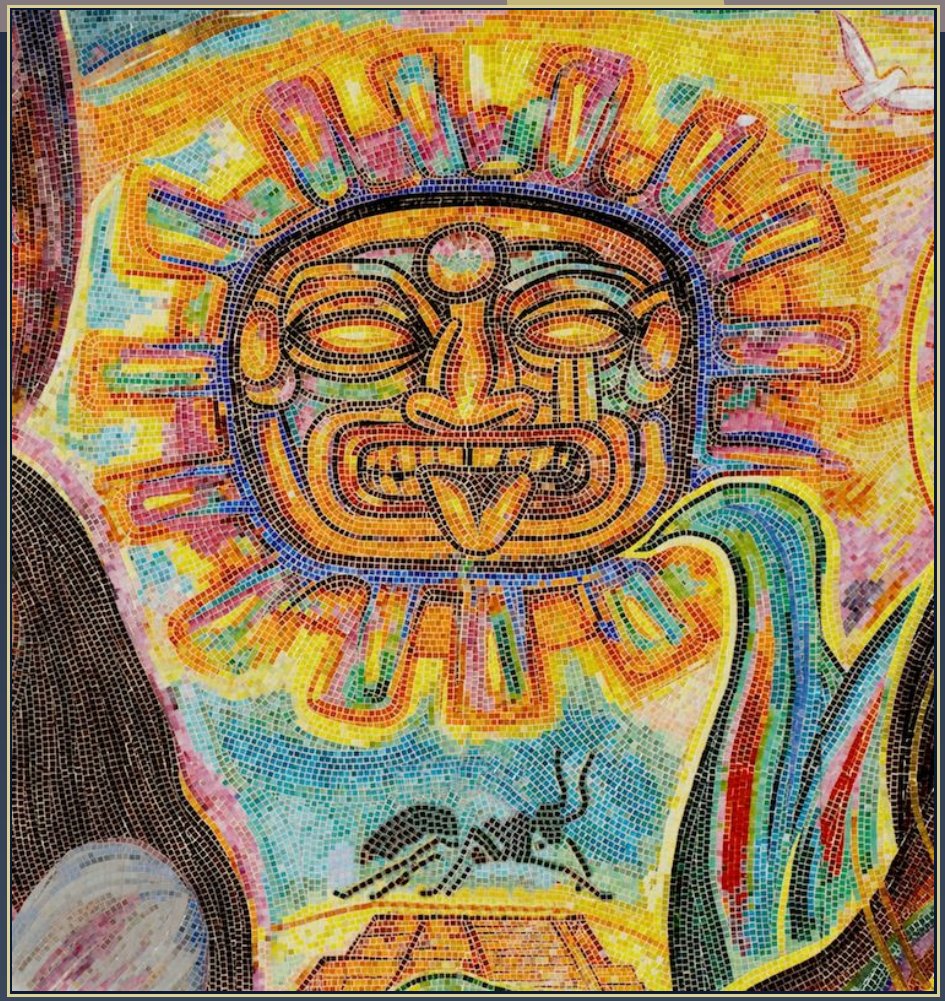
THE OPEN BOOK SERIES 1

ANTS X
Proceedings of the Tenth Algorithmic Number Theory Symposium

Elliptic factors in Jacobians of hyperelliptic curves with certain automorphism groups

Jennifer Paulhus



msp

THE OPEN BOOK SERIES **1** (2013)
Tenth Algorithmic Number Theory Symposium
dx.doi.org/10.2140/obs.2013.1.487

msp

Elliptic factors in Jacobians of hyperelliptic curves with certain automorphism groups

Jennifer Paulhus

We decompose the Jacobian varieties of hyperelliptic curves up to genus 20, defined over an algebraically closed field of characteristic zero, with reduced automorphism group A_4, S_4, or A_5. Among these curves is a genus-4 curve with Jacobian variety isogenous to $E_1^2 \times E_2^2$ and a genus-5 curve with Jacobian variety isogenous to E^5, for E and E_i elliptic curves. These types of results have some interesting consequences for questions of ranks of elliptic curves and ranks of their twists.

1. Introduction

Curves with Jacobian varieties that have many elliptic curve factors in their decompositions up to isogeny have been studied in many different contexts. Ekedahl and Serre found examples of curves whose Jacobians split completely into elliptic curves (not necessarily isogenous to one another) [13] (see also [27], [14, §5]). In genus 2, Cardona showed connections between curves whose Jacobians have two isogenous elliptic curve factors and $\mathbb{Q}$-curves of degree 2 and 3 [5]. There are applications of such curves to ranks of twists of elliptic curves [24], results on torsion [19], and cryptography [12].

Let J_X denote the Jacobian variety of a curve X and let $\sim$ represent an isogeny between abelian varieties. Consider the following question.

Question 1. For a fixed genus g, what is the largest positive integer t such that $J_X \sim E^t \times A$ for some genus-g curve X over the algebraic closure of $\mathbb{Q}$, where E is an elliptic curve and A an abelian variety?

MSC2010: primary 14H40; secondary 11G30, 14H37.
Keywords: Jacobian varieties, hyperelliptic curves, automorphism groups of Riemann surfaces.

In [22] the author developed a method for decomposing the Jacobian variety of a curve X with automorphism group G, based on idempotent relations in the group ring $\mathbb{Q}[G]$. This technique yielded thitherto unknown examples of curves of genus 4 through 6 where t is as large as is possible — that is, t is equal to the genus g. For genus 7 through 10, examples of curves whose Jacobians have many isogenous elliptic curves in their decompositions were also found. All these examples are nonhyperelliptic curves.

In this paper we apply the methods of [22] to hyperelliptic curves with certain automorphism groups. Let X be a hyperelliptic curve defined over a field of characteristic 0, with hyperelliptic involution ω. The automorphism group of the curve X modulo the subgroup $\langle\omega\rangle$ is called the *reduced automorphism group* and must be one of the groups C_n, D_n, A_4, S_4, or A_5; here C_n represents the cyclic group of order n and D_n is the dihedral group of order $2n$. This follows from a result of Dickson on transformations of binary forms [7].

We study hyperelliptic curves with reduced automorphism group one of A_4, S_4, or A_5. These reduced automorphism groups were chosen for two reasons. First, results from genus 2 and 3 suggest that these families may yield curves with many isogenous elliptic curve factors in higher genus. Second, for any genus, the list of full automorphism groups with reduced automorphism group one of A_4, S_4, or A_5 is manageable.

Section 3 reviews the method from [22], and Section 4 gives proofs of results for genus up to 20. This bound of genus 20 is somewhat arbitrary. The technique will work for any genus, but the computations become more complicated as the genus increases. Section 5 discusses some computational obstructions to producing results in higher genus. In that section we also work with families of curves with three particular automorphism groups. These groups have special properties that allow us to prove results about the decomposition of the curves' Jacobians for arbitrary genus.

A brief word on fields of definition: Unless specifically stated otherwise, curves in this paper are defined over an algebraically closed field of characteristic zero. The method of decomposition works generally for curves over any field; however, a particular field must be specified in order to determine the automorphism group of the curve. In each individual case, the decomposition results will hold for the Jacobian of the curve defined over any field over which every geometric automorphism of the curve is defined. Partial answers to Question 1 are known for curves over fields of characteristic p; see, for example, [28; 17; 9].

2. Overview of results

The decompositions of Jacobian varieties of hyperelliptic curves with reduced automorphism group A_4, S_4, or A_5 up to genus 20 are summarized in Theorem 5.

Jacobian varieties with several isogenous elliptic curve factors are also found, and many are improvements on the best known results for t [22]. Two results of particular interest are:

Theorem 1. *The hyperelliptic curve of genus* 4 *with affine model*

$$X: \quad y^2 = x(x^4 - 1)(x^4 + 2\sqrt{-3}\,x^2 + 1)$$

has a Jacobian variety that decomposes as $E_1^2 \times E_2^2$ *for two elliptic curves* E_i.

Theorem 2. *The genus-*5 *hyperelliptic curve with affine model*

$$X: \quad y^2 = x(x^{10} + 11x^5 - 1)$$

has $J_X \sim E^5$ *for the elliptic curve* E *with equation* $y^2 = x(x^2 + 11x - 1)$.

The first theorem is an improvement from best decompositions of genus-4 hyperelliptic curves from [23]. The second theorem is, to the author's knowledge, the first example in the literature of a hyperelliptic curve with a Jacobian variety that decomposes into five isogenous elliptic curves over a number field. Proofs of these results may be found in Section 4.

3. Review of technique

Fix an algebraically closed field k of characteristic 0. Throughout the paper the word *curve* will mean a smooth projective variety of dimension 1. For simplicity, models are affine, when given. Any parameters in the affine model (labeled as "a_i") are elements of k. Also, ζ_n will denote a primitive n-th root of unity.

Given a curve X of genus g over k, the *automorphism group* of X is the automorphism group of the field extension $k(X)$ over k, where $k(X)$ is the function field of X. This group will always be finite for $g \geq 2$. Throughout, G will denote the automorphism group of a curve X. In the case of hyperelliptic curves over algebraically closed fields of characteristic zero, all possible automorphism groups are known for a given genus [2; 4; 25].

Kani and Rosen [20] proved a result connecting certain idempotent relations in the endomorphism algebra $\mathrm{End}^0 J_X = (\mathrm{End}\, J_X) \otimes_{\mathbb{Z}} \mathbb{Q}$ to isogenies among images of J_X under endomorphisms. If α_1 and α_2 are elements of $\mathrm{End}^0 J_X$, we write $\alpha_1 \sim \alpha_2$ if $\chi(\alpha_1) = \chi(\alpha_2)$ for all $\mathbb{Q}$-characters χ of $\mathrm{End}^0 J_X$.

Theorem 3 [20, Theorem A]. *Let* $\varepsilon_1, \ldots, \varepsilon_n, \varepsilon'_1, \ldots, \varepsilon'_m \in \mathrm{End}^0 J_X$ *be idempotents. Then the idempotent relation*

$$\varepsilon_1 + \cdots + \varepsilon_n \sim \varepsilon'_1 + \cdots + \varepsilon'_m$$

holds in $\mathrm{End}^0 J_X$ *if and only if there is the isogeny relation*

$$\varepsilon_1(J_X) \times \cdots \times \varepsilon_n(J_X) \sim \varepsilon'_1(J_X) \times \cdots \times \varepsilon'_m(J_X).$$

There is a natural $\mathbb{Q}$-algebra homomorphism from $\mathbb{Q}[G]$ to $\mathrm{End}^0 J_X$, which we will denote by e. It is a well-known result of Wedderburn [11, §18.2] that any group ring of the form $\mathbb{Q}[G]$ has a decomposition into a direct sum of matrix rings over division rings Δ_i:

$$\mathbb{Q}[G] \cong \bigoplus_i M_{n_i}(\Delta_i). \tag{1}$$

Define $\pi_{i,j}$ to be the idempotent in $\mathbb{Q}[G]$ which is the zero matrix for all components except the i-th component where it is the matrix with a 1 in the (j, j) position and zeros elsewhere. The following equation is an idempotent relation in $\mathbb{Q}[G]$:

$$1_{\mathbb{Q}[G]} = \sum_{i,j} \pi_{i,j}.$$

Applying the map e to this relation and using Theorem 3, we find

$$J_X \sim \bigoplus_{i,j} e(\pi_{i,j}) J_X. \tag{2}$$

Recall that our primary goal is to study isogenous elliptic curves that appear in the decomposition above. In order to identify which summands in (2) have dimension 1, we use results from [15, §5.2] to compute the dimensions of these factors. This requires a certain representation of G.

Definition. The *Hurwitz representation* V of a group G is defined by the action of G on $H_1(X, \mathbb{Z}) \otimes \mathbb{Q}$.

The character of this representation is computed as follows. Let $\rho: X \to Y = X/G$ be the natural map from X to its quotient by G. Suppose ρ is branched at s points, with monodromy $g_1, \ldots, g_s \in G$ (unique up to conjugation). Let χ_{triv} be the trivial character of G, and for each i let $\chi_{\langle g_i \rangle}$ denote the character of G induced from the trivial character of the subgroup $\langle g_i \rangle$ of G; observe that $\chi_{\langle 1_G \rangle}$ is the character of the regular representation. If we let g_Y denote the genus of Y, then the character of the Hurwitz representation V is defined as

$$\chi_V = 2\chi_{\mathrm{triv}} + 2(g_Y - 1)\chi_{\langle 1_G \rangle} + \sum_i \big(\chi_{\langle 1_G \rangle} - \chi_{\langle g_i \rangle}\big). \tag{3}$$

Note that for a hyperelliptic curve X, we have $X/G \cong \mathbb{P}^1$ (since G contains the hyperelliptic involution) and so $g_Y = 0$. Also, $\chi_{\langle g_i \rangle} = \chi_{\langle g_j \rangle}$ if $\langle g_i \rangle$ and $\langle g_j \rangle$ are conjugate subgroups.

Via the regular representation, each element g_i can be written as an element of the symmetric group S_n, where $n = \#G$. The monodromy type of a cover will be written as an ordered tuple $(t_1^{(a_1)}, \ldots, t_s^{(a_s)})$ where $t_i^{(a_i)}$ corresponds to g_i and denotes a permutation consisting of a_i t_i-tuples. If χ_i is the irreducible $\mathbb{Q}$-character

associated to the i-th component from (1), then the dimensions of the summands in (2) are

$$\dim e(\pi_{i,j})J_X = \tfrac{1}{2}\dim_{\mathbb{Q}} \pi_{i,j}V = \tfrac{1}{2}\langle \chi_i, \chi_V \rangle. \tag{4}$$

See [15, §5.2] for more information on the dimension computations.

Hence, given the automorphism group G of a curve X and monodromy for the cover X over Y, to compute these dimensions we first determine the degrees of the irreducible $\mathbb{Q}$-characters of G, which will be the n_i values in (1). Next we identify elements of the automorphism group that satisfy the monodromy conditions. We compute the Hurwitz character for this group and covering using (3), and finally compute the inner product of the irreducible $\mathbb{Q}$-characters with the Hurwitz character.

Again, our particular interest is in factors that are *isogenous* to one another. The following proposition gives a condition for the factors to be isogenous.

Proposition 4 [23]. *With notation as above*, $e(\pi_{i,j_1})J_X \sim e(\pi_{i,j_2})J_X$.

Suppose a curve of genus g has automorphism group with group ring decomposition as in (1) with at least one matrix ring of degree close to g; that is, one n_i value close to g — call it n_j. If the computations of dimensions of abelian variety factors outlined above lead to a dimension-1 variety in the place corresponding to that matrix ring (the j-th place), Proposition 4 implies that the Jacobian variety decomposition consists of n_j isogenous elliptic curves. Our goal then is to apply the steps above to hyperelliptic curves of genus up to 20 and with reduced automorphism group isomorphic to A_4, S_4, or A_5.

4. Results

For hyperelliptic curves over an algebraically closed field of characteristic zero, the existence of curves of a fixed genus with reduced automorphism group isomorphic to one of A_4, S_4, or A_5 is completely determined by whether the genus is in certain residue classes modulo 6, 12, and 30, respectively [25].

For each reduced automorphism group there are several possible full automorphism groups. Table 1 lists all groups and the modular conditions for their existence in a certain genus, as well as monodromy type, listed using the notation described in the previous section. The data from this table is taken from [25, Table 1, p. 250]. Explanations of how this data was produced may be found in [25], along with affine models for all of the corresponding families. The groups

$$W_2 = \langle u, v \mid u^4, v^3, vu^2v^{-1}u^2, (uv)^4 \rangle,$$
$$W_3 = \langle u, v \mid u^4, v^3, u^2(uv)^4, (uv)^8 \rangle$$

mentioned in the table are both of order 48.

Automorphism group			
Reduced	Full	Genus restrictions	Monodromy
A_4	$A_4 \times C_2$	$5 \bmod 6$	$(3^{(8)}, 3^{(8)}, 2^{(12)}, \ldots, 2^{(12)})$
	$A_4 \times C_2$	$1 \bmod 6$	$(3^{(8)}, 6^{(4)}, 2^{(12)}, \ldots, 2^{(12)})$
	$A_4 \times C_2$	$3 \bmod 6$, $g > 3$	$(6^{(4)}, 6^{(4)}, 2^{(12)}, \ldots, 2^{(12)})$
	$\mathrm{SL}_2(3)$	$2 \bmod 6$, $g > 2$	$(4^{(6)}, 3^{(8)}, 3^{(8)}, 2^{(12)}, \ldots, 2^{(12)})$
	$\mathrm{SL}_2(3)$	$4 \bmod 6$	$(4^{(6)}, 3^{(8)}, 6^{(4)}, 2^{(12)}, \ldots, 2^{(12)})$
	$\mathrm{SL}_2(3)$	$0 \bmod 6$, $g > 6$	$(4^{(6)}, 6^{(4)}, 6^{(4)}, 2^{(12)}, \ldots, 2^{(12)})$
S_4	$S_4 \times C_2$	$11 \bmod 12$	$(3^{(16)}, 4^{(12)}, 2^{(24)}, \ldots, 2^{(24)})$
	$S_4 \times C_2$	$3 \bmod 12$	$(6^{(8)}, 4^{(12)}, 2^{(24)}, \ldots, 2^{(24)})$
	$\mathrm{GL}_2(3)$	$2 \bmod 12$	$(3^{(16)}, 8^{(6)}, 2^{(24)}, \ldots, 2^{(24)})$
	$\mathrm{GL}_2(3)$	$6 \bmod 12$	$(6^{(8)}, 8^{(6)}, 2^{(24)}, \ldots, 2^{(24)})$
	W_2	$5 \bmod 12$	$(4^{(12)}, 4^{(12)}, 3^{(16)}, 2^{(24)}, \ldots, 2^{(24)})$
	W_2	$9 \bmod 12$	$(4^{(12)}, 4^{(12)}, 6^{(8)}, 2^{(24)}, \ldots, 2^{(24)})$
	W_3	$8 \bmod 12$	$(4^{(12)}, 3^{(16)}, 8^{(6)}, 2^{(24)}, \ldots, 2^{(24)})$
	W_3	$0 \bmod 12$	$(4^{(12)}, 6^{(8)}, 8^{(6)}, 2^{(24)}, \ldots, 2^{(24)})$
A_5	$A_5 \times C_2$	$29 \bmod 30$	$(3^{(40)}, 5^{(24)}, 2^{(60)}, \ldots, 2^{(60)})$
	$A_5 \times C_2$	$5 \bmod 30$	$(3^{(40)}, 10^{(12)}, 2^{(60)}, \ldots, 2^{(60)})$
	$A_5 \times C_2$	$15 \bmod 30$	$(6^{(20)}, 10^{(12)}, 2^{(60)}, \ldots, 2^{(60)})$
	$A_5 \times C_2$	$9 \bmod 30$	$(6^{(20)}, 5^{(24)}, 2^{(60)}, \ldots, 2^{(60)})$
	$\mathrm{SL}_2(5)$	$14 \bmod 30$	$(4^{(30)}, 3^{(40)}, 5^{(24)}, 2^{(60)}, \ldots, 2^{(60)})$
	$\mathrm{SL}_2(5)$	$20 \bmod 30$	$(4^{(30)}, 3^{(40)}, 10^{(12)}, 2^{(60)}, \ldots, 2^{(60)})$
	$\mathrm{SL}_2(5)$	$24 \bmod 30$	$(4^{(30)}, 6^{(20)}, 5^{(24)}, 2^{(60)}, \ldots, 2^{(60)})$
	$\mathrm{SL}_2(5)$	$0 \bmod 30$	$(4^{(30)}, 6^{(20)}, 10^{(12)}, 2^{(60)}, \ldots, 2^{(60)})$

Table 1. Full automorphism groups of hyperelliptic curves with certain reduced automorphism groups. For each group $\tilde{G}$ in the first column, we list the possible automorphism groups G occurring for hyperelliptic curves with reduced automorphism group $\tilde{G}$. The third column lists restrictions on the genus g of hyperelliptic curves with the given automorphism group, and the fourth column lists the monodromy of such curves.

Applying the technique in Section 3 to hyperelliptic curves of genus 3 through 20 produces results that are summarized in the following theorem.

Theorem 5. *For hyperelliptic curves up to genus* 20 *defined over an algebraically closed field of characteristic zero with reduced automorphism group A_4, S_4, or A_5, Table 2 gives a decomposition of the Jacobian of these curves up to isogeny. In the table E_i represents an elliptic curve and $A_{i,j}$ is an abelian variety of dimension $i > 1$, indexed if necessary by j. The dimension of the family with each automorphism group in the moduli space is also included.*

Genus	Automorphism Group	Dimension	Jacobian decomposition
3	$S_4 \times C_2$	0	E^3
4	$\mathrm{SL}_2(3)$	0	$E_1^2 \times E_2^2$
5	$A_4 \times C_2$	1	$E^3 \times A_2$
	W_2	0	$E_1^2 \times E_2^3$
	$A_5 \times C_2$	0	E^5
6	$\mathrm{GL}_2(3)$	0	$E_1^2 \times E_2^4$
7	$A_4 \times C_2$	1	$E_1 \times E_2^3 \times E_3^3$
8	$\mathrm{SL}_2(3)$	1	$A_{2,1}^2 \times A_{2,2}^2$
	W_3	0	$E^4 \times A_2^2$
9	$A_4 \times C_2$	1	$E^3 \times A_2^3$
	W_2	0	$E_1 \times E_2^2 \times A_2^3$
	$A_5 \times C_2$	0	$E_1^4 \times E_2^5$
10	$\mathrm{SL}_2(3)$	1	$A_2^2 \times A_3^2$
11	$A_4 \times C_2$	2	$A_2 \times A_3^3$
	$S_4 \times C_2$	1	$E^3 \times A_{2,1} \times A_{2,2}^3$
12	$\mathrm{SL}_2(3)$	1	$A_2^2 \times A_4^2$
	W_3	0	$A_{2,1}^2 \times A_{2,2}^4$
13	$A_4 \times C_2$	2	$E \times A_{3,1} \times A_{3,2}^3$
14	$\mathrm{SL}_2(3)$	2	$A_3^2 \times A_4^2$
	$\mathrm{GL}_2(3)$	1	$A_2^4 \times A_3^2$
	$\mathrm{SL}_2(5)$	0	$E_1^4 \times E_2^6 \times A_2^2$
15	$A_4 \times C_2$	2	$A_2^3 \times A_3^3$
	$S_4 \times C_2$	1	$E_1 \times E_2^2 \times A_{2,1}^3 \times A_{2,2}^3$
	$A_5 \times C_2$	0	$E_1^4 \times E_2^5 \times A_2^3$
16	$\mathrm{SL}_2(3)$	2	$A_3^2 \times A_5^2$
17	$A_4 \times C_2$	3	$E \times A_{4,1} \times A_{4,2}^3$
	W_2	1	$E \times A_2^2 \times A_4^3$
18	$\mathrm{SL}_2(3)$	2	$A_3^2 \times A_6^2$
	$\mathrm{GL}_2(3)$	1	$A_{3,1}^2 \times A_{3,2}^4$
19	$A_4 \times C_2$	3	$E \times A_2^3 \times A_4^3$
20	$\mathrm{SL}_2(3)$	3	$A_4^2 \times A_6^2$
	W_3	1	$A_3^4 \times A_4^2$
	$\mathrm{SL}_2(5)$	0	$E^4 \times A_{2,1}^2 \times A_{2,2}^6$

Table 2. Jacobian variety decompositions. For each genus g and automorphism group G, we list the dimension of the moduli space of genus-g hyperelliptic curves with automorphism group G, along with a decomposition of the Jacobian of these curves. The notation is explained in Theorem 5.

The technique described in the previous section does not necessarily guarantee the finest decomposition of the Jacobian varieties. We have not ruled out the pos-

sibility that some of the abelian varieties $e(\pi_{i,j})J_X$ from (2) decompose further. In fact, in many cases there will be subfamilies where the decomposition is finer. However, for those curves in Table 2 which have affine models defined over $\mathbb{Q}$, we found a finite field where the factorization of the zeta function of that curve is no better than what our Jacobian decompositions predict. Hence, in those cases, the decomposition cannot be any finer, at least over $\mathbb{Q}$. Using ideas similar to those employed by Stoll [26, §2] one could show that, in fact, many of these decompositions cannot be refined even over the algebraic closure of $\mathbb{Q}$.

4.1. ***Finding monodromy and $\mathbb{Q}$-characters.*** The list of possible automorphism groups for hyperelliptic curves is well known, and most of these groups have easily identifiable character tables; thus, for hyperelliptic curves the most computationally difficult part of the technique summarized in Section 3 is finding the branching data. Breuer [3] developed an algorithm to generate a database of automorphism groups of Riemann surfaces, and he implemented this algorithm, up to genus 48, in the computer algebra package GAP [16]. Breuer's algorithm relies on the classifications of small groups in GAP. While the algorithm itself computes branching data, specific information about the monodromy was not recorded when Breuer originally ran the program.

We have now implemented in Magma [1] a version of Breuer's algorithm which *does* output the monodromy data. In cases below where the monodromy may not be obvious (for instance, if there is more than one conjugacy class of elements of a certain order for a particular automorphism group), our program provides the monodromy data.

We use Magma to compute the Hurwitz character χ_V and the inner product of χ_V with the irreducible $\mathbb{Q}$-characters. The $\mathbb{Q}$-character tables for the groups considered in this paper are well known in the literature so, alternatively, the computations could be done by hand.

4.2. ***Reduced automorphism group A_4.*** If a hyperelliptic curve has reduced automorphism group isomorphic to A_4, its full automorphism group is isomorphic to $\mathrm{SL}_2(3)$ or $A_4 \times C_2$. For $3 \leq g \leq 20$ the former group occurs in genus 4 and in all even genera greater than or equal to 8, while the latter group occurs in odd genera at least 5.

The group $\mathrm{SL}_2(3)$ has seven conjugacy classes. The identity, the unique element of order 2, and all the order-4 elements form three distinct conjugacy classes. The order-3 and order-6 elements each split into two conjugacy classes. The group ring $\mathbb{Q}[G]$ has Wedderburn decomposition

$$\mathbb{Q}[\mathrm{SL}_2(3)] \cong \mathbb{Q} \oplus \mathbb{Q}(\zeta_3) \oplus M_2(\mathbb{Q}) \oplus M_2(\mathbb{Q}(\zeta_3)) \oplus M_3(\mathbb{Q}).$$

	Conjugacy class order						
Character	1	2	3	3	4	6	6
χ_1	1	1	1	1	1	1	1
χ_2	2	2	−1	−1	2	−1	−1
χ_3	2	−2	−1	−1	0	1	1
χ_4	4	−4	1	1	0	−1	−1
χ_5	3	3	0	0	−1	0	0

Table 3. $\mathbb{Q}$-character table for $\mathrm{SL}_2(3)$.

So $\mathrm{SL}_2(3)$ has two $\mathbb{Q}$-characters of degree 1 (which we denote by χ_1 and χ_2), two of degree 2 (which we denote by χ_3 and χ_4), and one of degree 3 (which we denote by χ_5). The values of these characters on the conjugacy classes of $\mathrm{SL}_2(3)$ are well known [10, §38] and given in Table 3.

Recall from Section 2:

Theorem 1. *The hyperelliptic curve of genus* 4 *with affine model*

$$X: \quad y^2 = x(x^4-1)(x^4+2\sqrt{-3}\,x^2+1)$$

has a Jacobian variety that decomposes as $E_1^2 \times E_2^2$ *for two elliptic curves* E_i.

Everett Howe used an order-3 automorphism of X to compute that one of the factors of J_X (up to isogeny), say E_1, is given by E_1 with equation $y^2 = x^3 - 21x^2 + 12x + 8$.

Proof. Shaska [25, Tables 1 and 2, pp. 250, 252] shows that the curve X has automorphism group $\mathrm{SL}_2(3)$ and monodromy type $(4^{(6)}, 3^{(8)}, 6^{(4)})$. Thus the monodromy consists of elements g_1, g_2, and $g_3 \in \mathrm{SL}_2(3)$ of order 4, 3, and 6, respectively. As noted above, the six elements of order 4 are all in the same conjugacy class. Thus $\chi_{\langle g\rangle}$ (the induced character of the trivial character of the subgroup generated by $g \in G$) will be the same for all g of order 4, and likewise for the elements of order 3 and the elements of order 6, since all order-3 elements generate conjugate subgroups, as do the order-6 elements. Computing the Hurwitz character yields

$$\begin{aligned}\chi_V &= 2\chi_{\mathrm{triv}} - 2\chi_{\langle 1_G\rangle} + (\chi_{\langle 1_G\rangle} - \chi_{\langle g_1\rangle}) + (\chi_{\langle 1_G\rangle} - \chi_{\langle g_2\rangle}) + (\chi_{\langle 1_G\rangle} - \chi_{\langle g_3\rangle}) \\ &= 2\chi_{\mathrm{triv}} + \chi_{\langle 1_G\rangle} - \chi_{\langle g_1\rangle} - \chi_{\langle g_2\rangle} - \chi_{\langle g_3\rangle}.\end{aligned}$$

The value of χ_V on conjugacy classes (listed in the same order as in Table 3) is the 7-tuple $(8, -8, -1, -1, 0, 1, 1)$. Computing the inner product of the irreducible $\mathbb{Q}$-characters with χ_V yields a value of 2 for each of the degree-2 characters and 0 for all the other characters. Applying (4) and Proposition 4 gives $J_X \sim E_1^2 \times E_2^2$. □

Similar results may be found for $g \geq 8$. See Section 5 for the generalization to arbitrary even genus.

The group $A_4 \times C_2$ has four irreducible $\mathbb{Q}$-characters of degree 1 and two of degree 3. For genus 5, the family of curves with affine model

$$X: \ y^2 = x^{12} - ax^{10} - 33x^8 + 2ax^6 - 33x^4 - ax^2 + 1$$

has automorphism group $A_4 \times C_2$ and monodromy type $(3^{(8)}, 3^{(8)}, 2^{(12)}, 2^{(12)})$; see Shaska [25, Tables 1 and 2, pp. 250, 252]. We compute the Hurwitz character using the monodromy found through Breuer's algorithm, and then compute the inner products of the irreducible $\mathbb{Q}$-characters and the Hurwitz character. The inner product is 4 for one of the degree-1 characters and 2 for one of the degree-3 characters. By (4), the Jacobian variety of X decomposes into a 2-dimensional variety and three 1-dimensional varieties. Proposition 4 asserts that the three elliptic curves in this decomposition are isogenous to one another, so $J_X \sim A_2 \times E^3$ for some abelian surface A_2 and elliptic curve E.

Computations similar to those in the genus-5 case give the decompositions for higher odd genus described in Table 2.

4.3. ***Reduced automorphism group S_4.*** When a hyperelliptic curve has reduced automorphism group S_4, there are four options for its full automorphism group: $S_4 \times C_2$, $\mathrm{GL}_2(3)$, and the groups W_2 and W_3 defined at the beginning of this section. (The notation for the latter two groups of order 48 is as in [25].)

In genus 3, 11, and 15 there are curves with full automorphism group $S_4 \times C_2$. In [23], the Jacobian variety of the genus-3 curve was decomposed into the product of three isogenous elliptic curves. This result also appears in the literature using other techniques [21].

The decompositions of the families of genus-11 and genus-15 curves may be found using monodromy computed with Breuer's algorithm. The group $S_4 \times C_2$ has three irreducible $\mathbb{Q}$-characters of degree 1, two of degree 2, and three of degree 3. Combining this information with the technique in Section 3 yields the decompositions listed in Table 2.

As determined in [25], there is one genus-6 curve, up to isomorphism, with automorphism group $\mathrm{GL}_2(3)$:

$$X: \ y^2 = x(x^4 - 1)(x^8 + 14x^4 + 1).$$

Additionally, there are 1-dimensional families of curves of genus 14 and 18 with this automorphism group.

The group $\mathrm{GL}_2(3)$ has two irreducible $\mathbb{Q}$-characters each of degrees 1, 2, and 3, as well as one of degree 4. In genus 6, the inner products of the irreducible $\mathbb{Q}$-characters with the Hurwitz character give values of 2 for one of the degree-2

characters and for the degree-4 character; from this we may conclude that $J_X \sim E_1^2 \times E_2^4$. Similar computations yield $J_X \sim A_3^2 \times A_4^2$ for the genus-14 curves and $J_X \sim A_{3,1}^2 \times A_{3,2}^4$ for the genus-18 curves.

For genus 5 and 9 there is one curve with automorphism group W_2, and in genus 17 there is a 1-dimensional family of curves with this automorphism group. In genus 5 the curve has an affine model

$$X: \quad y^2 = x^{12} - 33x^8 - 33x^4 + 1,$$

in genus 9 a model is

$$X: \quad y^2 = (x^8 + 14x^4 + 1)(x^{12} - 33x^8 - 33x^4 + 1),$$

and in genus 17 a model is

$$X: \quad y^2 = (x^{12} - 33x^8 - 33x^4 + 1)\big(x^{24} + ax^{20} + (759 - 4a)x^{16} + 2(3a + 1288)x^{12} + (759 - 4a)x^8 + ax^4 + 1\big).$$

This group has eight irreducible $\mathbb{Q}$-characters: three of degree 1, two of degree 2, and three of degree 3. Computations with the genus-5 curve yield $J_X \sim E_1^2 \times E_2^3$, while for genus 9 we have $J_X \sim E_1 \times E_2^2 \times A_2^3$ and for genus 17, $J_X \sim E \times A_2^2 \times A_4^3$.

In genus 8 the curve with model

$$X: \quad y^2 = x(x^4 - 1)(x^{12} - 33x^8 - 33x^4 + 1)$$

has automorphism group W_3 and monodromy type $(4^{(12)}, 3^{(16)}, 8^{(6)})$. The irreducible $\mathbb{Q}$-characters consist of two each of degrees 1, 2, and 3, as well as one of degree 4. Computations show the Jacobian of this curve decomposes as $A_2^2 \times E^4$. For higher-genus curves with this automorphism group, see the general results in Section 5.3.

In [22], in the course of considering different families of curves up to genus 10 we found a genus-8 curve with Jacobian decomposition $A_4 \times E_1^2 \times E_2^2$, so the result above is an improvement on our previous results on the bound on t from Question 1 in the introduction.

4.4. ***Reduced automorphism group A_5.*** As we see from Table 1, if a hyperelliptic curve has reduced automorphism group isomorphic to A_5, its full automorphism group is isomorphic to $A_5 \times C_2$ or $\mathrm{SL}_2(5)$. In genus 14 and 20 there is a hyperelliptic curve with automorphism group isomorphic to $\mathrm{SL}_2(5)$. This group has special properties that allow us to prove results about the decomposition of Jacobians generally for any genus. In Section 5.2 we discuss the general results.

Up to isomorphism, there is one curve of genus 5 with automorphism group $A_5 \times C_2$, one of genus 9, and one of genus 15. Here we prove the following result, which was mentioned in Section 2.

	Conjugacy class order									
Character	1	2	2	2	3	5	5	6	10	10
χ_1	1	1	1	1	1	1	1	1	1	1
χ_2	1	−1	1	−1	1	1	1	−1	−1	−1
χ_3	6	−6	−2	2	0	1	1	0	−1	−1
χ_4	6	6	−2	−2	0	1	1	0	1	1
χ_5	4	4	0	0	1	−1	−1	1	−1	1
χ_6	4	−4	0	0	1	−1	−1	−1	1	1
χ_7	5	5	1	1	−1	0	0	−1	0	0
χ_8	5	−5	1	−1	−1	0	0	1	0	0

Table 4. $\mathbb{Q}$-character table for $A_5 \times C_2$.

Theorem 2. *The genus-5 hyperelliptic curve with affine model*

$$X: \ y^2 = x(x^{10} + 11x^5 - 1)$$

has $J_X \sim E^5$ for the elliptic curve E with equation $y^2 = x(x^2 + 11x - 1)$.

Proof. We see from [25, §4.5] that the curve X has automorphism group $A_5 \times C_2$ and monodromy type $(3^{(40)}, 10^{(12)}, 2^{(60)})$ — although note that the coefficient 11 in the model given for X was misprinted in [25]. The irreducible $\mathbb{Q}$-characters of this group consist of two characters each of degrees 1, 3, 4, and 5. The monodromy consists of elements g_1, g_2, and $g_3 \in G$ of order 3, 10, and 2 respectively; this may be computed using Breuer's algorithm [3]. Table 4 gives the values of the irreducible $\mathbb{Q}$-characters on the conjugacy classes of $A_5 \times C_2$.

The Hurwitz character is

$$\begin{aligned}\chi_V &= 2\chi_{\text{triv}} - 2\chi_{\langle 1_G\rangle} + (\chi_{\langle 1_G\rangle} - \chi_{\langle g_1\rangle}) + (\chi_{\langle 1_G\rangle} - \chi_{\langle g_2\rangle}) + (\chi_{\langle 1_G\rangle} - \chi_{\langle g_3\rangle}) \\ &= 2\chi_{\text{triv}} + \chi_{\langle 1_G\rangle} - \chi_{\langle g_1\rangle} - \chi_{\langle g_2\rangle} - \chi_{\langle g_3\rangle}\end{aligned}$$

and its value on conjugacy classes (in the same order as Table 4) is given by the 10-tuple $(10, -10, 2, -2, -2, 0, 0, 2, 0, 0)$. The inner product of each of the irreducible $\mathbb{Q}$-characters with χ_V results in a value of 0 for all except one of the degree-5 characters, where the inner product is 2. By (4) and Proposition 4 this gives the desired decomposition. □

Applying this same idea to the genus-9 curve with affine model

$$X: \ y^2 = x^{20} - 228x^{15} + 494x^{10} - 228x^5 + 1$$

yields inner products with a value of 0 for all irreducible $\mathbb{Q}$-characters except for one degree-4 and one degree-5 character, where the inner product is 2. Again,

by (4) and Proposition 4, we find that J_X is isogenous to $E_1^4 \times E_2^5$, for elliptic curves E_i.

Similar computations in genus 15 for a curve with model

$$X: \quad y^2 = x(x^{10} + 11x - 1)(x^{20} - 228x^{15} + 494x^{10} - 228x^5 + 1)$$

yield the decomposition $J_X \sim E_1^4 \times E_2^5 \times A_2^3$.

5. General results

One obstacle to extending these results to higher genus is the computation of the monodromy for the cover $X \to X/G$. Beyond genus 48, Breuer's algorithm cannot currently compute the monodromy in many cases.

The groups $\mathrm{SL}_2(3)$, $\mathrm{SL}_2(5)$, and W_3 all share the following property: If X is a curve with automorphism group isomorphic to one of these groups, and if m is the order of any element of the monodromy of the cover X over X/G, then $\chi_{\langle g_i \rangle} = \chi_{\langle g_j \rangle}$ whenever $|g_i| = |g_j| = m$. We will denote this common character by $\chi_{(m)}$. Note that this property allows us to compute the Hurwitz character for X just by knowing the monodromy type. We then apply the technique from Section 3 to produce general decompositions for arbitrary genus.

Keep in mind that our technique does not necessarily guarantee the finest decomposition of the Jacobian variety. It is possible that for specific genera below the Jacobian decomposes further.

5.1. ***The group*** $\mathbf{SL_2(3)}$**.** Every even genus $g > 2$, except genus 6, has a hyperelliptic curve over k with automorphism group $\mathrm{SL}_2(3)$. For a given g, let $d = \lfloor (g-1)/6 \rfloor$, and let

$$G(x) = \prod_{i=1}^{d} (x^{12} - a_i x^{10} - 33x^8 + 2a_i x^6 - 33x^4 - a_i x^2 + 1),$$

where the a_i are distinct elements of k. Table 5 gives affine models and monodromy for curves of each even genus. These results may be found in [25]. Also recall the Wedderburn decomposition of $\mathbb{Q}[\mathrm{SL}_2(3)]$ and the irreducible characters of $\mathrm{SL}_2(3)$ from Section 4.2.

Computing the Hurwitz character given by (3) requires computing $\chi_{\langle g_i \rangle}$, the trivial character of $\langle g_i \rangle$ induced to $\mathrm{SL}_2(3)$, for each branched point g_i. The monodromy types listed in Table 5 give us the order of each branch point. As mentioned above, for this particular group, the order of the element is sufficient to compute the induced character. Table 6 lists the values of these induced characters on each conjugacy class.

Suppose X is a curve of genus g with automorphism group $\mathrm{SL}_2(3)$. Let $d = \lfloor (g-1)/6 \rfloor$ be as above. The computation of χ_V depends on the value of g mod 6.

g mod 6	Affine model	Monodromy
0	$y^2 = x(x^4-1)(x^8+14x^4+1)G(x)$	$(4^{(6)}, 6^{(4)}, 6^{(4)}, \underbrace{2^{(12)}, \ldots, 2^{(12)}}_{d})$
2	$y^2 = x(x^4-1)G(x)$	$(4^{(6)}, 3^{(8)}, 3^{(8)}, \underbrace{2^{(12)}, \ldots, 2^{(12)}}_{d})$
4	$y^2 = x(x^4-1)(x^4+2sx^2+1)G(x)$	$(4^{(6)}, 3^{(8)}, 6^{(4)}, \underbrace{2^{(12)}, \ldots, 2^{(12)}}_{d})$

Table 5. Hyperelliptic curves with automorphism group $\mathrm{SL}_2(3)$. For each even genus $g > 2$, we give a model for the generic hyperelliptic curve of genus g with automorphism group $\mathrm{SL}_2(3)$, together with its monodromy. Here $d = \lfloor (g-1)/6 \rfloor$, $s^2 = -3$, and $G(x)$ is as defined at the beginning of Section 5.1.

- Suppose $g \equiv 2 \bmod 6$. Applying the monodromy information given in Table 5 to (3) yields

$$\chi_V = 2\chi_{\text{triv}} + (d+1)\chi_{(1)} - \chi_{(4)} - 2\chi_{(3)} - d\chi_{(2)}.$$

  Computing the inner product of each irreducible $\mathbb{Q}$-character (see Table 3) with χ_V gives $J_X \sim A_{d+1}^2 \times A_{2d}^2$.
- Suppose $g \equiv 4 \bmod 6$. Applying the monodromy information from Table 5, we find that

$$\chi_V = 2\chi_{\text{triv}} + (d+1)\chi_{(1)} - \chi_{(4)} - \chi_{(6)} - \chi_{(3)} - d\chi_{(2)}.$$

  This gives $J_X \sim A_{d+1}^2 \times A_{2d+1}^2$.
- Finally, suppose $g \equiv 0 \bmod 6$. Using Table 5, we compute that

$$\chi_V = 2\chi_{\text{triv}} + (d+1)\chi_{(1)} - \chi_{(4)} - 2\chi_{(6)} - d\chi_{(2)}.$$

  This gives $J_X \sim A_{d+1}^2 \times A_{2(d+1)}^2$.

5.2. ***The group*** $\mathbf{SL_2(5)}$**.** If g is congruent to 0, 14, 20, or 24 modulo 30 there is a hyperelliptic curve of genus g with automorphism group $\mathrm{SL}_2(5)$. Letting

	Conjugacy class order						
Character	1	2	3	3	4	6	6
$\chi_{(2)}$	12	12	0	0	0	0	0
$\chi_{(3)}$	8	0	2	2	0	0	0
$\chi_{(4)}$	6	6	0	0	2	0	0
$\chi_{(6)}$	4	4	1	1	0	1	1

Table 6. Induced characters for $\mathrm{SL}_2(3)$.

$d = \lfloor (g-1)/30 \rfloor$, the moduli space of such hyperelliptic curves has dimension d, and can be described as follows (see [25, §4.5]): Given d elements $a_1, \ldots, a_d$ of k, set

$$\begin{aligned} G_i(x) = (a_i - 1)x^{60} &- 36(19a_i + 29)x^{55} + 6(26239a_i - 42079)x^{50} \\ &- 540(23199a_i - 19343)x^{45} + 105(737719a_i - 953143)x^{40} \\ &- 72(1815127a_i - 145087)x^{35} - 4(8302981a_i + 49913771)x^{30} \\ &+ 72(1815127a_i - 145087)x^{25} + 105(737719a_i - 953143)x^{20} \\ &+ 540(23199a_i - 19343)x^{15} + 6(26239a_i - 42079)x^{10} \\ &+ 36(19a_i + 29)x^5 + (a_i - 1) \end{aligned}$$

and

$$\begin{aligned} G(x) &= \prod_{i=1}^{d} G_i(x) \\ F(x) &= x^{30} + 522x^{25} - 10005x^{20} - 10005x^{10} - 522x^5 + 1 \\ H(x) &= x^{20} - 228x^{15} + 494x^{10} + 228x^5 + 1 \\ K(x) &= x(x^{10} + 11x^5 - 1). \end{aligned}$$

Then Table 7 lists models and monodromy for the genus-g hyperelliptic curves with automorphism group $\mathrm{SL}_2(5)$, depending on the congruence class of the genus modulo 30.

Again, the induced characters depend only upon the order of the element generating the subgroup. The values for these induced characters on the conjugacy

g mod 30	Affine model	Monodromy
0	$y^2 = K(x)H(x)F(x)G(x)$	$(4^{(30)}, 6^{(20)}, 10^{(12)}, \underbrace{2^{(60)}, \ldots, 2^{(60)}}_{d})$
14	$y^2 = F(x)G(x)$	$(4^{(30)}, 3^{(40)}, 5^{(24)}, \underbrace{2^{(60)}, \ldots, 2^{(60)}}_{d})$
20	$y^2 = K(x)F(x)G(x)$	$(4^{(30)}, 3^{(40)}, 10^{(12)}, \underbrace{2^{(60)}, \ldots, 2^{(60)}}_{d})$
24	$y^2 = H(x)F(x)G(x)$	$(4^{(30)}, 6^{(20)}, 5^{(24)}, \underbrace{2^{(60)}, \ldots, 2^{(60)}}_{d})$

Table 7. Hyperelliptic curves with automorphism group $\mathrm{SL}_2(5)$. For each genus g congruent to 0, 14, 20, or 24 modulo 30, we give a model for the generic hyperelliptic curve of genus g with automorphism group $\mathrm{SL}_2(5)$, together with its monodromy. Here $d = \lfloor (g-1)/30 \rfloor$, and the polynomials $F(x)$, $G(x)$, $H(x)$, and $K(x)$ are as defined at the beginning of Section 5.2.

	Conjugacy class order								
Character	1	2	3	4	5	5	6	10	10
$\chi_{(2)}$	60	60	0	0	0	0	0	0	0
$\chi_{(3)}$	40	0	4	0	0	0	0	0	0
$\chi_{(4)}$	30	30	0	2	0	0	0	0	0
$\chi_{(5)}$	24	0	0	0	4	4	0	0	0
$\chi_{(6)}$	20	20	2	0	0	0	2	0	0
$\chi_{(10)}$	12	12	0	0	2	2	0	2	2

Table 8. Induced characters for $\mathrm{SL}_2(5)$.

classes are listed in Table 8. The group ring for this group is

$$\mathbb{Q}[\mathrm{SL}_2(5)] \cong \mathbb{Q} \oplus M_2(\mathbb{Q}(\sqrt{5})) \oplus M_3(\mathbb{Q}(\sqrt{5})) \oplus M_4(\mathbb{Q}) \oplus M_4(\mathbb{Q}) \oplus M_5(\mathbb{Q}) \oplus M_6(\mathbb{Q}).$$

Computing the inner products of the irreducible $\mathbb{Q}$-characters (which are well known [10, §38]) with χ_V (listed below for the four congruence classes of g) produces decompositions of the form $A_{2(d+1)}^2 \times A_j^4 \times A_k^6$, where d, j, and k are determined by the congruence class of g modulo 30, and where $d = \lfloor (g-1)/30 \rfloor$ is the dimension of the family of curves with this automorphism group.

- Suppose $g \equiv 14 \bmod 30$. Then the Hurwitz character is
$$\chi_V = 2\chi_{\text{triv}} + (d+1)\chi_{(1)} - \chi_{(4)} - \chi_{(3)} - \chi_{(5)} - d\chi_{(2)},$$
and we have $j = 2d+1$ and $k = 3d+1$.
- Suppose $g \equiv 20 \bmod 30$. Then the Hurwitz character is
$$\chi_V = 2\chi_{\text{triv}} + (d+1)\chi_{(1)} - \chi_{(4)} - \chi_{(3)} - \chi_{(10)} - d\chi_{(2)},$$
and we have $j = 2d+1$ and $k = 3d+2$.
- Suppose $g \equiv 24 \bmod 30$. Then the Hurwitz character is
$$\chi_V = 2\chi_{\text{triv}} + (d+1)\chi_{(1)} - \chi_{(4)} - \chi_{(6)} - \chi_{(5)} - d\chi_{(2)},$$
and we have $j = 2(d+1)$ and $k = 3d+2$.
- Finally, suppose $g \equiv 0 \bmod 30$. Then the Hurwitz character is
$$\chi_V = 2\chi_{\text{triv}} + (d+1)\chi_{(1)} - \chi_{(4)} - \chi_{(6)} - \chi_{(10)} - d\chi_{(2)},$$
so $j = 2(d+1)$ and $k = 3(d+1)$.

g mod 12	Affine model	Monodromy
0	$y^2 = (x^8 + 14x^4 + 1)H(x)G(x)$	$(4^{(12)}, 6^{(8)}, 8^{(6)}, \underbrace{2^{(24)}, \ldots, 2^{(24)}}_{d})$
8	$y^2 = H(x)G(x)$	$(4^{(12)}, 3^{(16)}, 8^{(6)}, \underbrace{2^{(24)}, \ldots, 2^{(24)}}_{d})$

Table 9. Hyperelliptic curves with automorphism group W_3. For each genus g congruent to 0 or 8 modulo 12, we give a model for the generic hyperelliptic curve of genus g with automorphism group W_3, together with its monodromy. Here $d = \lfloor (g-1)/12 \rfloor$, and the polynomials $G(x)$ and $H(x)$ are as defined at the beginning of Section 5.3.

5.3. ***The group W_3.*** When g is congruent to 0 or 8 modulo 12, there is a curve of genus g with automorphism group W_3. Models for these curves and their monodromy are listed in Table 9, where we use the notation $d = \lfloor (g-1)/12 \rfloor$,

$$G(x) = \prod_{i=1}^{d} \big(x^{24} + a_i x^{20} + (759 - 4a_i)x^{16} + 2(3a_i + 1288)x^{12} + (759 - 4a_i)x^8 + a_i x^4 + 1\big),$$

and $H(x) = x(x^4 - 1)(x^{12} - 33x^8 - 33x^4 + 1)$. Again, explanations of these models and monodromy can be found in [25].

The group W_3 has seven irreducible $\mathbb{Q}$-characters: two each of degrees 1, 2, and 3, and one of degree 4. The group ring decomposes as follows:

$$\mathbb{Q}[W_3] \cong \mathbb{Q} \oplus \mathbb{Q} \oplus M_2(\mathbb{Q}) \oplus M_2(\mathbb{Q}(\sqrt{2})) \oplus M_3(\mathbb{Q}) \oplus M_3(\mathbb{Q}) \oplus M_4(\mathbb{Q}).$$

As in the previous two cases, there is only one possible value for the induced character, except for the characters induced from subgroups generated by order-4 elements. However, only certain order-4 elements show up in the monodromy and they all have the same induced character. The values for these induced characters on the conjugacy classes are listed in Table 10.

	Conjugacy class order							
Character	1	2	3	4	4	6	8	8
$\chi_{(2)}$	24	24	0	0	0	0	0	0
$\chi_{(3)}$	16	0	4	0	0	0	0	0
$\chi_{(4)}$	12	12	0	2	0	0	0	0
$\chi_{(6)}$	8	8	2	0	0	2	0	0
$\chi_{(8)}$	6	6	0	2	0	0	2	2

Table 10. Induced characters for W_3.

We compute the decomposition of the Jacobian in the two cases as follows:

- When $g \equiv 8 \bmod 12$, the Hurwitz character is
$$\chi_V = 2\chi_{\text{triv}} + (d+1)\chi_{(1)} - \chi_{(4)} - \chi_{(3)} - \chi_{(8)} - d\chi_{(2)}$$
and $J_X \sim A^2_{2(d+1)} \times A^4_{2d+1}$.
- When $g \equiv 0 \bmod 12$, the Hurwitz character is
$$\chi_V = 2\chi_{\text{triv}} + (d+1)\chi_{(1)} - \chi_{(4)} - \chi_{(6)} - \chi_{(8)} - d\chi_{(2)}$$
and $J_x = A^2_{2(d+1),1} \times A^4_{2(d+1),2}$.

Acknowledgments

The author would like to thank the anonymous referees for their helpful suggestions, including pointing out a hitherto unknown word usage issue, and Jordan Ellenberg and Everett Howe for helpful discussions related to this work. The author also appreciates useful comments during the ANTS X conference from Nils Bruin, Noam Elkies, Kiran Kedlaya, and John Voight.

References

[1] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system*, *I*: *The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. MR 1484478

[2] Rolf Brandt and Henning Stichtenoth, *Die Automorphismengruppen hyperelliptischer Kurven*, Manuscripta Math. **55** (1986), no. 1, 83–92. MR 87m:14033

[3] Thomas Breuer, *Characters and automorphism groups of compact Riemann surfaces*, London Mathematical Society Lecture Note Series, no. 280, Cambridge University Press, 2000. MR 2002i:14034

[4] E. Bujalance, J. M. Gamboa, and G. Gromadzki, *The full automorphism groups of hyperelliptic Riemann surfaces*, Manuscripta Math. **79** (1993), no. 3-4, 267–282. MR 94f:20093

[5] Gabriel Cardona, $\mathbb{Q}$*-curves and abelian varieties of* $\mathrm{G}L_2$*-type from dihedral genus* 2 *curves*, in Cremona et al. [6], 2004, pp. 45–52. MR 2005b:11075

[6] John Cremona, Joan-Carles Lario, Jordi Quer, and Kenneth Ribet (eds.), *Modular curves and abelian varieties*: *Papers from the conference held in Bellaterra*, *July* 15–18, 2002, Progress in Mathematics, no. 224, Birkhäuser, Basel, 2004. MR 2004k:11004

[7] Leonard Eugene Dickson, *Invariants of binary forms under modular transformations*, Trans. Amer. Math. Soc. **8** (1907), no. 2, 205–232, errata: [8]. MR 1500782

[8] ———, *Errata*: *"Invariants of binary forms under modular transformations" [Trans. Amer. Math. Soc.* 8 (1907), *no.* 2, 205–232; 1500782*]*, Trans. Amer. Math. Soc. **8** (1907), no. 4, 535. MR 1500482

[9] Claus Diem and Jasper Scholten, *Ordinary elliptic curves of high rank over* $\overline{\mathbb{F}}_p(x)$ *with constant* j*-invariant*, *II*, J. Number Theory **124** (2007), no. 1, 31–41. MR 2008b:11063

[10] Larry Dornhoff, *Group representation theory*, *part A*: *Ordinary representation theory*, Pure and Applied Mathematics, no. 7, Marcel Dekker, New York, 1971. MR 50 #458a

[11] David S. Dummit and Richard M. Foote, *Abstract algebra*, Prentice Hall, Upper Saddle River, NJ, 1999.

[12] Iwan Duursma and Negar Kiyavash, *The vector decomposition problem for elliptic and hyperelliptic curves*, J. Ramanujan Math. Soc. **20** (2005), no. 1, 59–76. MR 2006b:14038

[13] Torsten Ekedahl and Jean-Pierre Serre, *Exemples de courbes algébriques à jacobienne complètement décomposable*, C. R. Acad. Sci. Paris Sér. I Math. **317** (1993), no. 5, 509–513. MR 94j:14029

[14] Noam D. Elkies, Everett W. Howe, and Christophe Ritzenthaler, *Genus bounds for curves with fixed Frobenius eigenvalues*, 2010. arXiv 1006.0822 [math.NT]

[15] Jordan S. Ellenberg, *Endomorphism algebras of Jacobians*, Adv. Math. **162** (2001), no. 2, 243–271. MR 2003c:11061

[16] The GAP Group, *GAP — Groups, Algorithms, and Programming* (*version* 4.4), 2006. http://www.gap-system.org

[17] Josep González, *Fermat Jacobians of prime degree over finite fields*, Canad. Math. Bull. **42** (1999), no. 1, 78–86. MR 2000h:11065

[18] Hoon Hong (ed.), *ISSAC* 2003—*Proceedings of the* 2003 *International Symposium on Symbolic and Algebraic Computation held in Philadelphia, PA, August* 3–6, 2003, Association for Computing Machinery (ACM), New York, 2003. MR 2004j:68018

[19] Everett W. Howe, Franck Leprévost, and Bjorn Poonen, *Large torsion subgroups of split Jacobians of curves of genus two or three*, Forum Math. **12** (2000), no. 3, 315–364. MR 2001e:11071

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

[21] Masato Kuwata, *Quadratic twists of an elliptic curve and maps from a hyperelliptic curve*, Math. J. Okayama Univ. **47** (2005), 85–97. MR 2006i:11061

[22] Jennifer Paulhus, *Decomposing Jacobians of curves with extra automorphisms*, Acta Arith. **132** (2008), no. 3, 231–244. MR 2009c:14049

[23] Jennifer R. Paulhus, *Elliptic factors in Jacobians of low genus curves*, Ph.D. thesis, University of Illinois at Urbana-Champaign, 2007. http://search.proquest.com/docview/304849148

[24] Karl Rubin and Alice Silverberg, *Rank frequencies for quadratic twists of elliptic curves*, Experiment. Math. **10** (2001), no. 4, 559–569. MR 2002k:11081

[25] Tanush Shaska, *Determining the automorphism group of a hyperelliptic curve*, in Hong [18], 2003, pp. 248–254. MR 2005c:14037

[26] Michael Stoll, *Two simple* 2*-dimensional abelian varieties defined over* $\mathbf{Q}$ *with Mordell-Weil group of rank at least* 19, C. R. Acad. Sci. Paris Sér. I Math. **321** (1995), no. 10, 1341–1345. MR 96j:11084

[27] Takuya Yamauchi, *On* $\mathbb{Q}$*-simple factors of Jacobian varieties of modular curves*, Yokohama Math. J. **53** (2007), no. 2, 149–160. MR 2008k:11062

[28] Noriko Yui, *On the Jacobian variety of the Fermat curve*, J. Algebra **65** (1980), no. 1, 1–35. MR 82m:14016

JENNIFER PAULHUS: paulhusj@grinnell.edu
Department of Mathematics and Statistics, Grinnell College, Grinnell, IA 50112, United States

VOLUME EDITORS

Everett W. Howe
Center for Communications Research
4320 Westerra Court
San Diego, CA 92121-1969
United States

Kiran S. Kedlaya
Department of Mathematics
University of California, San Diego
9500 Gilman Drive #0112
La Jolla, CA 92093-0112

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-00-2 (print), 978-1-935107-01-9 (electronic)

First published 2013.

MATHEMATICAL SCIENCES PUBLISHERS
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org **http://msp.org**

THE OPEN BOOK SERIES 1

Tenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the tenth ANTS meeting, held July 9–13, 2012, at the University of California, San Diego. It includes revised and edited versions of the 25 refereed papers presented at the conference, together with extended abstracts of two of the five invited talks.

TABLE OF CONTENTS