ACTA ARITHMETICA
132.3 (2008)

Decomposing Jacobians of curves with extra automorphisms

by

Jennifer Paulhus (Urbana, IL, and Manhattan, KS)

1. Introduction. Many interesting questions may be asked about the decomposition of Jacobians of curves. For instance, Ekedahl and Serre [6] find curves which have completely decomposable Jacobians (Jacobians which are isogenous to the product of g not necessarily isogenous elliptic curves). Number-theoretic properties of the elliptic curves that show up in the decomposition of Jacobians of genus 2 curves have been extensively studied. Over finite fields, curves whose Jacobians decompose in certain ways have applications in cryptography [5]. We are particularly interested in the following questions for curves over an algebraically closed field of characteristic zero.

Question 1. *For which genus g can we find a curve X of genus g such that the Jacobian variety J_X of that curve is isogenous to the product of g copies of one elliptic curve E?*

If we cannot find such a curve for a certain genus, we would like to know the bound on the number of isogenous elliptic curves in the decompositions of Jacobians for curves of that genus.

Question 2. *Given a fixed genus g, what is the largest possible integer t such that t copies of an elliptic curve E appear in the decomposition of J_X for some curve X of genus g?*

For curves over a field of characteristic p, partial positive answers to Question 1 are already known. For example, let $r = p^k$ and consider the curve $X : x^{r+1} + y^{r+1} + z^{r+1} = 0$ over the algebraic closure of $\mathbb{F}_p$. For each k the Jacobian variety of this curve is isogenous to E^g for some elliptic curve E where g is the genus of this curve, $g = r(r-1)/2$.

In this paper, we find new examples of nontrivial lower bounds on t for curves of genus up to 10 and positively answer Question 1 for genus 4

2000 *Mathematics Subject Classification*: 14H40, 14H45, 11G05, 14H37.

Key words and phrases: Jacobian varieties, elliptic curves, hyperelliptic curves, low genus curves.

through 6. In genus 3 it is known that the Jacobian variety of the (nonhyperelliptic) Klein curve $x^3y+y^3z+z^3x=0$ is isomorphic to the product of three isomorphic elliptic curves [16]. We find a hyperelliptic curve of genus 3 which positively answers Question 1. This particular curve is also demonstrated in [13] using different techniques.

In Section 2 we describe our methods for decomposing Jacobians. In Sections 3 and 4 we evaluate the factors of these decompositions, first for hyperelliptic curves of genus 3 and 4 and then for arbitrary curves up to genus 10.

We denote the cyclic group and dihedral group of order n as C_n and D_n, respectively. The group D_n is generated by elements r and s of orders $n/2$ and 2, respectively. The group U_n is given by generators and relations $\langle a,b \mid a^2, b^{2n}, abab^{n+1}\rangle$, the group V_n is $\langle a,b \mid a^4, b^n, (ab)^2, (a^{-1}b)^2\rangle$, and the group H_n is $\langle a,b \mid a^4, b^2a^2, (ab)^n\rangle$. Throughout, any field will be of characteristic 0, ζ_n denotes a primitive nth root of unity, and the E_i denote elliptic curves.

2. Techniques. Given a curve X with $G \subseteq \mathrm{Aut}(X)$, there is a canonical map of $\mathbb{Q}$-algebras $e : \mathbb{Q}[G] \to \mathrm{End}_0(J_X) = \mathrm{End}(J_X) \otimes_{\mathbb{Z}} \mathbb{Q}$. Relations on the idempotents of $\mathrm{End}_0(J_X)$ may be defined as follows.

Definition. For $\varepsilon_i \in \mathrm{End}_0(J_X)$, we say that $\varepsilon_1 \sim \varepsilon_2$ if $\chi(\varepsilon_1) = \chi(\varepsilon_2)$ for all virtual $\mathbb{Q}$-characters χ of $\mathrm{End}_0(J_X)$.

The following result of Kani and Rosen shows that these relations in turn lead to isogeny relations among the images of J_X under these idempotent endomorphisms.

Theorem 1 (Theorem A, [12]). *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 we have the isogeny relation

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

Idempotent relations in $\mathbb{Q}[G]$ lead via the map e to idempotent relations in $\mathrm{End}_0(J_X)$. We find idempotent relations in $\mathbb{Q}[G]$ which involve the identity of the group ring and which translate, through e and Theorem 1, to isogeny relations among J_X itself and images of J_X under various endomorphisms. By evaluating these images, we find a decomposition of J_X.

Given a subgroup H of G, one way to create isogeny relations in $\mathbb{Q}[G]$ is to consider relations among the idempotents of the form

$$\varepsilon_H = \frac{1}{|H|} \sum_{h \in H} h.$$

In particular, this leads to a decomposition of J_X in terms of Jacobians of quotient curves X/H.

THEOREM 2 (Theorem B, [12]). *Given a curve X, let $G \leq \mathrm{Aut}(X)$ be a finite group such that $G = H_1 \cup \cdots \cup H_m$ where the subgroups H_i satisfy $H_i \cap H_j = 1_G$ if $i \neq j$. Then we have the following isogeny relation*:

$$J_X^{m-1} \times J_{X/G}^{g} \sim J_{X/H_1}^{h_1} \times \cdots \times J_{X/H_m}^{h_m},$$

where $g = |G|$ and $h_i = |H_i|$ and J^r means the product of J with itself r times.

This method of generating idempotent relations has several limitations. Certain groups have no nontrivial relations on these idempotents (for instance the quaternion group of order 8 which is the automorphism group of a genus 4 hyperelliptic curve). Any factors of J_X that are not Jacobians of quotients of X by a subgroup of G will also not appear. However, finding genera and equations for the quotient curves X/H_i is straightforward.

A second way to create isogeny relations involves decomposing the group ring $\mathbb{Q}[G]$ into a sum of matrix rings over division rings. A theorem of Wedderburn ([4, Chapter 18, Theorem 4]) implies that, for any finite group G, the group ring $\mathbb{Q}[G]$ is isomorphic to the direct sum of matrix rings over division rings $\varDelta_i$, $\mathbb{Q}[G] \cong \bigoplus_i M_{n_i}(\varDelta_i)$. Let $\pi_{i,j}$ denote the idempotent of $\mathbb{Q}[G]$ which is zero everywhere except at the ith component in this decomposition where it is the matrix with a 1 in the (j,j) position and 0 elsewhere. Let $e : \mathbb{Q}[G] \to \mathrm{End}_0(J_X)$ be as above. We apply Theorem 1 to the idempotent relation $1_{\mathbb{Q}[G]} = \sum_{i,j} \pi_{i,j}$ to get the relation

$$J_X \sim \bigoplus_{i,j} e(\pi_{i,j}) J_X. \tag{1}$$

This relation exists for any group G but evaluating the factors is more difficult than in the previous case. This equation is also derived in [7] using a different technique.

3. Hyperelliptic curves. We begin by studying hyperelliptic curves of genus 3 and 4 since these curves have well known automorphism groups [1], [18]. While the techniques we use to decompose Jacobians work for curves over any field, we must fix a field to compute the curve's automorphism group. Since in [1] and [18] the authors compute automorphism groups of curves defined over algebraically closed fields of characteristic zero, our decompositions are for such fields. If we consider the curves to be defined over the field of definition of their automorphism group, as computed in the papers above, then the curve will still have the same automorphism group and thus the same Jacobian decomposition as we find below.

Given a genus 3 or 4 hyperelliptic curve X whose automorphism group contains a subgroup G satisfying the conditions of Theorem 2, we apply Theorem 2 to produce an isogeny relation between the Jacobian of the curve and the product of Jacobians of some of its quotient curves. We use the following well known results to determine the structure of these factors.

THEOREM 3 (Hurwitz). *Given a nonconstant separable map $\phi : X \to Y$ of smooth curves over k, let $e_\phi(P)$ be the ramification index of ϕ at P. Then*

$$2g_X - 2 = (\deg \phi)(2g_Y - 2) + \sum_{P\in X} (e_\phi(P) - 1).$$

FACT 1. *If X is a curve of genus g then J_X has dimension g.*

FACT 2. *Suppose H_1 and H_2 are subgroups of any finite group G that are conjugates of each other. Then $X/H_1 \cong X/H_2$.*

Depending on the particular curve, we may use these results in a variety of ways.

• Suppose a curve X has an automorphism group that contains a subgroup G satisfying the conditions of Theorem 2 and that H is one of the subgroups from Theorem 2. We apply Theorem 3 to the map $\phi_H : X \to X/H$ (recall this map has degree $|H|$) to determine the genus of X/H, which gives us, by Fact 1, the dimension of one factor of the Jacobian of X.

In order to apply Theorem 3 we must be able to determine $e_{\phi(P)}$ for every point P at which ϕ_H is ramified. We use the fixed points of the automorphism σ to determine these values. See Hartshorne ([10, Ex. 4.2.5]) for the relation between ramification and fixed points.

• Sometimes we have an isogeny relation from Theorem 2 involving a power of the Jacobian we would like to decompose. For instance, if the automorphism group of a curve contains the group $\langle a, b\rangle \cong C_2 \times C_2$, Theorem 2 produces the following isogeny:

$$J_X^2 \times J_{X/\langle a,b\rangle}^4 \sim J_{X/\langle a\rangle}^2 \times J_{X/\langle b\rangle}^2 \times J_{X/\langle ab\rangle}^2. \tag{2}$$

However we are interested in how the Jacobian of the curve itself decomposes. To rectify this situation we apply Poincaré's complete reducibility theorem to (2) to get

$$J_X \times J_{X/\langle a,b\rangle}^2 \sim J_{X/\langle a\rangle} \times J_{X/\langle b\rangle} \times J_{X/\langle ab\rangle}. \tag{3}$$

• Finally, the isogeny relation in Theorem 2 must have equal total dimensions on both sides so we may also use dimension arguments to find the dimension of some of the factors if others are known.

Invariants for computing the automorphism group of genus 2 curves were classified by Igusa [11] and decompositions of the Jacobians of these curves have already been studied [9]. For higher genus hyperelliptic curves all possible automorphism groups have also been classified [1], [18]. We therefore begin by applying the preceding techniques to the list of groups which are automorphism groups of hyperelliptic curves of genus 3 and 4. The Jacobian decompositions we find will work for any curve of the given genus with automorphism group containing the group we list, regardless of the field over which the curve is defined.

Again, this technique is not able to give us information about certain genus 3 and 4 curves. For example, the curve $y^2 = x(x^4 - 1)(x^4 + 1)$ has automorphism group Q_8, the quaternion group of order 8. Since the subgroup of order 2 is contained in every nontrivial subgroup of this group, we cannot find a nontrivial relation among the idempotents and so cannot find a decomposition of the Jacobian using the method outlined above.

THEOREM 4. *If X is a genus 3 or 4 curve with automorphism group containing one of the groups in the first columns of Table 1, then J_X decomposes as in the second columns of this table, where Y is a genus 2 curve and E_i some elliptic curve.*

Table 1. Decompositions for genus 3 and 4 hyperelliptic curves

Genus 3

Auto. group	Jacobian decomposition
$C_2 \times C_2$	$E \times J_Y$
$D_4 \times C_2$	$E_1 \times E_2 \times E_3$
H_2	$E_1^2 \times E_2$
U_2	$E_1^2 \times E_2$
D_{12}	$E_1^2 \times E_2$
$D_8 \times C_2$	$E_1^2 \times E_2$
U_6	$E_1^2 \times E_2$
V_8	$E_1^2 \times E_2$
$S_4 \times C_2$	E^3

Genus 4

Auto. group	Jacobian decomposition
$C_2 \times C_2$	$J_{Y_1} \times J_{Y_2}$
$V_2 \cong D_8$	J_Y^2
D_8	J_Y^2
D_{16}	J_Y^2
$D_{10} \times C_2$	$J_{Y_1} \times J_{Y_2}$
U_8	J_Y^2
V_{10}	J_Y^2

We prove this theorem in Sections 3.2 and 3.3. We begin with several general results which will assist us in proving Theorem 4.

3.1. *General cases*

3.1.1. $C_2 \times C_2$. Any hyperelliptic curve of the form $y^2 = x^{2g+2} + \alpha_1 x^{2g} + \alpha_2 x^{2g-2} + \cdots + \alpha_g x^2 + 1$, where g is the genus of the curve, has automorphism group containing $C_2 \times C_2$. We use Theorem 2 to give us a decomposition of the Jacobian of curves of this form for any genus.

THEOREM 5. *Any curve X of the form above has a Jacobian that decomposes as $J_X \sim J_{X_1} \times J_{X_2}$.*

- *If* $g \equiv 0 \pmod 2$ *then* $g_{X_1} = g_{X_2} = g/2$.
- *If* $g \equiv 1 \pmod 2$ *then* $g_{X_1} = (g-1)/2$ *and* $g_{X_2} = (g+1)/2$.

Proof. Applying Theorem 2 to the group $C_2 \times C_2$ gives the following isogeny:

$$J_X^2 \sim J_{X/\langle a\rangle}^2 \times J_{X/\langle b\rangle}^2 \times J_{X/\langle ab\rangle}^2. \tag{4}$$

The three nontrivial automorphisms of this curve send y to $-y$ and fix x (b), send x to $-x$ and fix y (a), and send both x and y to their negatives (ab).

In both cases, the first automorphism is the hyperelliptic involution and so the quotient of X by this automorphism is a genus 0 curve so we disregard it in (4) to get

$$J_X \sim J_{X_1} \times J_{X_2},$$

where $X_1 = X/\langle a\rangle$ and $X_2 = X/\langle ab\rangle$.

When $g \equiv 0 \pmod 2$, the automorphism a has two fixed points $(0, \pm 1)$, as does the automorphism ab (the two points at infinity are fixed). If we apply Theorem 3 to either automorphism, we see that

$$\begin{aligned} 2g - 2 &= 2(2g_{X_i} - 2) + 2, \\ g &= 2g_{X_i}, \end{aligned}$$

so $g_{X_i} = g/2$.

When $g \equiv 1 \pmod 2$, the automorphism a has four fixed points, $(0, \pm 1)$ as well as the two points at infinity. However, the automorphism ab has no fixed points. In these cases Theorem 3 gives

$$\begin{aligned} 2g - 2 &= 2(2g_{X_1} - 2) + 4, \\ g - 1 &= 2g_{X_1}, \end{aligned}$$

and

$$\begin{aligned} 2g - 2 &= 2(2g_{X_2} - 2) + 0, \\ g + 1 &= 2g_{X_2}, \end{aligned}$$

so $g_{X_1} = (g-1)/2$ and $g_{X_2} = (g+1)/2$. ∎

3.1.2. D_{2m}. Let X be a curve with $\mathrm{Aut}(X) \supseteq D_{2m} = \langle r, s \mid r^m, s^2, (rs)^2\rangle$. We consider two cases, m odd and m even.

- *m odd.* In this case, all involutions in D_{2m} are in the same conjugacy class. Applying Theorem 2 gives us

$$J_X \times J_{X/D_{2m}}^2 \sim J_{X/\langle r\rangle} \times J_{X/\langle s\rangle}^2. \tag{5}$$

We let $P(A/B)$ denote the Prym variety of A over B. If $J_{X/D_{2m}} \cong \mathbb{P}^1$ then

$$J_{X/\langle r\rangle} \times P(X \,/\, X/\langle r\rangle) \sim J_X \sim J_{X/\langle r\rangle} \times J_{X/\langle s\rangle}^2,$$

and so by Poincaré's complete reducibility theorem we have $P(X \,/\, X/\langle r\rangle) \cong J^2_{X/\langle s\rangle}$. This particular result is stated in [17] with a different proof.

More general results involving Jacobian decompositions and Prym varieties may also be found in [3]. We obtain several of their decompositions using our techniques by replacing $J_{X/\langle r\rangle}$ with $J_{X/D_{2m}} \times P(X/\langle r\rangle \,/\, X/D_{2m})$ and replacing $J_{X/\langle s\rangle}$ with $J_{X/D_{2m}} \times P(X/\langle s\rangle \,/\, X/D_{2m})$ in (5).

- *m even.* In this case we have from Theorem 2 the decomposition

$$J_X \times J^2_{X/D_{2m}} \sim J_{X/\langle r^{m/4}\rangle} \times J_{X/\langle s\rangle} \times J_{X/\langle sr^{m/4}\rangle}. \tag{6}$$

When m is a power of two, s and $sr^{m/4}$ are conjugates of each other, which yields

$$J_X \times J^2_{X/D_{2m}} \sim J_{X/\langle r^{m/4}\rangle} \times J^2_{X/\langle s\rangle}. \tag{7}$$

When D_{2m} is the full automorphism group of the curve, $r^{m/4}$ is the hyperelliptic involution and so (6) becomes

$$J_X \sim J_{X/\langle s\rangle} \times J_{X/\langle sr^{m/4}\rangle},$$

while (7) is

$$J_X \sim J^2_{X/\langle s\rangle}.$$

3.2. *Genus 3.* In most genus 3 cases, we obtain the finest decomposition by looking at a subgroup of the automorphism group isomorphic to $C_2 \times C_2$ ($\langle a, b\rangle$) and applying Theorem 5. We prove Theorem 4 for a few cases. The other cases follow in a similar way.

3.2.1. $C_2 \times C_2$. Any curve X whose full automorphism group is isomorphic to $C_2 \times C_2$ has only two nonhyperelliptic involutions. By Theorem 5 we know that the quotient of X by one of the involutions must be of genus 1 and the other quotient must be of genus 2. (We can also see this by applying Theorem 3 and information about the fixed points of each automorphism.) Thus $J_X \sim E \times J_Y$ for some elliptic curve E and a genus 2 curve Y.

3.2.2. $D_4 \times C_2$. This group has subgroups isomorphic to $C_2 \times C_2$, $\langle a, c\rangle$. Unlike our previous case, however, there are subgroups of this form which do not contain the hyperelliptic involution and so we are able to get more information about the Jacobian of this curve. Theorem 2 produces

$$J_X \times J^2_{X/\langle a,c\rangle} \sim J_{X/\langle a\rangle} \times J_{X/\langle c\rangle} \times J_{X/\langle ac\rangle}.$$

Considering fixed points and using Theorem 3, we conclude that each quotient on the right has genus 1 and so $J_X \sim E_1 \times E_2 \times E_3$ for three elliptic curves.

3.2.3. D_{12}. The group D_{12} has a subgroup isomorphic to S_3 generated by s and r^2. Theorem 2 then gives

$$J_X^3 \times J_{X/\langle r^2,s\rangle}^6 \sim J_{X/\langle r^2\rangle}^3 \times J_{X/\langle s\rangle}^2 \times J_{X/\langle sr^2\rangle}^2 \times J_{X/\langle sr^4\rangle}^2. \tag{8}$$

The last three Jacobians of quotient curves on the right are isogenous by Fact 2 and so (8) may be rewritten as

$$J_X^3 \times J_{X/\langle r^2,s\rangle}^6 \sim J_{X/\langle r^2\rangle}^3 \times J_{X/\langle s\rangle}^6. \tag{9}$$

By applying Poincaré's complete reducibility theorem to (9) we reduce the exponents

$$J_X \times J_{X/\langle r^2,s\rangle}^2 \sim J_{X/\langle r^2\rangle} \times J_{X/\langle s\rangle}^2. \tag{10}$$

Both curves on the right side of (10) are genus 1 and so $X/\langle r^2, s\rangle$ must be genus 0 by dimension arguments. Thus J_X is isogenous to the product of three elliptic curves, two of which are isogenous.

Any hyperelliptic curve of genus 3 with automorphism group containing D_{12} over an algebraically closed field of characteristic zero is isomorphic to a curve of the form $y^2 = x(x^6 + \alpha x^3 + 1)$ for some α in the field.

The automorphism group of this curve is given by generators $r : (x, y) \mapsto (\zeta_3 x, \zeta_6 y)$ and $s : (x, y) \mapsto (1/x, y/x^4)$. The quotient map from X to $X/\langle s\rangle$ is given by

$$(x, y) \mapsto \left(x + \frac{1}{x}, y + \frac{y}{x^4}\right),$$

while the quotient map from X to $X/\langle r^2\rangle$ is given by

$$(x, y) \mapsto (x^3, xy).$$

Computations with resultants show that $X/\langle s\rangle$ is isomorphic to the curve $y^2 = x^3 - 3x + \alpha$ which has j-invariant $6912/(4 - \alpha^2)$, while $X/\langle r^2\rangle$ is isomorphic to $y^2 = x^3 + \alpha x^2 + x$ which has j-invariant $256(\alpha^2 - 3)^3/(\alpha^2 - 4)$.

3.2.4. $S_4 \times C_2$. There is only one curve over an algebraically closed field of characteristic zero, up to isomorphism, with automorphism group $S_4 \times C_2$, the curve $X : y^2 = x^8 + 14x^4 + 1$. This group has a subgroup $H = \langle((12)(34), 1_{C_2}), ((13)(24), 1_{C_2})\rangle$ which is isomorphic to $C_2 \times C_2$. The element $((12)(34), 1_{C_2})$ represents the automorphism that sends (x, y) to $(-1/x, y/x^4)$, and the element $((13)(24), 1_{C_2})$ represents the automorphism that sends (x, y) to $(-x, y)$. Applying Theorem 2 to the subgroup H gives

$$J_X \sim J_{X/\langle((12)(34),1_{C_2})\rangle} \times J_{X/\langle((13)(24),1_{C_2})\rangle} \times J_{X/\langle((14)(23),1_{C_2})\rangle}. \tag{11}$$

All the subgroups on the right side of (11) are conjugates, and thus $J_X \sim E^3$ by Fact 2. This positively answers Question 1 for genus 3. This elliptic curve is $y^2 = x^4 + 14x^2 + 1$ which has j-invariant $35152/9$ and is isogenous to $X_0(24)$.

3.3. *Genus 4.* As with the genus 3 cases, all the automorphism groups of genus 4 curves which we consider have subgroups isomorphic to $C_2 \times C_2$. Theorem 5 shows that $J_X \sim J_{X_1} \times J_{X_2}$, where X_i are possibly isogenous genus 2 curves.

Unfortunately, all the genus 2 quotient curves have cyclic automorphism groups and so we cannot decompose them further (at least using this method) into the product of two elliptic curves. Again, we demonstrate with several examples.

3.3.1. D_8 *and* D_{16}. Let X be a curve whose automorphism group contains D_8 or D_{16}. Let $n = 8$ or 16 (the order of the group). In either case, we form the following isogeny relation from Theorem 2:

$$J_X \times J^2_{X/\langle r^{n/4}, s\rangle} \sim J_{X/\langle r^{n/4}\rangle} \times J_{X/\langle s\rangle} \times J_{X/\langle sr^{n/4}\rangle}. \tag{12}$$

In both cases $r^{n/4}$ is the hyperelliptic involution and so $X/\langle r^{n/4}\rangle$ has genus 0. Also, s and $sr^{n/4}$ are in the same conjugacy class so $J_{X/\langle s\rangle}$ and $J_{X/\langle sr^{n/4}\rangle}$ (both genus 2 curves) are isogenous. So, from (12) we conclude that J_X is the square of the Jacobian of a genus 2 curve. Alternatively we may draw the same conclusion from Section 3.1.2, m even.

3.3.2. $D_{10} \times C_2 \simeq D_{20}$. As with the previous cases, there are quite a few subgroups of D_{20} which are isomorphic to $C_2 \times C_2$ and contain the hyperelliptic involution r^5. However, unlike the previous case, none of these subgroups contain two elements from the same conjugacy class. The best we can conclude is that the Jacobian of curves in this family is the product of two Jacobians of genus 2 curves

$$J_X \sim J_{X/\langle s\rangle} \times J_{X/\langle sr^5\rangle}. \tag{13}$$

3.4. *Genus 5.* As a special example of Theorem 2, we demonstrate an infinite family of hyperelliptic curves of genus 5 whose Jacobians are isogenous to the product of four isogenous copies of one elliptic curve and one copy of a nonisogenous elliptic curve.

The curve $X : y^2 = x^{12} + \alpha x^6 + 1$, for α in our algebraically closed field of characteristic zero, has automorphism group $D_{12} \times C_2$ over $\mathbb{Q}(\sqrt{-3})$, the field of definition of the automorphism group of this curve over $\mathbb{C}$. We apply Theorem 2 to the subgroup of the automorphism group of this curve that is generated by the hyperelliptic involution and the involution that sends x to $-x$ and fixes y. This gives $J_X \sim J_{A_1} \times J_{A_2}$, where $A_1 : y^2 = x^6 + \alpha x^3 + 1$ and $A_2 : y^2 = x(x^6 + \alpha x^3 + 1)$. The Jacobian of A_1 is isogenous to the square of the elliptic curve $E_1 : y^2 = x^3 + (3x + 2 + \alpha)^2$ (see [5]), while we know from Section 3.2.3 that the Jacobian of A_2 is isogenous to $E_2^2 \times E_3$, where $E_2 : y^2 = x^3 - 3x + \alpha$ and $E_3 : y^2 = x^3 + \alpha x^2 + x$.

For every positive integer n there is a polynomial in two variables $\Phi_n(j_1, j_2)$ which takes as input two j-invariants of elliptic curves and outputs a zero if there is an n-isogeny between the curves (often referred to as a "modular polynomial"). Hence, for all $n \in \mathbb{Z}_{>0}$ there is an α which is found by plugging the j-invariants of E_1 and E_2 into Φ_n and solving for the α that makes this polynomial zero. The E_1 and E_2 with this particular α value are thus n-isogenous. This produces an infinite family of hyperelliptic curves such that $J_X \cong E_1^4 \times E_3$.

4. Curves with $g \leq 10$. For higher genus curves, the idempotent relations we use above often do not give fine enough decompositions to answer Questions 1 and 2. We therefore use the second idempotent relations discussed in Section 2. Recall (1) from Section 2,

$$J_X \sim \bigoplus_{i,j} e(\pi_{i,j}) J_X. \tag{14}$$

Our primary goal is to study elliptic curves that show up in the decomposition above so we need to identify which summands in (14) have dimension 1. We use work of Ellenberg in [7] to compute the dimensions of these factors. We first define a special representation of G.

Definition. Given a map of curves from X to $Y = X/G$ (where Y has genus g_Y), branched at s points with monodromy $g_1, \ldots, g_s$, let $\chi_{\langle g_i \rangle}$ denote the character of G induced from the trivial character of the subgroup generated by g_i, and let χ_{triv} be the trivial character of G. There is a special character of G which is the character for a rational representation, defined as

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

A *Hurwitz representation* of G is the rational representation of such a character.

Suppose V is a Hurwitz representation for G. We have the equality

$$\dim e(\pi_{i,j}) J_X = \frac{1}{2} \dim_{\mathbb{Q}} \pi_{i,j} V.$$

If χ, χ_i are the characters associated to V and V_i, the irreducible $\mathbb{Q}$-representations of G, then the dimension over $\mathbb{Q}$ of $\pi_{i,j} V$ is $\langle \chi_i, \chi \rangle$. Observe that the dimension of $e(\pi_{i,j})$ is not dependent on j.

In [14], the authors compute automorphism groups and monodromies of covers for certain curves up to genus 10. We use the method outlined above on their data to search for examples of curves that answer the questions posed in Section 1. Since the original questions we pose involve finding curves whose Jacobians have many isogenous elliptic curve factors, the following theorem will be useful.

THEOREM 6. *With notation as above*, $e(\pi_{i,j})J_X$ *is isogenous to* $e(\pi_{i,k})J_X$.

Proof. Let M denote the $i \times i$ matrix with zeros at the (j, j) and (k, k) entries, a value of 1 on the rest of the diagonal entries, a 1 at the (j, k) and (k, j) entries, and zeros everywhere else. It is a quick exercise in matrix multiplication to show that M has order 2. Conjugating $\pi_{i,j}$ by M gives $\pi_{i,k}$. We see this by observing that $M\pi_{i,j} = \pi_{i,k}M$.

Now since e is a homomorphism and M is, in particular, a unit, $e(M\pi_{i,j}) = M'e(\pi_{i,j}) = e(\pi_{i,k}M) = e(\pi_{i,k})M'$, where M' is also a unit, hence an isogeny of the Jacobian. But then, since M' is an isogeny, $M'e(\pi_{i,j})J_X \sim e(\pi_{i,j})J_X$ and $e(\pi_{i,k})M'J_X \sim e(\pi_{i,k})J_X$. Hence $e(\pi_{i,j})J_X \sim e(\pi_{i,k})J_X$. ■

Our goal, then, is to use the data in [14] to find automorphism groups G of curves up to genus 10 such that $\mathbb{Q}[G]$ has a summand of the form $M_g(\varDelta)$ somewhere in its decomposition. The groups in that paper are listed with their ordered pair number from the table of small groups in the computer algebra package GAP [8], where the first number is the order of the group and the second number is the group's number in the GAP table for that order of group. We will use this notation for certain groups in Theorems 7 and 8. A program being developed for GAP [2], [15] computes the decomposition of $\mathbb{Q}[G]$ for almost all G which we encounter in low genus.

Once we have such examples, we compute the dimension of the summands from (14) by finding both the Hurwitz character and the irreducible $\mathbb{Q}$-representations, and then computing the inner products of the irreducible $\mathbb{Q}$-characters with the Hurwitz character.

If the summand corresponding to the summand of $\mathbb{Q}[G]$ of the form $M_g(\varDelta)$ is of dimension 1 then we have found a curve such that $J_X \sim E^g$.

THEOREM 7. *For genus* 3 *through* 6 *we demonstrate curves which positively answer Question* 1. *The automorphism groups of the curves are listed in Table* 2. *Except for the genus* 3 *case*, *the curves are not hyperelliptic.*

Table 2. Examples positively answering Question 1

Genus	Automorphism group	Jacobian decomposition
3	$S_4 \times C_2$	$J_X \sim E^3$
4	$(72, 40)$	$J_X \sim E^4$
5	$(160, 234)$	$J_X \sim E^5$
6	$(72, 15)$	$J_X \sim E^6$

We prove the theorem above for genus 5. The genus 4 and 6 cases work in much the same way. The genus 3 case is the same curve from Section 3.2.4.

4.1. *Genus 5.* In genus 5 there is one curve, up to isomorphism, whose automorphism group G is group number $(160, 234)$ from the table of small groups in GAP [8]. The monodromy of this cover consists of an order 2 element, an order 4 element, and an order 5 element. See [14] for a proof of these statements. Also,

$$\mathbb{Q}[G] \cong 2\mathbb{Q} \oplus M_2(\mathbb{Q}(\zeta_5 + \zeta_5^{-1})) \oplus 6M_5(\mathbb{Q}).$$

A quick search of all combinations of one each of order 2, 4, and 5 elements reveals a limited number of such combinations whose product is 1_G and which generate G. One of these must be the monodromy for the covering $X \to X/G$. We compute the Hurwitz character for each possible monodromy and, regardless of which one we use, the inner product of any of these Hurwitz characters with the two linear $\mathbb{Q}$-characters is zero. Hence, by a simple dimension argument, the dimension of $e(\pi_{i,j})J_X$ for i equal to one of 4 through 9 must be one, while the dimension of the others, as well as $i = 3$, must be zero. By Theorem 6, this means that $J_X \sim E^5$.

4.2. *Lower bounds on t for low genus.* For genus greater than 6, our computations produced no groups G from the data in [14] such that there is a $g \times g$ matrix ring in the decomposition of $\mathbb{Q}[G]$. However, we can still use the method above to find nontrivial lower bounds for the t mentioned in the introduction.

For instance, the GAP group $G = (192, 955)$ is the automorphism group of a curve of genus 9,

$$\mathbb{Q}[G] \cong 4\mathbb{Q} \oplus 4M_3(\mathbb{Q}) \oplus 2M_2(\mathbb{Q}) \oplus 4M_6(\mathbb{Q}),$$

and when we compute the inner product of the cover's monodromy with the irreducible $\mathbb{Q}$-characters, we get a value of 2 for one of the order 3 characters and one of the order 6 characters and a value of 0 for the rest of the inner products. Thus $J_X \sim E_1^3 \times E_2^6$ and so for genus 9, $t \geq 6$.

Table 3. Examples for bounds on t

Genus	Automorphism group	Jacobian decomposition
7	$(32, 43)$	$J_X \sim E_1 \times E_2^2 \times E_3^4$
	$S_3 \times S_3$	
	$S_3 \times D_8$	
8	$(32, 18)$	$J_X \sim E_1^2 \times E_2^2 \times A$
9	$(192, 955)$	$J_X \sim E_1^3 \times E_2^6$
10	$(72, 40)$	$J_X \sim E_1^2 \times E_2^4 \times E_3^4$

Theorem 8. *For genus* 7 *through* 10 *we find nontrivial lower bounds for* t *in Question* 2. *We summarize our results in Table* 3 *where* E_i *denotes an elliptic curve and* A *is some abelian variety. The curves with such automorphism groups are not hyperelliptic.*

In the genus 7 case there are three separate one-dimensional families which give a lower bound of 4 for t. In genus 8 and 10, the automorphism groups given are the automorphism groups of one-dimensional families of curves. In genus 9, the group listed is the automorphism group of one curve of that genus, up to isomorphism.

References

[1] R. Brandt und H. Stichtenoth, *Die Automorphismengruppen hyperelliptischer Kurven*, Manuscripta Math. 55 (1986), 83–92.

[2] O. Broche Cristo, A. Konovalov, A. Olivieri, G. Olteanu, and Á. del Río, *Wedderga–Wedderburn decomposition of group algebras, Version 4.1*, 2006, http://www.um.es/adelrio/wedderga.htm.

[3] A. Carocca, S. Recillas, and R. E. Rodríguez, *Dihedral groups acting on Jacobians*, in: Complex Manifolds and Hyperbolic Geometry (Guanajuato, 2001), Contemp. Math. 311, Amer. Math. Soc., Providence, RI, 2002, 41–77.

[4] D. S. Dummit and R. M. Foote, *Abstract Algebra*, 2nd ed., Prentice-Hall, Upper Saddle River, NJ, 1999.

[5] I. Duursma and N. Kiyavash, *The vector decomposition problem for elliptic and hyperelliptic curves*, J. Ramanujan Math. Soc. 20 (2005), 59–76.

[6] T. Ekedahl et J.-P. Serre, *Exemples de courbes algébriques à jacobienne complètement décomposable*, C. R. Acad. Sci. Paris Sér. I Math. 317 (1993), 509–513.

[7] J. S. Ellenberg, *Endomorphism algebras of Jacobians*, Adv. Math. 162 (2001), 243–271.

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

[9] P. Gaudry and É. Schost, *On the invariants of the quotients of the Jacobian of a curve of genus 2*, in: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (Melbourne, 2001), Lecture Notes in Comput. Sci. 2227, Springer, Berlin, 2001, 373–386.

[10] R. Hartshorne, *Algebraic Geometry*, Grad. Texts in Math. 52, Springer, New York, 1977.

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

[12] E. Kani and M. Rosen, *Idempotent relations and factors of Jacobians*, Math. Ann. 284 (1989), 307–327.

[13] M. Kuwata, *Quadratic twists of an elliptic curve and maps from a hyperelliptic curve*, Math. J. Okayama Univ. 47 (2005), 85–97.

[14] K. Magaard, T. Shaska, S. Shpectorov, and H. Völklein, *The locus of curves with prescribed automorphism group*, in: Communications in Arithmetic Fundamental Groups (Kyoto, 1999/2001), Sūrikaisekikenkyūsho Kōkyūroku, 1267 (2002), 112–141.

[15] A. Olivieri and Á. del Río, *An algorithm to compute the primitive central idempotents and the Wedderburn decomposition of a rational group algebra*, J. Symbolic Comput. 35 (2003), 673–687.

[16] D. T. Prapavessi, *On the Jacobian of the Klein curve*, Proc. Amer. Math. Soc. 122 (1994), 971–978.

[17] J. Ries, *The Prym variety for a cyclic unramified cover of a hyperelliptic Riemann surface*, J. Reine Angew. Math. 340 (1983), 59–69.

[18] T. Shaska, *Determining the automorphism group of a hyperelliptic curve*, in: Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2003, 248–254.

[19] *University of Sydney*, MAGMA, Version 2.11, 2004, http://magma.maths.usyd.edu.au/magma/.

Department of Mathematics
University of Illinois at Urbana-Champaign
Urbana, IL 61801, U.S.A.

Current address:
Department of Mathematics
Kansas State University
Manhattan, KS 66506, U.S.A.
E-mail: paulhus@math.ksu.edu

Received on 10.1.2007
and in revised form on 12.1.2008 (5366)