds under the additional assumption $p > g+1$, with one exception: the function field $F = K(x, y)$ with $y^p - y = x^2$ has genus $g = \frac{1}{2}(p-1)$ and $8g(g+1)(2g+1)$ automorphisms.

Stichtenoth (1973) gives a general estimate for the number of automorphisms of a smooth projective curve in characteristic $p > 0$. He proves the inequality

$$|G| < 16 \cdot g^4,$$

but also with one series of exceptions: the function field $F = K(x, y)$ with $y^{p^n} + y = x^{p^{n+1}}$ has genus $g = \frac{1}{2}p^n(p^n - 1)$ and $|G| = p^{3n}(p^{3n} + 1)(p^{2n} - 1)$ automorphisms, so $|G|$ is in this case slightly larger than $16g^4$.

Let X denote a smooth, genus g algebraic curve defined over k, char $k = p > 0$. A theorem of Blichfeld on invariants (in char 0) of subgroups of $PGL_3(k)$ implies

that the genus g curve lifts to characteristic 0 for $p > 2g+1$; see [20, pg. 236-254]. Hence, for large enough p (i.e., $p > 2g+1$) methods described in [18] can be used to determine such groups. Thus, to determine the list of groups that occur as automorphism groups of genus g curves we have to classify the groups that occur for all primes $p \leq 2g+1$.

Since the methods used in [18] are no longer valid in characteristic $p > 0$, a new approach is needed for cases of small characteristic. We suggest the following long term problem:

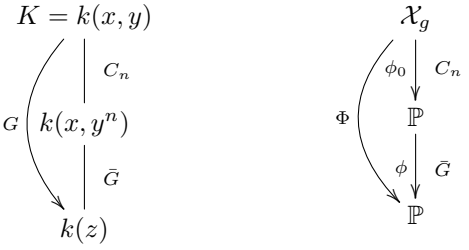
Problem 8. Determine the list of groups which occur as full automorphism groups for genus $g \leq 10$ algebraic curves defined over a field of positive characteristic.

For $g = 2$ this list is well known (it appears also in [34]). However, for $g > 3$ such list of groups is unknown. It would be nice to have a complete list for "small genus", say $g \leq 10$. Since, such lists tend to grow as genus grows, such information could be organized in a database and be very helpful to the mathematics community.

There is a class of curves for which the above problem is a bit easier. These are "cyclic" curves which will be treated next. There is an attempt in [23] to classify all groups which occur as full automorphism groups for genus $g \leq 10$ algebraic curves defined over a field of positive characteristic, including the equations of the curves.

4.1. **Cyclic curves in characteristic $p > 0$.** Let k be an algebraically closed field of characteristic p and $\mathcal{X}_g$ be a genus g cyclic curve defined over k and given by the equation $y^n = f(x)$. Let $K := k(x,y)$ be the function field of $\mathcal{X}_g$. Then $k(x)$ is degree n genus zero subfield of K. Let $G = Aut(K/k)$. Since $C_n := Gal(K/k(x)) = \langle \tau \rangle$, with $\tau^n = 1$ such that $\langle \tau \rangle \lhd G$, then group $\bar{G} := G/C_n$, also $\bar{G} \leq PGL_2(k)$. Hence $\bar{G}$ is isomorphic to one of the following: C_m, D_m, A_4, S_4, A_5, semi direct product of elementary Abelian group with cyclic group, $PSL(2,q)$ and $PGL(2,q)$, see [23].

The group $\bar{G}$ acts on $k(x)$ via the natural way. The fixed field is a genus 0 field, say $k(z)$. Thus z is a degree $|\bar{G}|$ rational function in x, say $z = \phi(x)$. We illustrate with the following diagram:



Let $\phi_0 : \mathcal{X}_g \longrightarrow \mathbb{P}^1$ be the cover which corresponds to the degree n extension $K/k(x)$. Then $\Phi := \phi \circ \phi_0$ has monodromy group $G := Aut(\mathcal{X}_g)$. From the basic covering theory, the group G is embedded in the group S_n where $n = deg\ \Phi$. There is an r-tuple $\overline{\sigma} := (\sigma_1, ..., \sigma_r)$, where $\sigma_i \in S_n$ such that $\sigma_1, ..., \sigma_r$ generate G and $\sigma_1 ... \sigma_r = 1$. The signature of ϕ is an r-tuple of conjugacy classes $\mathbf{C} := (C_1, ..., C_r)$ in S_n such that C_i is the conjugacy class of σ_i. 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 $\phi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ one finds out the signature of $\Phi : \mathcal{X}_g \longrightarrow \mathbb{P}^1$ for any given g and G.

Let E be the fixed field of G, the Hurwitz genus formula states that

$$2(g_K - 1) = 2(g_E - 1)|G| + deg(\mathfrak{D}_{K/E}) \tag{1}$$

with g_K and g_E the genera of K and E respectively and $\mathfrak{D}_{K/E}$ the different of K/E. Let $\overline{P}_1, \overline{P}_2, ..., \overline{P}_r$ be ramified primes of E. If we set $d_i = deg(\overline{P}_i)$ and let e_i be the ramification index of the $\overline{P}_i$ and let β_i be the exponent of $\overline{P}_i$ in $\mathfrak{D}_{K/E}$. Hence, Eq. (1) may be written as

$$2(g_K - 1) = 2(g_E - 1)|G| + |G| \sum_{i=1}^{r} \frac{\beta_i}{e_i} d_i \tag{2}$$

If $\overline{P}_i$ is tamely ramified then $\beta_i = e_i - 1$ or if $\overline{P}_i$ is wildly ramified then $\beta_i = e_i^* q_i + q_i - 2$ with $e_i = e_i^* q_i$, e_i^* relatively prime to p, q_i a power of p and $e_i^* | q_i - 1$.

Let $\bar{G}$ be a finite subgroup of $PGL_2(q)$ acting on the field $\mathbb{F}_q(x)$. Then, $\bar{G}$ is isomorphic to one of the following groups C_m, D_m, A_4, S_4, A_5, $U = (\mathbb{Z}/p\mathbb{Z})^t$, K_m, $PSL_2(q)$ and $PGL_2(q)$. Then, G is a degree n extension of one of these groups.

Problem 9. Determine the list of groups that occur as full automorphism groups of cyclic curves defined over an algebraically closed field of characteristic $p > 0$.

As stated above, there is an attempt in [23] to completely solve this problem.

5. On the decomposition of Jacobians of algebraic curves with automorphisms

Let $\mathcal{X}$ be a genus g algebraic curve with automorphism group $G := \text{Aut}\,(\mathcal{X})$. 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,

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

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 $H_1, \ldots, H_t \leq G$ 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 $n_1, \ldots, n_t \in \mathbb{Z}$ the conditions

$$\sum n_i n_j g_{ij} = 0, \quad \sum_{j=1}^{t} n_j g_{ij} = 0,$$

imply the isogeny relation

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

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

$$\text{Jac}\,(\mathcal{X}) \sim \text{Jac}\,(\mathcal{X}/H_2) \times \cdots \times \text{Jac}\,(\mathcal{X}/H_t)$$

The reader can check [14, 13] for the proof of the above statements.

Problem 10. Using the structure of automorphism groups of algebraic curves of genus $g \leq 48$, determine possible decompositions of Jacobians for these curves.

Next we focus on the case $g = 3$. This hopefully will give an idea to the reader that such computations are possible.

5.1. **Decomposing Jacobians of genus three algebraic curves with automorphisms.** The inclusions of the loci $\mathcal{M}_3(G, \mathbf{C})$ will help us determine relations in terms of the theta-nulls in each case. We need the following result the proof of each is elementary and we skip the details.

Let $\mathcal{X}$ be a genus 3 curve and $\sigma \in \text{Aut}\,(\mathcal{X})$ an involution. Denote by π the quotient map

$$\pi : \mathcal{X} \to \mathcal{X}/\langle\sigma\rangle$$

The quotient curve $\mathcal{X}/\langle\sigma\rangle$ has genus 0 or 1. If $g(\mathcal{X}/\langle\sigma\rangle) = 0$ then $\mathcal{X}$ is an hyperelliptic curve and σ is the hyperelliptic involution. If $g(\mathcal{X}/\langle\sigma\rangle) = 1$ then σ is called an **elliptic involution**. Then, we have the following.

Lemma 11. *Every involution of a genus 3 non-hyperelliptic curve is an elliptic involution*

Denote by N_i the number of elliptic involutions of a curve $\mathcal{X}$ and the number of conjugacy classes of involutions in Aut $(\mathcal{X})$ by N_c. Both N_i and N_c are displayed for non-hyperelliptic case. We use the information on the automorphism groups to decompose the corresponding Jacobians of 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.

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

$$\text{Jac}\,(\mathcal{X}_2) \sim \mathcal{E} \times \text{Jac}\,(\mathcal{X}_2)$$

5.1.2. *The Klein 4-group.* Next, we focus on the automorphism groups G such that $V_4 \hookrightarrow G$. As can be seen from Fig. 1, most groups contain an isomorphic copy of V_4. 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

$$\text{Jac}\,^2(\mathcal{X}) \sim \mathcal{E}_1^2 \times \mathcal{E}_2^2 \times \mathcal{E}_3^2$$

of three elliptic curves. By applying the Poincare duality we get

$$\text{Jac}\,(\mathcal{X}) \sim \mathcal{E}_1 \times \mathcal{E}_2 \times \mathcal{E}_3$$

5.1.3. *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, Jac $(\mathcal{X}) \sim \mathcal{E}_1^2 \times E_2$, for some elliptic curves $\mathcal{E}_1, \mathcal{E}_2$.

5.1.4. *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, Jac $(\mathcal{X}) \sim \mathcal{E}^3$, for some elliptic curve $\mathcal{E}$.

5.1.5. *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

$$\text{Jac }^3(\mathcal{X}) \sim \mathcal{E}_1^2 \times \mathcal{E}_2^2 \times \mathcal{E}_3^2 \times \text{Jac }^3(\mathcal{Y})$$

for three elliptic curves $\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3$ 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 $\mathcal{E}_4$. Since all the transpositions of S_3 are in the same conjugacy class then $\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3$ are isomorphic. Then by applying the Poincare duality we have that

$$\text{Jac }(X) \sim \mathcal{E}^2 \times \mathcal{E}'$$

Summarizing, we have the following:

Theorem 12. *Let $\mathcal{X}$ be a genus 3 curve and G its automorphism group. Then,*
a) If $\mathcal{X}$ is hyperelliptic then

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

$$Jac\ (\mathcal{X}) \sim \mathcal{E} \times Jac\ (\mathcal{X}_2)$$

ii) If G is isomorphic to C_2^3 then Jac (X) is isogenous to the product of three elliptic curves

$$Jac\ (\mathcal{X}) \sim \mathcal{E}_1 \times \mathcal{E}_2 \times \mathcal{E}_3$$

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 curve such that two of them are isomorphic

$$Jac\ (\mathcal{X}) \sim \mathcal{E}_1^2 \times \mathcal{E}_2$$

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 $\mathcal{X}_2$

$$Jac\ (\mathcal{X}) \sim \mathcal{E} \times Jac\ (\mathcal{X}_2)$$

ii) If G is isomorphic to V_4 then Jac (X) is isogenous to the product of three elliptic curves

$$Jac\ (\mathcal{X}) \sim \mathcal{E}_1 \times \mathcal{E}_2 \times \mathcal{E}_3$$

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

$$Jac\ (\mathcal{X}) \sim \mathcal{E}_1^2 \times \mathcal{E}_2$$

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

$$Jac\ (\mathcal{X}) \sim \mathcal{E}^3.$$

Proof. The proof of the hyperelliptic case is similar and we skip the details. The reader interested in details can check [21].

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 Fig. 2. 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. □

It is possible that given the equation of $\mathcal{X}$ one can determine the equations of the elliptic or genus 2 components in all cases of the theorem. However, we feel that is outside the scope of this paper.

Problem 13. Determine all algebraic curves of genus $g \leq 10$ such that their Jacobian splits into a product of elliptic curves.

Of course, hyperelliptic curves are an easy exercise to do. There is a little more work for non-hyperelliptic curves since a description of the automorphism group is needed.

6. Invariants of binary forms

It is an interesting and difficult problem in algebraic geometry is to obtain a generalization of the theory of elliptic modular functions to the case of higher genus. In the elliptic case this is done by the so-called *j-invariant* of elliptic curves. In the case of genus $g = 2$, Igusa (1960) gives a complete solution via *absolute invariants* i_1, i_2, i_3 of genus 2 curves. Generalizing such results to higher genus is much more difficult due to the existence of non-hyperelliptic curves. However, even restricted to the hyperelliptic moduli $\mathcal{H}_g$ the problem is still unsolved for $g \geq 3$. In other words, there is no known way of identifying isomorphism classes of hyperelliptic curves of genus $g \geq 3$. In terms of classical invariant theory this means that the field of invariants of binary forms of degree $2g + 2$ is not known for $g \geq 3$.

The following is a special case of $g = 3$.

Problem 14. Find invariants which classify the isomorphism classes of genus 3 hyperelliptic curves.

This is equivalent with determining the field of invariants of binary octavics. The covariants of binary octavics were determined in 1880 by von Gall. The generators of the ring of invariants were determined by Shioda in 1965 where the relations among the $SL_2(\mathbb{C})$ invariants were also determined. However, we believe that such relations are not correct and have been unable to verify them using computational algebra tools.

Problem 15. Determine the ring of invariants of binary octavics.

Other invariants: In a joint paper with J. Gutierrez, we find invariants that identify isomorphism classes of genus g hyperelliptic curves with extra (non-hyperelliptic) involutions; see [11]. This result gives a nice way of doing computations with these curves. We call such invariants *dihedral invariants* of hyperelliptic curves. Let $\mathcal{L}_g$ be the locus in $\mathcal{H}_g$ of hyperelliptic curves with extra involutions. $\mathcal{L}_g$ is a g-dimensional subvariety of $\mathcal{H}_g$. The dihedral invariants yield a birational parametrization of $\mathcal{L}_g$. Computationally these invariants give an efficient way of determining a point of the moduli space $\mathcal{L}_g$.

Dihedral invariants were generalized by Antoniadis and Kontogeorgis to all cyclic curves defined over any algebraically closed field (positive characteristic included); see [4] for details.

Recall that such invariants were defined for "cyclic" curves with extra involutions. Indeed they parameterize the locus of the cyclic curves on the top levels of the diagrams; see genus 3 and 4 cases.

Problem 16. Define similar invariants for all cases of cyclic curves which correspond to higher dimension locus in the moduli $\mathcal{M}_g$. In other words, describe the "cyclic" moduli similar to the hyperelliptic moduli in all cases.

Problem 17. Determine algebraic relations among "dihedral" invariants for all subloci of the "cyclic" moduli.

7. Theta functions of algebraic curves

Let $\pi\colon \mathcal{X}_g \to \mathcal{X}_{g_0}$ be a m-sheeted covering of Riemann surfaces of genus g and g_0, where $g_0 \geq 1$. The general goal is to find properties that $\mathcal{X}_g$ (or rather, the Jacobian of $\mathcal{X}_g$) has, due to the existence of the covering π. This is done by the theta functions of the $\mathcal{X}_g$. This is an old problem that goes back to Riemann and Jacobi. Many other mathematicians have worked on the cases of small genus and small degree, most notably Frobenius, Prym, Königsberger, Rosenhein, Göpel, among others. In [22] we give a historical account of such problems and the significance in modern mathematics.

Let $\mathcal{X}_g$ be an irreducible, smooth, projective curve of genus $g \geq 3$, defined over the complex field $\mathbb{C}$. We denote by $\mathcal{M}_g$ the moduli space of smooth curves of genus g and by Aut $(\mathcal{X}_g)$ the automorphism group of $\mathcal{X}_g$. Each group $G \leq$ Aut $(\mathcal{X}_g)$ acts faithfully on the g-dimensional vector space of holomorphic differential forms on $\mathcal{X}_g$.

The locus of curves in $\mathcal{M}_g$ with fixed automorphism group consists of finitely many components; to determine their number requires mapping class group action on generating systems. We denote by $\mathcal{M}_g(G, \sigma)$ be the sublocus in $\mathcal{M}_g$ of all the genus g curves $\mathcal{X}$ with $G \hookrightarrow$ Aut $(\mathcal{X})$ and signature σ.

Problem 18. Describe the loci $\mathcal{M}_g(G, \sigma)$ in terms of the theta nulls for any given g, G, and σ.

Next we describe in more detail the basic definitions and what is known about this problem.

7.1. **Theta functions and Jacobians of curves.** Let $\mathcal{H}_g$ be the Siegel upper-half space. The symplectic group $Sp(2g, \mathbb{Z})$ acts on $\mathcal{H}_g$ and there is in injection

$$\mathcal{M}_g \hookrightarrow \mathcal{H}_g / SP(2g, \mathbb{Z}) =: \mathcal{A}_g$$

For any $z \in \mathbf{C}^g$ and $\tau \in \mathcal{H}_g$ the **Riemann's theta function** is defined as

$$\theta(z, \tau) = \sum_{u \in \mathbb{Z}^g} e^{\pi i (u^t \tau u + 2u^t z)}.$$

It is holomorphic on $\mathbf{C}^g \times \mathcal{H}_g$ and satisfies

$$\theta(z + u, \tau) = \theta(z, \tau), \quad \theta(z + u\tau, \tau) = e^{-\pi i (u^t \tau u + 2z^t u)} \cdot \theta(z, \tau),$$

where $u \in \mathbb{Z}^g$.

Now let $\mathcal{X}$ be a genus $g \geq 2$ algebraic curve. Choose a symplectic homology basis for $\mathcal{X}$, say

$$\{A_1, \dots A_g, B_1, \dots, B_g\}$$

such that the intersection products $A_i \cdot A_j = B_i \cdot B_j = 0$ and $A_i \cdot B_j = \delta_{ij}$.

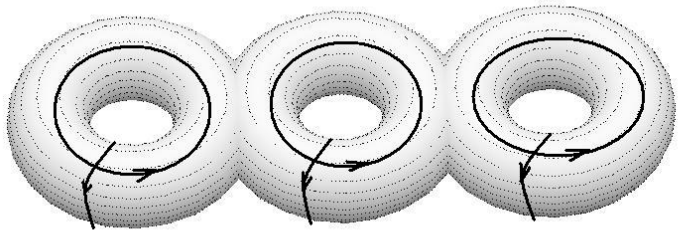


FIGURE 2. A symplectic basis for a genus 3 Riemann surface

We choose a basis $\{w_i\}$ for the space of holomorphic 1-forms such that $\int_{A_i} w_j = \delta_{ij}$. The matrix $\Omega = \left[\int_{B_i} w_j\right]$ is the period matrix of $\mathcal{X}$ and $\Omega \in \mathcal{H}_g$. The columns of the matrix $[I\ |\Omega]$ form a lattice L in $\mathbf{C}^g$ and the Jacobian Jac $(\mathcal{X})$ of $\mathcal{X}$ is Jac $(\mathcal{X}) = \mathbf{C}^g/L$. The **Riemann's theta function** of $\mathcal{X}$ with respect to the above basis is

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

and the locus

$$\Theta := \{z \in \mathbf{C}^g/L : \theta(z, \Omega) = 0\}$$

is called the **theta divisor** of $\mathcal{X}$. Points of order n on Jac $(\mathcal{X})$ are called the $\frac{1}{n}$-**periods**. In the next section we will use the half-periods and quarter-periods to describe the locus of curves in $\mathcal{M}_g$ with fixed automorphism group. For any two half-periods α, β we identify them with their images in $\mathbb{H}_1(\mathcal{X}_g, \mathbb{Z}_2)$, then the **Weil pairing** is defined as

$$|\alpha, \beta| = (-1)^{\alpha \cdot \beta}$$

where $\alpha \cdot \beta$ is the intersection product.

Problem 19. Let G be an automorphism group of a genus $\mathcal{X}_g$ curve and $\mathcal{M}_g(G, \sigma)$ denote the locus of genus g curves with automorphism group G of some signature σ. For $g \geq 4$, describe the locus $\mathcal{M}_g(G, \sigma)$ in terms of the vanishing theta-nulls.

Part 2. Higher dimension varieties

In this part we suggest some problems on higher dimensional varieties. This is by no means a list which includes the most important problems, but simply a list of problems which have special interest to the author.

8. The degree of a rational map

Let k be a field and $\phi : k^n \to k^m$ be a rational map. It is an important problem in algebraic geometry to determine the degree of the map phi. Let us assume that

$$\begin{aligned} \phi : \ & k^n \to k^m \\ & (x_1, \ldots, x_n) \to (f_1, \ldots, f_m) \end{aligned}$$

where $f_1, \ldots, f_m \in k(x_1, \ldots, x_m)$. We assume that $f_i = \frac{p_i(x)}{q_i(x)}$ and $\deg f_i = d_i$, for $i = 1, \ldots, m$. The classical way to determine the degree of such map is as follows: pick a general point $y = (y_1, \ldots, y_m) \in k^m$ such that $\phi(x) = y$. Solve the system of equations

$$\begin{cases} p_1(x) - y_1 q_1(x) = 0 \\ \qquad\qquad\qquad \ldots \\ \qquad\qquad\qquad \ldots \\ p_m(x) - y_m q_m(x) = 0 \end{cases}$$

the number of solutions of such system is bounded by $\Pi_{i=1}^m d_i$. There are some computational issues with this approach though. First, how do we make sure that the point $y \in k^m$ is a generic point. Second, the solution of the above system will involve a Groebener basis argument. Such method is extremely inefficient and will not work well for high degrees.

Problem 20. Combine the symbolic and numerical methods to design an efficient algorithm for determining the degree of a rational map.

There are some attempts to do this by Sommesse et al. However, we are still not aware of how efficient their methods are and if they have been implemented.

9. Parameterizing surfaces

It is a well known fact that if an algebraic curve has genus zero than it can be parameterizable. There are many papers on the parametrization of algebraic curves. The algorithms on parametrization of curves are quite efficient. Furthermore, there are even some results on how to find a "good" parametrization. There are no analogue results for higher dimensional varieties, even though there have been some attempts for algebraic surfaces. The following problem is important theoretically and in applications. [24]

Problem 21. Let $\mathcal{X}$ be a parametric algebraic surface. Design an algorithm which finds a parametrization of $\mathcal{X}$.

While many authors have studied this problem, we are not aware of any results which would do this efficiently.

10. Acknowledgements

Some of the problems and ideas described in this survey come from many discussions with my collaborators, my students, and other colleagues. I would like to thank them all for sharing their knowledge and insight. In particular, I would like to thank K. Magaard for sharing the tables of automorphism groups with me.

References

[1] Robert D. M. Accola, *On the number of automorphisms of a closed Riemann surface*, Trans. Amer. Math. Soc. **131** (1968), 398–408. MR MR0222281 (36 #5333)

[2] ———, *Two theorems on Riemann surfaces with noncyclic automorphism groups.*, Proc. Amer. Math. Soc. **25** (1970), 598–602. MR MR0259105 (41 #3747)

[3] Robert D. M. Accola and Emma Previato, *Covers of tori: genus two*, Lett. Math. Phys. **76** (2006), no. 2-3, 135–161. MR MR2235401 (2007c:14019)

[4] Jannis A. Antoniadis and Aristides Kontogeorgis, *On cyclic covers of the projective line*, Manuscripta Math. **121** (2006), no. 1, 105–130. MR MR2258533 (2007f:14025)

[5] H. Babu and P. Venkataraman, *Group action on genus 3 curves and their Weierstrass points*, Computational aspects of algebraic curves, Lecture Notes Ser. Comput., vol. 13, World Sci. Publ., Hackensack, NJ, 2005, pp. 264–272. MR MR2182045 (2006h:14044)

[6] Walter L. Baily, Jr., *On the automorphism group of a generic curve of genus* > 2, J. Math. Kyoto Univ. **1** (1961/1962), no. 101–108; correction, 325. MR MR0142552 (26 #121)

[7] Thomas Breuer, *Characters and automorphism groups of compact Riemann surfaces*, London Mathematical Society Lecture Note Series, vol. 280, Cambridge University Press, Cambridge, 2000. MR MR1796706 (2002i:14034)

[8] Algebraic curves and their applications, *"http://algcurves.albmath.org/"*, 2007.

[9] Gerhard Frey, *On elliptic curves with isomorphic torsion structures and corresponding curves of genus* 2, Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993), Ser. Number Theory, I, Int. Press, Cambridge, MA, 1995, pp. 79–98. MR MR1363496 (96k:11067)

[10] GAP, *Groups, algorithms and programming, http://www.gap-system.org/*, 2006.

[11] J. Gutierrez and T. Shaska, *Hyperelliptic curves with extra involutions*, LMS J. Comput. Math. **8** (2005), 102–115 (electronic). MR MR2135032 (2006b:14049)

[12] Jaime 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. MR MR2182037 (2006j:14038)

[13] E. Kani and M. Rosen, *Idempotent relations and factors of Jacobians*, Math. Ann. **284** (1989), no. 2, 307–327. MR MR1000113 (90h:14057)

[14] Ernst Kani and Michael Rosen, *Idempotent relations among arithmetic invariants attached to number fields and algebraic varieties*, J. Number Theory **46** (1994), no. 2, 230–254. MR MR1269254 (95c:11080)

[15] Robert M. Kuhn, *Curves of genus* 2 *with split Jacobian*, Trans. Amer. Math. Soc. **307** (1988), no. 1, 41–49. MR MR936803 (89f:14027)

[16] C. Maclachlan, *Abelian groups of automorphisms of compact Riemann surfaces*, Proc. London Math. Soc. (3) **15** (1965), 699–712. MR MR0179348 (31 #3596)

[17] ———, *A bound for the number of automorphisms of a compact Riemann surface.*, J. London Math. Soc. **44** (1969), 265–272. MR MR0236378 (38 #4674)

[18] K. Magaard, T. Shaska, S. Shpectorov, and H. Völklein, *The locus of curves with prescribed automorphism group*, Sūrikaisekikenkyūsho Kōkyūroku (2002), no. 1267, 112–141, Communications in arithmetic fundamental groups (Kyoto, 1999/2001). MR MR1954371

[19] K. Magaard, T. Shaska, and H. Völklein, *Genus two curves with degree 5 elliptic subcovers*, Forum Math.

[20] G. A. Miller, H. F. Blichfeldt, and L. E. Dickson, *Theory and applications of finite groups*, Dover Publications Inc., New York, 1961. MR MR0123600 (23 #A925)

[21] J. Paulhus, *Decomposing jacobians of hyperelliptic curves*, preprint.

[22] E. Previato, T. Shaska, and G. S. Wijesiri, *Thetanulls of curves of small genus with automorphisms*, Albanian J. Math. **1** (2007), 253–270.

[23] Sanjeewa R. and Shaska T., *Cyclic curves and their automorphisms*, work in progress.

[24] D. Sevilla and T. Shaska, *Hyperelliptic curves with reduced automorphism group* A_5, Appl. Algebra Engrg. Comm. Comput. **18** (2007), no. 1-2, 3–20. MR MR2280308

[25] T. Shaska, *Curves of genus 2 with* (N, N) *decomposable Jacobians*, J. Symbolic Comput. **31** (2001), no. 5, 603–617. MR MR1828706 (2002m:14023)

[26] ———, *Computational algebra and algebraic curves.*, SIGSAM Bull. **37** (2003), no. 4, 117–124.

[27] ———, *Computational aspects of hyperelliptic curves*, Computer mathematics, Lecture Notes Ser. Comput., vol. 10, World Sci. Publ., River Edge, NJ, 2003, pp. 248–257. MR MR2061839 (2005h:14073)

[28] ———, *Determining the automorphism group of a hyperelliptic curve*, Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation (New York), ACM, 2003, pp. 248–254 (electronic). MR MR2035219 (2005c:14037)

[29] ———, *Genus 2 fields with degree 3 elliptic subfields*, Forum Math. **16** (2004), no. 2, 263–280. MR MR2039100 (2004m:11097)

[30] ———, *Some special families of hyperelliptic curves*, J. Algebra Appl. **3** (2004), no. 1, 75–89. MR MR2047637 (2005i:14028)

[31] T. Shaska (ed.), *Computational aspects of algebraic curves*, Lecture Notes Series on Computing, vol. 13, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2005, Papers from the conference held at the University of Idaho, Moscow, ID, May 26–28, 2005. MR MR2182657 (2006e:14003)

[32] ———, *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. MR MR2182041 (2006g:14051)

[33] ———, *Subvarieties of the hyperelliptic moduli determined by group actions*, Serdica Math. J. **32** (2006), no. 4, 355–374. MR MR2287373 (2007k:14055)

[34] T. Shaska and H. Völklein, *Elliptic subfields and automorphisms of genus 2 function fields*, Algebra, arithmetic and geometry with applications (West Lafayette, IN, 2000), Springer, Berlin, 2004, pp. 703–723. MR MR2037120 (2004m:14047)

[35] Tetsuji Shioda, *On the graded ring of invariants of binary octavics*, Amer. J. Math. **89** (1967), 1022–1046. MR MR0220738 (36 #3790)

Department of Mathematics and Statistics,
Oakland University
Rochester, MI, 48386.
Email: shaska@oakland.edu