Determining whether an isogeny class contains a Jacobian.
Part II: Prospects and questions

Everett W. Howe
Unaffiliated mathematician

Curves over Finite Fields: Past, Present, and Future
Centro de Ciencias de Benasque Pedro Pascual (virtual)
25–29 May 2021

Email: however@alumni.caltech.edu  Web site: ewhowe.com  Twitter: @howe
I have tried to come up with a variety of questions, at least some of which are approachable, that might shed light on the problem of determining whether there is a Jacobian in an isogeny class.

I have also included a question about finding large, easy-to-analyze families of curves that could help produce examples of various sorts.
At my talk yesterday, Nils Bruin asked:
Is there any intuition on whether there is a finite set of methods/criteria that can give necessary and sufficient conditions?

If the question is about principally-polarized varieties in isogeny classes:
I think there is a chance. Evidence? The problem is completely answered for ordinary isogeny classes.

If the question is about Jacobians in isogeny classes:
I am very doubtful. But one never knows!
If there is a simple test for Jacobians in an isogeny class, here is an easy goal:

**Challenge**

For some $q \geq 127$, find an absolutely irreducible ordinary 4-dimensional isogeny class over $\mathbb{F}_q$ with Weil polynomial $f$ such that

- the number field defined by $f$ contains no roots of unity other than $\pm 1$ and
- the number field is ramified over its maximal real subfield,

and determine whether or not this isogeny class contains a Jacobian.

But! No fair cheating...
What counts as cheating?

First, remember that “cheating” sometimes is another name for “seeing a clever way around the problem,” so please go ahead and be clever!

But these ideas seem like they would be missing the spirit of the challenge

First too-clever idea:
- Choose a genus-4 curve over $\mathbb{F}_q$ and compute its Weil polynomial $f$.
- If $f$ satisfies the requirements, chose that for your challenge $f$!
- Answer with confidence that your isogeny class contains a Jacobian.

Second too-clever idea:
- Choose genus-4 $C/\mathbb{F}_q$ with $\text{Aut } C_{\mathbb{F}_q}$ trivial, and compute its Weil polynomial $f_0$.
- Repeat until $f_0$ satisfies requirements, and isogeny class has unique PPAV.
- Take $f$ to be $f_0(-x)$, corresponding to the quadratic twist of $\text{Jac } C$.
- Answer with confidence that your isogeny class does not contain a Jacobian.
If you have trouble convincing your friends that you did not cheat, feel free to focus on the isogeny class over $\mathbb{F}_{127}$ given by the real Weil polynomial

$$x^4 - 4x^3 - 484x^2 + 2537x + 3297.$$ 

This has the nice property that $\mathbb{Z}[F, V]$ is a maximal order, and I promise I chose it by picking coefficients at random from a reasonable region inside the parameter space of Weil polynomials.
Principally polarized varieties in non-ordinary isogeny classes

Challenge
Consider one of the equivalences of categories that is not Deligne’s:

- Centeleghhe/Stix (2015): Abelian varieties over $\mathbb{F}_p$ with no real Frobenius eigenvalues
- Oswal/Shankar (2020): Almost-ordinary abelian varieties over $\mathbb{F}_q$

Find an efficient procedure to decide whether an isogeny class of such varieties contains a principally polarized variety.

Bergström/Karemaker/Marseglia (2021) have already done considerable work on this, so don’t reinvent the wheel.
You say you want a challenge?

**Challenge**

Construct a new equivalence of categories from some collection of non-ordinary abelian varieties to some category of modules with extra structure.

Possible hint? Thirty years ago Milne opined that representations of gerbes might be useful for this.
When searching for examples of curves with many points, it helps to have some families that are easy to control.

**Example: Genus-4 curves with $V_4$ action**

If $D/F_q$ has genus 4 and if $V_4 \subseteq \text{Aut } D$, there are three possibilities:

- $V_4$ contains a hyperelliptic involution.
- The $V_4$ involutions are non-hyperelliptic, and $D/V_4 \cong \mathbb{P}^1$.
- The $V_4$ involutions are non-hyperelliptic, and $D/V_4$ has genus 1.
\( V_4 \) contains a hyperelliptic involution

In this arrangement, \( D/V_4 \cong \mathbb{P}^1 \), two of the intermediate curves have genus 2, and the third is again a \( \mathbb{P}^1 \).

The Jacobian of \( D \) decomposes: \( \text{Jac} \, D \sim \text{Jac} \, C_1 \times \text{Jac} \, C_2 \).

The ramification points of \( C_1 \to \mathbb{P}^1 \) and \( C_2 \to \mathbb{P}^1 \) and \( \mathbb{P}^1 \to \mathbb{P}^1 \) have to line up to make this work:

\[
\begin{align*}
C_1 &: \quad \circ \circ \circ \circ \circ \circ \\
C_2 &: \quad \circ \circ \circ \circ \circ \circ \circ \\
\mathbb{P}^1 &: \quad \circ \circ
\end{align*}
\]

If you start with a fixed \( C_1 \), you have one parameter to play with. There are \( O(q^3) \) possible \( C_2 \)'s, and \( O(q^{3/2}) \) isogeny classes of \( C_2 \)'s.
The $V_4$ involutions are non-hyperelliptic, and $D/V_4 \cong \mathbb{P}^1$

In this arrangement, $D/V_4 \cong \mathbb{P}^1$, two of the intermediate curves have genus 1, and the third has genus 2.

The Jacobian of $D$ decomposes: $\text{Jac } D \sim \text{Jac } C \times E_1 \times E_2$.

The ramification points of $E_1 \to \mathbb{P}^1$ and $E_2 \to \mathbb{P}^1$ and $C \to \mathbb{P}^1$ have to line up to make this work:

- $E_1$:
  - $\circ \circ \circ \circ \circ$

- $E_2$:
  - $\circ \circ \circ \circ \circ$

- $C$:
  - $\circ \circ \circ \circ \circ \circ \circ$

If you start with a fixed $C$, you have one parameter to play with. There are $O(q^2)$ possible pairs $(E_1, E_2)$, and $O(q)$ possible pairs of isogeny classes for the $E_i$. 
The $V_4$ involutions are non-hyperelliptic, and $D/V_4$ has genus 1.

In this arrangement, $D/V_4$ has genus 1 and the three intermediate curves have genus 2.

Each $\text{Jac } C_i$ is isogenous to $E \times E_i$ for an elliptic curve $E_i$.

The Jacobian of $D$ decomposes: $\text{Jac } D \sim E \times E_1 \times E_2 \times E_3$.

The ramification points of $C_i \to E$ have to line up:

- $C_1$: \( \circ \circ \)
- $C_2$: \( \circ \circ \circ \)
- $C_3$: \( \circ \circ \circ \)

If you start with a fixed $E$, $E_1$, and $E_2$, you have no parameters left to play with. There are $O(q)$ possible $E_3$, and $O(\sqrt{q})$ possible isogeny classes of $E_3$. 
Utility of the constructions

<table>
<thead>
<tr>
<th>First construction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not very much flexibility.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Second construction</th>
</tr>
</thead>
<tbody>
<tr>
<td>A little more freedom...</td>
</tr>
<tr>
<td>- In [Howe 2016] this allowed for quickly constructing genus-4 curves with small defect. Heuristically, for large $q$ should be able to get defect $\leq 4$.</td>
</tr>
<tr>
<td>- In [Kudo/Harashita/Howe 2020] this allowed for quickly constructing superspecial curves.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Third construction</th>
</tr>
</thead>
<tbody>
<tr>
<td>The third construction also has much freedom, and always gives completely split Jacobians. Note: Over the algebraic closure, if we take $E$ to have $j = 0$, we can take $E_1 \cong E_2 \cong E_3$ to be an arbitrary elliptic curve.</td>
</tr>
</tbody>
</table>
Constructions for higher genus

Challenge

Find similar constructions for larger genus —
That is, constructions that let us quickly build up genus-\(g\) curves from lower-genus curves, with as much freedom as possible.
Questions and further challenges

Any further challenges to propose?

Questions about yesterday’s talk, or today’s?

Now is the time for them.
Once again, thanks

Thank you to Serre . . .

Thank you to the organizers . . .

Thank you to those present here for listening . . .

Thank you to all who have contributed to the beautiful results in this field . . .

And thank you to those who will contribute in the future.
Extra bonus slides!
(Concerning the third construction.)
The third construction, over the algebraic closure

If $E$ has genus 1 and the $C_i$ have genus 2, then $D$ has genus 4.

Each $C_i$ has Jacobian 2-power isogenous to $E \times E_i$ for an elliptic curve $E_i$.

The Jacobian of $D$ decomposes: $\text{Jac} \ D \sim E \times E_1 \times E_2 \times E_3$.

The ramification points of $C_i \to E$ have to line up:

$C_1 : \quad \circ \quad \circ$

$C_2 : \quad \circ \quad \circ \quad \circ$

$C_3 : \quad \circ \quad \circ \quad \circ$
An invariant of genus-2 double covers of $E$

Let $E$ be given by $y^2 = x(x - 1)(x - \lambda)$.

Every genus-2 double cover $C \to E$ can be written $z^2 = f$, where

$$\text{div } f = [Q] + [R] - 2[S],$$

with $2S = Q + R$ on $E$.

By translating by $-S$, we get an isomorphic cover where now


The orbit of $P$ under $\text{Aut } E$ is an invariant of $C \to E$. When $\text{Aut } E = \{ \pm 1 \}$, this means that for a fixed model of $E$ the $x$-coordinate of $P$ is an invariant of the cover.
Suppose $F$ is given by $y^2 = x(x - 1)(x - \mu)$.

Let $\psi : E[2] \to F[2]$ be the isomorphism given by

$$(0, 0) \mapsto (0, 0), \quad (1, 0) \mapsto (1, 0), \quad (\lambda, 0) \mapsto (\mu, 0).$$

The quotient of $A = E \times F$ by the graph of $\psi$ is a principally polarized surface.

If $\lambda \neq \mu$, this surface is the Jacobian of a curve $C$ with a degree-2 map $C \to E$.

**Lemma**

*The invariant of the cover $C \to E$ is $\lambda(1 - \mu)/(\lambda - \mu)$.***
Lining up ramification points

Given three covers $C_i \to E$ obtained in this way, when can we line their ramification points up to get a genus-4 curve $D$?

We can express the answer in terms of the invariants $x_i$, or the points $P_i$ (which are determined only up to sign):

**Theorem**

The three covers can be lined up correctly if and only if we can choose signs so that $\pm P_1 \pm P_2 \pm P_3 = O$ on $E$.

Equivalently, we can line the three covers up correctly if $S(x_1, x_2, x_3) = 0$, where $S$ is the third summation polynomial for (the given model of) $E$. 

A polynomial relation

We have formulas for the $x_i$ in terms of $\lambda$ and the $\mu_i$.

We know the summation polynomial for $E$.

So we obtain:

Corollary

The three covers can be lined up correctly if and only if

$$\lambda^4 + (-2s_1 + 2s_2 - 4s_3)\lambda^3 + (s_1^2 - 2s_1s_2 + s_2^2 + 6s_3)\lambda^2 + (2s_1s_3 - 2s_2s_3 - 4s_3)\lambda + s_3^2 = 0,$$

where the $s_i$ are the symmetric functions in the $\mu_j$. 
For a prime $p$, we can list the supersingular $\lambda$-invariants. There are $(p - 1)/2$ of them, and they are all elements of $\mathbb{F}_{p^2}$.

We can enumerate all quadruples $(\lambda, \mu_1, \mu_2, \mu_3)$ with $\lambda \neq \mu_i$ for all $i$, and see whether the polynomial in the Corollary is satisfied.

Naïvely, we expect to obtain $\Theta(p^2)$ quadruples that work, and this is borne out by computational evidence. We find examples for all $p > 13$ that we have tried.

**Question**

For $p > 13$, are there always supersingular $\lambda$-invariants that satisfy the Corollary? If so, then we have shown that there are superspecial genus-4 curves for all $p > 7$. 
A fortuitous example

Suppose we take a curve $F: y^2 = x(x - 1)(x - \mu)$, and take

$$
\begin{align*}
\mu_1 &= \mu, \\
\mu_2 &= \frac{1}{1 - \mu}, \\
\mu_3 &= \frac{\mu}{\mu - 1},
\end{align*}
$$

so that the elliptic curves $E_1, E_2, E_3$ are all isomorphic to $F$ (but the isomorphisms $\psi_i: E[2] \to F[2]$ are all different).

Then the polynomial in the Corollary simplifies — dramatically — to become

$$(\lambda^2 - \lambda + 1)^2.$$  

The corresponding values of $\lambda$ give us the elliptic curve with $j = 0$.

**Corollary**

*Let $E$ be the elliptic curve with $j$-invariant 0, and let $F$ be any other elliptic curve. Then there is a genus-4 curve $X$ whose Jacobian is 2-power isogenous to $E \times F^3$.***