ELLIPTIC FACTORS IN JACOBIANS OF HYPERELLIPTIC CURVES WITH CERTAIN AUTOMORPHISM GROUPS

JENNIFER PAULHUS

Abstract. We decompose the Jacobian variety 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 to 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 have been studied in many different contexts. Ekedahl and Serre found examples of curves whose Jacobians split completely into elliptic curves (not necessarily isogenous) [10]. 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 [18], results on torsion [13], and cryptography [9].

Let J_X denote the Jacobian variety of a curve X and $\sim$ 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 curve X of genus g, where E is an elliptic curve and A an abelian variety?

In [16] a method for decomposing the Jacobian variety J_X of a curve X with automorphism group G was developed, 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 maximal possible (t equals 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 consisted of non-hyperelliptic curves.

In this paper we apply the methods in [16] 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 where 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 [6].

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.

The method from [16] is reviewed in Section 3 and proofs of results for genus up to 20 appear in Section 4. 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 3 particular automorphism groups. These groups have special properties which allow us to prove results about the decomposition of the curves' Jacobians for arbitrary genus.

A brief word on which field the curves are defined over in this paper. Unless specifically stated otherwise, curves 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 containing the field of definition of the automorphism group of that particular curve. Partial answers to the question posed above are known for curves over fields of characteristic p.

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 4. Jacobian varieties with several isogenous elliptic curve factors are also found and many are improvements on best known results for t [16]. Two results of particular interest are:

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

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

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*

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

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

The first theorem is an improvement from best known decompositions of genus 4 hyperelliptic curves from [17]. The second theorem is, to the author's knowledge, the first known example in the literature of a hyperelliptic curve with a Jacobian variety that decomposes into 5 isogenous elliptic curves over a number field. Proofs of these results may be found in Section 4.

3. Review of Technique

Fix k an algebraically closed field 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 in k. Also ζ_n will denote a primitive nth root of unity.

Given a curve X of genus g over a field 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], [19].

Kani and Rosen prove a result connecting certain idempotent relations in $\mathrm{End}_0(J_X) = \mathrm{End}(J_X) \otimes_{\mathbb{Z}} \mathbb{Q}$ to isogenies among images of J_X under endomorphisms. If α_1 and α_2 are elements in $\mathrm{End}_0(J_X)$ then $\alpha_1 \sim \alpha_2$ if $\chi(\alpha_1) = \chi(\alpha_2)$, for all $\mathbb{Q}$-characters χ of $\mathrm{End}_0(J_X)$.

Theorem 3. *(Theorem A, [14]) 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 $\mathrm{End}_0(J_X)$, denoted by e. It is a well known result of Wedderburn [8, §18.2] that any group ring of the form $\mathbb{Q}[G]$ has a decomposition into the 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 ith 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 $\mathbb{Q}[G]$:

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

Applying the map e and Theorem 3 to it gives

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

Recall 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, work in [11, §5.2] is used to compute the dimensions of these factors. This requires a certain representation of G.

Definition. A **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 may be computed as follows. Given a map of curves from X to $Y = X/G$ (where Y has genus g_Y), branched at s points with monodromy $g_1, \ldots, g_s \in G$, let $\chi_{\langle g_i \rangle}$ denote the character of G induced from the trivial character of the subgroup of G generated by g_i (observe that $\chi_{\langle 1_G \rangle}$ is the character of the regular representation) and let χ_{triv} be the trivial character of G. The character of V is defined as

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

Note that for a hyperelliptic curve X, the quotient $X/G \cong \mathbb{P}^1$ (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.

Each g_i may be written as a permutation in some S_n, the symmetric group on n elements. 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 ith component from (1), then the dimensions of the summands in (2) are

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

See [11, §5.2] for more information on the dimension computations.

Hence given an 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 which 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, the particular interest is in *isogenous* factors. The following proposition gives a condition for the factors to be isogenous.

Proposition 1. [17] *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 (so 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 jth place), Proposition 1 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 up to genus 20 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, there is at most one family of curves of a given genus with reduced automorphism group isomorphic to each of A_4, S_4, and A_5. A curve with such a reduced automorphism group exists only if the genus is in certain residue classes modulo 6, 12, and 30, respectively [19].

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. This table is a reproduction of one in [19]. Explanations of how the data in this table was produced may be found there, along with affine models for all families. The groups $W_2 = \langle u, v, \mid u^4, v^3, vu^2v^{-1}u^2, (uv)^4\rangle$ and $W_3 = \langle u, v \mid u^4, v^3, u^2(uv)^4, (uv)^8\rangle$ are both groups of order 48.

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

Theorem 4. *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.*

The technique described in the previous section does not necessarily guarantee the finest decomposition of the Jacobian varieties. We have not ruled out the possibility that that some of the abelian varieties $e(\pi_{i,j})J_X$ from (2) decompose further. 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 $\mathbb{Q}$.

4.1. **Finding Monodromy and $\mathbb{Q}$-characters.** Computationally for hyperelliptic curves, finding the branching data is the most difficult part of the technique summarized in Section 3, since the list of possible automorphism groups is well known and most of these groups have easily identifiable character tables. An algorithm to generate a database of automorphism groups of Riemann surfaces was developed in the computer algebra package GAP [12] and implemented up to genus 48 by Breuer [3]. The algorithm relies on

Table 1. Full Automorphism Groups of Hyperelliptic Curves with Certain Reduced Automorphism Groups

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

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.

In Magma [1] we have now implemented a working 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 1 conjugacy class of elements of a certain order for a particular automorphism group) this 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

Table 2. Jacobian Variety Decompositions

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	$E \times E_2^2 \times A_4^3$
	$A_5 \times C_2$	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	$A_{2,1}^2 \times A_{2,2}^2 \times A_3^4$
	$\mathrm{SL}_2(5)$	0	$E^4 \times A_{2,1}^2 \times A_{2,2}^6$

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 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 split into two conjugacy classes. The group ring $\mathbb{Q}[G]$ has Wedderburn decomposition

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

So $\mathrm{SL}_2(3)$ has two $\mathbb{Q}$-characters of degree 1 (χ_1 and χ_2), two of degree 2 (χ_3 and χ_4), and one of degree 3 (χ_5). The values of these characters on the conjugacy classes of $\mathrm{SL}_2(3)$ are well known and given in Table 3 [7].

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

	Conjugacy Class Order						
	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

Recall from Section 2:

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

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

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

Proof. This curve has automorphism group $\mathrm{SL}_2(3)$ and monodromy type $(4^{(6)}, 3^{(8)}, 6^{(4)})$ [19]. 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 similarly for elements of order 3 or 6 since all order 3 and all order 6 elements generate conjugate subgroups. Computing the Hurwitz character yields

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

$$= 2\chi_{triv} + \chi_{\langle 1_G \rangle} - \chi_{\langle g_1 \rangle} - \chi_{\langle g_2 \rangle} - \chi_{\langle g_3 \rangle}.$$

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 zero for all the other characters. Applying (4) and Proposition 1 gives $J_X \sim E_1^2 \times E_2^2$. □

Similar results may be found for $g \geq 8$. See Section 5 for 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 $(3^{(8)}, 3^{(8)}, 2^{(12)}, 2^{(12)})$ [19]. 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 dimension 2 variety and three dimension 1 varieties. Proposition 1 asserts that the three elliptic curves in this decomposition are isogenous and so $J_X \sim A_2 \times E^3$ for some abelian variety A_2 and an elliptic curve E.

Similar computations as in the case of genus 5 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: $S_4 \times C_2$, $\mathrm{GL}_2(3)$, $W_2 = \langle u, v \mid u^4, v^3, vu^2v^{-1}u^2, (uv)^4 \rangle$ and $W_3 = \langle u, v \mid u^4, v^3, u^2(uv)^4, (uv)^8 \rangle$ (the notation for the latter two groups of order 48 is as in [19]).

In genus 3, 11, and 15 there are curves with full automorphism group $S_4 \times C_2$. In [17], 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 [15].

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 degree 1, two degree 2, and three degree 3 irreducible $\mathbb{Q}$-characters. Applying this information to the technique in Section 3 yields the decompositions listed in Table 2

As determined in [19], there is one curve, up to isomorphism, of genus 6 with automorphism group $\mathrm{GL}_2(3)$:

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

Additionally, there is a 1-dimensional family of curves of genus 14 and 18 with this automorphism group.

This group has 2 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 which 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 one dimensional family of curves with this automorphism group. In genus 5 the curve has an affine model

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

in genus 9 a model is

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

and in genus 17 a model is

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

This group has 8 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, $J_X \sim E_1 \times E_2^2 \times A_2^3$ and for genus 17, $J_X \sim E \times A_2^2 \times A_4^3$.

In genus 8 the curve with model

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

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 give the Jacobian of this curve decomposing as $A_2^2 \times E^4$. For higher genus curves with this automorphism group, see general results in Section 5.3.

In [16], 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 the bound of t from the question in the introduction.

4.4. **Reduced Automorphism Group A_5.** Similar to the A_4 case, 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 $\mathrm{SL}_2(5)$ [19]. In genus 14 and 20 there is a hyperelliptic curve with automorphism group isomorphic to $\mathrm{SL}_2(5)$. This group has special properties which allow us to prove results about the decomposition of Jacobians generally for any genus. In Section 5.2 we discuss the general results.

There is one curve each, up to isomorphism, of genus 5, 9, and 15 with automorphism group $A_5 \times C_2$. In Section 2 the following result is mentioned, which we prove now.

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

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

has automorphism group $A_5 \times C_2$*, monodromy type* $(3^{(40)}, 10^{(12)}, 2^{(60)})$*, and* $J_X \sim E^5$ *for the elliptic curve* $E : y^2 = x(x^2 + 11x - 1)$*.*

Proof. The model, automorphism group, and monodromy are from [19] (although note the slight correction here of the model listed in that paper). The irreducible $\mathbb{Q}$-characters of this group consist of 2 each of degree 1, 3, 4, and 5 characters. The monodromy will be g_1, g_2, and $g_3 \in G$ of order 3, 10, and 2 respectively, which may be computed using Breuer's algorithm [3]. Table 4 gives the values of the irreducible $\mathbb{Q}$-characters on the conjugacy classes of $A_5 \times C_2$.

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

	Conjugacy Class Order									
	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

The Hurwitz character is

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

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 zero for all except one of the degree 5 characters, where the inner product is a 2. By (4) and Proposition 1 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 1, J_X is thus isogenous to $E_1^4 \times E_2^5$, for elliptic curves E_i.

Similar computations in genus 15 for a curve with model

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

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 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 $|g_i| = |g_j| = m$. This 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.

Since the induced characters of the trivial character of the subgroups generated by the monodromy elements are completely determined by the orders of the elements, from now on $\chi_{\langle g_i \rangle}$ will mean the induced character of the trivial character of the subgroup generated by an element of G of order i (so no longer the ith element of the monodromy).

Recall 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. $\mathbf{SL}_2(3)$.

For $g > 2$, every even order genus has a hyperelliptic curve over k with automorphism group $\mathrm{SL}_2(3)$. Let

$$G(x) = \prod_i (x^{12} - a_i x^{10} - 33x^8 + 2a_i x^6 - 33x^4 - a_i x^2 + 1).$$

Table 5 gives affine models and monodromy for curves of each even genus. These results may be found in [19]. 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 (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 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.

TABLE 5. Hyperelliptic Curves with Automorphism Group $\mathrm{SL}_2(3)$

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

TABLE 6. Induced Characters for $\mathrm{SL}_2(3)$

	Conjugacy Class Order						
	1	2	3	3	4	6	6
$\chi_{\langle g_2\rangle}$	12	12	0	0	0	0	0
$\chi_{\langle g_3\rangle}$	8	0	2	2	0	0	0
$\chi_{\langle g_4\rangle}$	6	6	0	0	2	0	0
$\chi_{\langle g_6\rangle}$	4	4	1	1	0	1	1

• If X is a curve with genus $g \equiv 2 \bmod 6$, let $d = \frac{g-2}{6}$ be the dimension of the family of curves of genus g with this automorphism group. Applying the monodromy information given in Table 5 to (3) yields

$$\chi_V = 2\chi_{triv} + (d+1)\chi_{\langle 1_g\rangle} - \chi_{\langle g_4\rangle} - 2\chi_{\langle g_3\rangle} - d\chi_{\langle g_2\rangle}.$$

Computing the inner product of each irreducible $\mathbb{Q}$-character (see Table 3) with χ_V gives $J_X \sim A_{d+1}^2 \times A_{2d}^2$.

• If X is a curve with genus $g \equiv 4 \bmod 6$ then $d = \frac{g-4}{6}$ and applying the monodromy information from Table 5,

$$\chi_V = 2\chi_{triv} + (d+1)\chi_{\langle 1_g\rangle} - \chi_{\langle g_4\rangle} - \chi_{\langle g_6\rangle} - \chi_{\langle g_3\rangle} - d\chi_{\langle g_2\rangle}.$$

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

• Finally, if X is a curve with genus $g \equiv 0 \bmod 6$ then $d = \frac{g-6}{6}$ and applying the monodromy in Table 5,

$$\chi_V = 2\chi_{triv} + (d+1)\chi_{\langle 1_g\rangle} - \chi_{\langle g_4\rangle} - 2\chi_{\langle g_6\rangle} - d\chi_{\langle g_2\rangle}.$$

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

5.2. $\mathbf{SL}_2(5)$. If $g \equiv 0$, 14, 20, or 24 mod 30 there is a hyperelliptic curve of that genus with automorphism group $\mathrm{SL}_2(5)$. Table 7 lists models and monodromy for these curves (see [19] for computations of these models) where,

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

$F(x) = x^{30} + 522x^{25} - 10005x^{20} - 10005x^{10} - 522x^5 + 1$
$H(x) = x^{20} - 228x^{15} + 494x^{10} + 228x^5 + 1$
$K(x) = x(x^{10} + 11x^5 - 1)$.

Table 7. Hyperelliptic Curves with Automorphism Group $\mathrm{SL}_2(5)$

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

Again, regardless of which element of a certain order is chosen, the induced character will be the same as those listed in Table 8. The group ring for this group is

$$\mathbb{Q}[\mathrm{SL}_2(5)] \cong \mathbb{Q} \oplus M_2(\mathbb{Q}(\zeta_5)) \oplus M_3(\mathbb{Q}(\zeta_5)) \oplus 2M_4(\mathbb{Q}) \oplus 2M_5(\mathbb{Q}) \oplus M_6(\mathbb{Q}).$$

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

	Conjugacy Class Order								
	1	2	3	4	5	5	6	10	10
$\chi_{\langle g_2 \rangle}$	60	60	0	0	0	0	0	0	0
$\chi_{\langle g_3 \rangle}$	40	0	4	0	0	0	0	0	0
$\chi_{\langle g_4 \rangle}$	30	30	0	2	0	0	0	0	0
$\chi_{\langle g_5 \rangle}$	24	0	0	0	4	4	0	0	0
$\chi_{\langle g_6 \rangle}$	20	20	2	0	0	0	2	0	0
$\chi_{\langle g_{10} \rangle}$	12	12	0	0	2	2	0	2	2

Computing the inner products of the irreducible $\mathbb{Q}$-characters (which are well known [7] and χ_V (listed below for the 4 cases) produces decompositions of the form $A^2_{2(d+1)} \times A^4_j \times A^6_k$ where d, j, and k are determined by the congruence class of g mod 30 (and d is the dimension of the family of curves with this automorphism group).

• If $g \equiv 14 \bmod 30$ then $d = \frac{g-14}{30}$ and the Hurwitz character is

$$\chi_V = 2\chi_{triv} + (d+1)\chi_{\langle 1_g \rangle} - \chi_{\langle g_4 \rangle} - \chi_{\langle g_3 \rangle} - \chi_{\langle g_5 \rangle} - d\chi_{\langle g_2 \rangle}$$

and $j = 2d+1$, and $k = 3d+1$.

• When $g \equiv 20 \bmod 30$ then $d = \frac{g-20}{30}$, the Hurwitz character is

$$\chi_V = 2\chi_{triv} + (d+1)\chi_{\langle 1_g \rangle} - \chi_{\langle g_4 \rangle} - \chi_{\langle g_3 \rangle} - \chi_{\langle g_{10} \rangle} - d\chi_{\langle g_2 \rangle},$$

$j = 2d+1$, and $k = 3d+2$.

• If $g \equiv 24 \bmod 30$ then $d = \frac{g-24}{30}$, the Hurwitz character is

$$\chi_V = 2\chi_{triv} + (d+1)\chi_{\langle 1_g \rangle} - \chi_{\langle g_4 \rangle} - \chi_{\langle g_6 \rangle} - \chi_{\langle g_5 \rangle} - d\chi_{\langle g_2 \rangle}$$

and $j = 2(d+1)$ and $k = 3d+2$.

• And if $g \equiv 0 \bmod 30$ then $d = \frac{g-30}{30}$ and the Hurwitz character is

$$\chi_V = 2\chi_{triv} + (d+1)\chi_{\langle 1_g \rangle} - \chi_{\langle g_4 \rangle} - \chi_{\langle g_6 \rangle} - \chi_{\langle g_{10} \rangle} - d\chi_{\langle g_2 \rangle}$$

so $j = 2(d+1)$ and $k = 3(d+1)$.

5.3. $\mathbf{W_3}$. When $g \equiv 0$ or $8 \bmod 12$, there is a curve of that genus with automorphism group W_3. Models and monodromy are listed in Table 9 where

$$G(x) = \prod_i \left(x^{24} + a_i x^{20} + (759 - 4a_i)x^{16} + 2(3a_i + 1288)x^{12} + (759 - 4a_i)x^8 + a_i x^4 + 1\right)$$

and $H(x) = x(x^4 - 1)(x^{12} - 33x^8 - 33x^4 + 1)$. Again, explanations of these models and monodromy are in [19].

TABLE 9. Hyperelliptic Curves with Automorphism Group W_3

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

W_3 has two each of degree 1, 2, and 3 irreducible $\mathbb{Q}$-characters and one of degree 4 and

$$\mathbb{Q}[W_3] \cong \mathbb{Q} \oplus \mathbb{Q} \oplus M_2(\mathbb{Q}) \oplus M_2(\mathbb{Q}(\zeta_8)) \oplus 2M_3(\mathbb{Q}) \oplus M_4(\mathbb{Q}).$$

As in the previous two cases, there is only one possible value for the induced character, except for order 4 elements. However only certain order 4 elements show up in the monodromy and they all have the same induced character.

TABLE 10. Induced Characters for W_3

	Conjugacy Class Order							
	1	2	3	4	4	6	8	8
$\chi_{\langle g_2\rangle}$	24	24	0	0	0	0	0	0
$\chi_{\langle g_3\rangle}$	16	0	4	0	0	0	0	0
$\chi_{\langle g_4\rangle}$	12	12	0	2	0	0	0	0
$\chi_{\langle g_6\rangle}$	8	8	2	0	0	2	0	0
$\chi_{\langle g_8\rangle}$	6	6	0	2	0	0	2	2

- When $g \equiv 8 \bmod 12$, $d = \frac{g-8}{12}$, the Hurwitz character is

$$\chi_V = 2\chi_{triv} + (d+1)\chi_{\langle 1_g\rangle} - \chi_{\langle g_4\rangle} - \chi_{\langle g_3\rangle} - \chi_{\langle g_8\rangle} - d\chi_{\langle g_2\rangle}$$

and $J_X \sim A^2_{2(d+1)} \times A^4_{2d+1}$.

- When $g \equiv 0 \bmod 12$ and $d = \frac{g-12}{12}$, the Hurwitz character is

$$\chi_V = 2\chi_{triv} + (d+1)\chi_{\langle 1_g\rangle} - \chi_{\langle g_4\rangle} - \chi_{\langle g_6\rangle} - \chi_{\langle g_8\rangle} - d\chi_{\langle g_2\rangle}$$

and $J_x = A^2_{2(d+1),1} \times A^4_{2(d+1),2}$.

6. Acknowledgements

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.

References

[1] Bosma, Wieb and Cannon, John and Playoust, Catherine. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, **24** (3-4): 235–265, 1997.

[2] Brandt, Rolf and Stichtenoth, Henning. Die Automorphismengruppen hyperelliptischer Kurven. *Manuscripta Math.*, **55** (1): 83–92, 1986.

[3] Breuer, Thomas. Characters and automorphism groups of compact Riemann surfaces. *London Mathematical Society Lecture Note Series*, v. 280. Cambridge University Press, Cambridge, 2000.

[4] Bujalance, E. and Gamboa, J.M., and Gromadzki, G. The full automorphism groups of hyperelliptic Riemann surfaces. *Manuscripta Mathematica*, v. 79: 267-282, 1993.

[5] Cardona, Gabriel. $\mathbb{Q}$-curves and abelian varieties of GL_2-type from dihedral genus 2 curves. *Modular curves and abelian varieties*, Progr. Math., **224** : 45–52, 2004.

[6] Dickson, Leonard Eugene. Invariants of binary forms under modular transformations. *Trans. Amer. Math. Soc.*, **8** (2): 205–232, 1907.

[7] Dornhoff, Larry. Group representation theory. Part A: Ordinary representation theory. *Pure and Applied Mathematics*, v. 7. Marcel Dekker Inc., New York, 1971.

[8] Dummit, David S. and Foote, Richard M. *Abstract Algebra*, 2nd edition. Prentice Hall, Upper Saddle River, N.J., 1999.

[9] Duursma, Iwan and Kiyavash, Negar. The vector decomposition problem for elliptic and hyperelliptic curves. *J. Ramanujan Math. Soc.*, **20** (1): 59–76, 2005.

[10] Ekedahl, Torsten and Serre, Jean-Pierre. Exemples de courbes algébriques à jacobienne complètement décomposable. *C. R. Acad. Sci. Paris Sér. I Math.*, **317** (5): 509–513, 1993.

[11] Ellenberg, Jordan S. Endomorphism algebras of Jacobians. *Advances in Mathematics*, **162** (2): 243–271, 2001.

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

[13] Howe, Everett W. and Leprévost, Franck and Poonen, Bjorn. Large torsion subgroups of split Jacobians of curves of genus two or three. *Forum Math.* **12** : 315–364, 2000.

[14] Kani, Ernst and Rosen, Michael. Idempotent relations and factors of Jacobians. *Math. Ann.* **284** (2): 307–327, 1989.

[15] Kuwata, Masato. Quadratic twists of an elliptic curve and maps from a hyperelliptic curve. *Math. J. Okayama Univ.*, **47** : 85–97, 2005.

[16] Paulhus, Jennifer. Decomposing Jacobians of curves with extra automorphisms. *Acta Arithmetica.* **132** : 231–244, 2008.

[17] Paulhus, Jennifer. *Elliptic factors in Jacobians of low genus curves.* PhD Thesis, University of Illinois at Urbana-Champaign, 2007.

[18] Rubin, Karl and Silverberg, Alice. Rank frequencies for quadratic twists of elliptic. curves, *Exper. Math.* **10**: 559–569, 2001.

[19] Shaska, Tanush. Determining the automorphism group of a hyperelliptic curve. *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation.* 248–254 (electronic), ACM, New York, 2003.

Department of Mathematics and Statistics, Grinnell College, Grinnell, IA 50112
E-mail address: paulhusj@grinnell.edu