Decomposing Jacobian varieties using automorphism groups

Jennifer Paulhus

Kansas State University
paulhus@math.ksu.edu
www.math.ksu.edu/∼paulhus

My original interest in Jacobian variety decomposition was motivated by the following question.

Question

Given a genus g, what is the largest integer t such that there is some curve X of genus g with $J_X \sim E^t \times A$ for some elliptic curve E and an abelian variety A?

The $\dim(J_X) = g$ so the largest t can possibly be is g.

Suppose we have a genus g hyperelliptic curve $X : y^2 = f(x)$ such that $J_X \sim E^g$.

Suppose we have a genus g hyperelliptic curve $X : y^2 = f(x)$ such that $J_X \sim E^g$. There is a map $\phi : X \to \underbrace{E \times E \times \cdots \times E}_{g}$.

Suppose we have a genus g hyperelliptic curve $X : y^2 = f(x)$ such that $J_X \sim E^g$. There is a map $\phi : X \to \underbrace{E \times E \times \cdots \times E}_{g}$.

If we let $K = \mathbb{Q}(\sqrt{f(s)})$ for $s \in \mathbb{Q}$ then there is a point $P = (s, \sqrt{f(s)}) \in X(K)$ and so for $P_i \in E/\mathbb{Q}(\sqrt{f(s)})$

$$\phi(P) = P_1 \times P_2 \times P_3 \times \cdots \times P_g.$$

Suppose we have a genus g hyperelliptic curve $X : y^2 = f(x)$ such that $J_X \sim E^g$. There is a map $\phi : X \to \underbrace{E \times E \times \cdots \times E}_{g}$.

If we let $K = \mathbb{Q}(\sqrt{f(s)})$ for $s \in \mathbb{Q}$ then there is a point $P = (s, \sqrt{f(s)}) \in X(K)$ and so for $P_i \in E/\mathbb{Q}(\sqrt{f(s)})$

$$\phi(P) = P_1 \times P_2 \times P_3 \times \cdots \times P_g.$$

We can do some work (using heights) to possibly show that the P_i are linearly independent and so E has rank at least g.

Suppose we have a genus g hyperelliptic curve $X : y^2 = f(x)$ such that $J_X \sim E^g$. There is a map $\phi : X \to \underbrace{E \times E \times \cdots \times E}_{g}$.

If we let $K = \mathbb{Q}(\sqrt{f(s)})$ for $s \in \mathbb{Q}$ then there is a point $P = (s, \sqrt{f(s)}) \in X(K)$ and so for $P_i \in E/\mathbb{Q}(\sqrt{f(s)})$

$$\phi(P) = P_1 \times P_2 \times P_3 \times \cdots \times P_g.$$

We can do some work (using heights) to possibly show that the P_i are linearly independent and so E has rank at least g.

So we would construct elliptic curves over an infinite number of quadratic extensions with rank at least g.

For genus 2 curves:

- Gaudry and Schost ('01) show that genus 2 curves with certain automorphism groups have Jacobians that decompose into the product of two elliptic curves which are 2-isogenous to each other.

For genus 2 curves:

- Gaudry and Schost ('01) show that genus 2 curves with certain automorphism groups have Jacobians that decompose into the product of two elliptic curves which are 2-isogenous to each other.
- Cardona, Quer and others ('99, '04, '07) show that genus 2 curves with dihedral groups as automorphism groups have elliptic factors with special arithmetic properties ($\mathbb{Q}$-curves, curves of GL_2-type).

Most of these results relied on a complete understanding of the moduli space of genus 2 curves.

Most of these results relied on a complete understanding of the moduli space of genus 2 curves.

Howe, Leprévost, and Poonen ('00) produce curves of genus 2 and 3 whose Jacobians have large torsion subgroups. Their construction specifically relies on the curves having split Jacobians.
Their method involves finding elliptic curves with large torsion subgroups and proving the product of these elliptic curves may be recognized as the Jacobian of a genus 2 or 3 curve. This is a somewhat ad hoc method.

Given a curve X of genus g we let J_X denote the Jacobian variety of X and we let G denote $\mathrm{Aut}(X)$.

D_n, C_n are the dihedral and cyclic groups of order n, respectively, ζ_n is a primitive n-th root of unity.

Given a curve X of genus g we let J_X denote the Jacobian variety of X and we let G denote $\mathrm{Aut}(X)$.

D_n, C_n are the dihedral and cyclic groups of order n, respectively, ζ_n is a primitive n-th root of unity.

An Example

$X : y^2 = x(x^6 + x^3 + 1)$

$$Aut(X) = D_{12} = \langle r, s \mid r^6, s^2, (rs)^2 \rangle \textit{ where}$$

$$r : (x, y) \to (\zeta_3 x, \zeta_6 y) \qquad s : (x, y) \to (1/x, y/x^4)$$

The techniques described below work for curves defined over any field. However a field must be specified in order to compute the automorphism group of the curve.

We assume all curves are defined over an algebraically closed field of characteristic zero.

The techniques described below work for curves defined over any field. However a field must be specified in order to compute the automorphism group of the curve.

We assume all curves are defined over an algebraically closed field of characteristic zero.

$\mathrm{End}_0(J_X) := \mathrm{End}(J_X) \otimes_{\mathbb{Z}} \mathbb{Q}$

Definition

Given $\varepsilon_1, \varepsilon_2 \in \mathrm{End}_0(J_X)$,

$$\varepsilon_1 \sim \varepsilon_2$$

when $\chi(\varepsilon_1) = \chi(\varepsilon_2)$ for all (virtual) characters χ in $\mathrm{End}_0 J_X$.

The techniques described below work for curves defined over any field. However a field must be specified in order to compute the automorphism group of the curve.

We assume all curves are defined over an algebraically closed field of characteristic zero.

$\mathrm{End}_0(J_X) := \mathrm{End}(J_X) \otimes_{\mathbb{Z}} \mathbb{Q}$

Definition

Given $\varepsilon_1, \varepsilon_2 \in \mathrm{End}_0(J_X)$,

$$\varepsilon_1 \sim \varepsilon_2$$

when $\chi(\varepsilon_1) = \chi(\varepsilon_2)$ for all (virtual) characters χ in $\mathrm{End}_0 J_X$.

Natural map of $\mathbb{Q}$-algebras $e : \mathbb{Q}[G] \to \mathrm{End}_0(J_X)$

An Example

Given a group G, let $H \leq G$. We define idempotents of $\mathbb{Q}[G]$

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

For many groups there are relations among these idempotents.

An Example

Given a group G, let $H \leq G$. We define idempotents of $\mathbb{Q}[G]$

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

For many groups there are relations among these idempotents. For example:

Let G be the Klein 4 group with proper, non-trivial subgroups H_1, H_2, H_3.

$$\varepsilon_{1_G} + 2\varepsilon_G = \varepsilon_{H_1} + \varepsilon_{H_2} + \varepsilon_{H_3}$$

Another Example

A theorem of Wedderburn says that for any finite group G,

$$\mathbb{Q}[G] = \bigoplus_i M_{n_i}(\Delta_i)$$

where Δ_i is a division ring.

Another Example

A theorem of Wedderburn says that for any finite group G,

$$\mathbb{Q}[G] = \bigoplus_i M_{n_i}(\Delta_i)$$

where Δ_i is a division ring.

Let $\pi_{i,j} \in \mathbb{Q}[G]$ be the idempotent which is the zero matrix in all components except the ith matrix where it is the matrix with a 1 in the j,j position and zeros elsewhere.

Another Example

A theorem of Wedderburn says that for any finite group G,

$$\mathbb{Q}[G] = \bigoplus_i M_{n_i}(\Delta_i)$$

where Δ_i is a division ring.

Let $\pi_{i,j} \in \mathbb{Q}[G]$ be the idempotent which is the zero matrix in all components except the ith matrix where it is the matrix with a 1 in the j,j position and zeros elsewhere.

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

Theorem (Kani-Rosen, '89)

If $\varepsilon_i, \varepsilon'_j \in End_0(J_X)$ *are idempotents, then*

$$\varepsilon_1 + \cdots + \varepsilon_m \sim \varepsilon'_1 + \cdots + \varepsilon'_n$$

if and only if

$$\varepsilon_1(J_X) \times \cdots \times \varepsilon_m(J_X) \sim \varepsilon'_1(J_X) \times \cdots \times \varepsilon'_n(J_X).$$

Theorem (Kani-Rosen, '89)

If $\varepsilon_i, \varepsilon'_j \in End_0(J_X)$ are idempotents, then

$$\varepsilon_1 + \cdots + \varepsilon_m \sim \varepsilon'_1 + \cdots + \varepsilon'_n$$

if and only if

$$\varepsilon_1(J_X) \times \cdots \times \varepsilon_m(J_X) \sim \varepsilon'_1(J_X) \times \cdots \times \varepsilon'_n(J_X).$$

Find idempotent relations in $\mathbb{Q}[G]$ containing the identity.

$$\begin{array}{ccc}
\mathbb{Q}[G] & & 1_{\mathbb{Q}[G]} \\
\downarrow & \{e\} & \downarrow \\
\mathrm{End}_0 J_X & & 1_{\mathrm{End}_0 J_X} \\
\downarrow & \{\text{Kani-Rosen}\} & \downarrow \\
\text{Jacobian isogenies} & & J_X
\end{array}$$

An Example

Applying the map e and Kani-Rosen to

$$\varepsilon_{1_G} + 2\varepsilon_G = \varepsilon_{H_1} + \varepsilon_{H_2} + \varepsilon_{H_3}$$

gives

$$J_X \times J_{X/G}^2 \sim J_{X/H_1} \times J_{X/H_2} \times J_{X/H_3}.$$

An Example

Applying the map e and Kani-Rosen to

$$\varepsilon_{1_G} + 2\varepsilon_G = \varepsilon_{H_1} + \varepsilon_{H_2} + \varepsilon_{H_3}$$

gives

$$J_X \times J_{X/G}^2 \sim J_{X/H_1} \times J_{X/H_2} \times J_{X/H_3}.$$

Theorem (Kani and Rosen, '89)

Given a curve X, let $G \leq Aut(X)$ be a finite group with $H_i \leq G$ such that $G = H_1 \cup \cdots \cup H_m$ and $H_i \cap H_j = \{1_G\}$ 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 $h_i = |H_i|$.

An Example

Applying the map e and Kani-Rosen to

$$\varepsilon_{1_G} + 2\varepsilon_G = \varepsilon_{H_1} + \varepsilon_{H_2} + \varepsilon_{H_3}$$

gives

$$J_X \times J_{X/G}^2 \sim J_{X/H_1} \times J_{X/H_2} \times J_{X/H_3}.$$

Theorem (Kani and Rosen, '89)

Given a curve X, let $G \leq Aut(X)$ be a finite group with $H_i \leq G$ such that $G = H_1 \cup \cdots \cup H_m$ and $H_i \cap H_j = \{1_G\}$ 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 $h_i = |H_i|$.

Cyclic groups or quaternion group of order 8 (automorphism group of a genus 4 hyperelliptic curve) can't be written this way.

Recall

$$\mathbb{Q}[G] = \bigoplus_i M_{n_i}(\Delta_i) \qquad 1_{\mathbb{Q}[G]} = \sum_{i,j} \pi_{i,j}$$

Recall

$$\mathbb{Q}[G] = \bigoplus_i M_{n_i}(\Delta_i) \qquad 1_{\mathbb{Q}[G]} = \sum_{i,j} \pi_{i,j}$$

Applying the map e and Kani-Rosen to this idempotent relation gives

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

Recall

$$\mathbb{Q}[G] = \bigoplus_i M_{n_i}(\Delta_i) \qquad 1_{\mathbb{Q}[G]} = \sum_{i,j} \pi_{i,j}$$

Applying the map e and Kani-Rosen to this idempotent relation gives

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

What are these $e(\pi_{i,j})J_X$? For our motivational question, we want many elliptic curves as factors.

Suppose the quotient map from X to $Y = X/G$ is branched at s points with monodromy $g_1, \ldots, g_s \in G$.

$\chi_{\langle g_i \rangle}$ is the character of G which is induced from the trivial character of $\langle g_i \rangle$ and χ_{triv} is the trivial character of G.

Definition

A **Hurwitz character** of a group G is a character of the form:

$$\chi = 2\chi_{\mathrm{triv}} + 2\left(g_Y - 1\right)\chi_{\langle 1_G \rangle} + \sum_{i=1}^{s} \left(\chi_{\langle 1_G \rangle} - \chi_{\langle g_i \rangle}\right)$$

V is the representation associated to this character and the V_i (with associated character χ_i) are the irreducible $\mathbb{Q}$-representations.

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

and

$$\dim_{\mathbb{Q}}\pi_{i,j}V = \langle \chi_i, \chi \rangle$$

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

Recall: We want to find lots of isogenous elliptic curves.

Theorem (P., '07)

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

Key Ingredients in the Proof

We find an $n_i \times n_i$ matrix M of order 2 such that conjugating $\pi_{i,j}$ by M gives $\pi_{i,k}$.
Now since e is a homomorphism and M is, in particular, a unit, $e(M)$ is an automorphism of the Jacobian and we can use this to prove $e(\pi_{i,j})J_X \sim e(\pi_{i,k})J_X$.

This theorem suggests we should find curves of genus g whose automorphism groups have an $M_g(\Delta_i)$ somewhere in the Wedderburn decomposition or at least try to maximize t in $M_t(\Delta_i)$.

This theorem suggests we should find curves of genus g whose automorphism groups have an $M_g(\Delta_i)$ somewhere in the Wedderburn decomposition or at least try to maximize t in $M_t(\Delta_i)$.

Work of Magaard, Shaska, Shpectorov, and Völklein ('02) classifies all full automorphism groups of “large” curves up to genus 10.

Large in their paper means $|G| > 4(g-1)$. In particular X/G is genus 0 in these cases.

Data in their paper provides information about monodromy of the quotient maps as well as dimensions of the families of curves with each particular automorphism group.

Genus	Auto. Group	Dim.	Jacobian Decomposition
4	$(72, 40)$	0	$J_X \sim E^4$
5	$(160, 234)$	0	$J_X \sim E^5$
6	$(72, 15)$	0	$J_X \sim E^6$
7	$(504, 156)$	0	$J_X \sim E^7$
8	$(336, 208)$	0	$J_X \sim E^8$
9	$(192, 955)$	0	$J_X \sim E_1^3 \times E_2^6$
10	$(360, 118)$	0	$J_X \sim E^{10}$

Genus	Auto. Group	Dim.	Jacobian Decomposition
4	$(72, 40)$	0	$J_X \sim E^4$
5	$(160, 234)$	0	$J_X \sim E^5$
6	$(72, 15)$	0	$J_X \sim E^6$
7	$(504, 156)$	0	$J_X \sim E^7$
8	$(336, 208)$	0	$J_X \sim E^8$
9	$(192, 955)$	0	$J_X \sim E_1^3 \times E_2^6$
10	$(360, 118)$	0	$J_X \sim E^{10}$

The genus 7 curve is a Hurwitz curve called the Macbeath curve. Students of Macbeath showed by other methods that $J_X \sim E^7$.

	Auto.		Jacobian
Genus	Group	Dim.	Decomposition
4	$(72, 40)$	0	$J_X \sim E^4$
5	$(160, 234)$	0	$J_X \sim E^5$
6	$(72, 15)$	0	$J_X \sim E^6$
7	$(504, 156)$	0	$J_X \sim E^7$
8	$(336, 208)$	0	$J_X \sim E^8$
9	$(192, 955)$	0	$J_X \sim E_1^3 \times E_2^6$
10	$(360, 118)$	0	$J_X \sim E^{10}$

Work of Brandt and Stichtenoth ('86) and Shaska ('03) completely classifies all possible full automorphism groups of hyperelliptic curves over an algebraically closed field of characteristic zero for any genus.

Let G is the automorphism group of a hyperelliptic curve X and ω the hyperelliptic involution. The reduced automorphism group ($G/\langle\omega\rangle$) must be one of D_n, C_n, A_4, S_4, A_5.

For any genus g there is at most one family of hyperelliptic curves of that genus with reduced automorphism group each of A_4, S_4, or A_5. This existence is completely determined by the residue class of g modulo 6, 12, and 30, respectively.

Genus	Automorp. Group	Dimen.	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	$A_2 \times E^3$
	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	$E \times A_2^3$
8	$\mathrm{SL}_2(3)$	1	$A_{2,1}^2 \times A_{2,2}^2$
	W_3	0	$A_2^2 \times E^4$
9	$A_4 \times C_2$	1	$A_2^3 \times E^3$
	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	$A_2^2 \times A_3^2$

Genus	Automorp. Group	Dimen.	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	$A_2 \times E^3$
	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	$E \times A_2^3$
8	$\mathrm{SL}_2(3)$	1	$A_{2,1}^2 \times A_{2,2}^2$
	W_3	0	$A_2^2 \times E^4$
9	$A_4 \times C_2$	1	$A_2^3 \times E^3$
	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	$A_2^2 \times A_3^2$

The End