Abelian Varieties not Isogenous to a Hyperelliptic Jacobian

Ravi Donepudi

University of Illinois at Urbana-Champaign

January 16, 2020

Joint work with
Edgar Costa (MIT), Ravi Fernando (UC-Berkeley),
Valentijn Karemaker (Utrecht), Caleb Springer (Penn State).
Mckenzie West (UW-Eau Claire)

Elliptic Curves

- Let p be an odd prime and $q = p^n$. Let k be the field with q elements.

Definition

An elliptic curve over k is a smooth, projective, geometrically integral curve of genus 1 with a chosen k-rational point on it.

- Elliptic curves are nice because they simultaneously have the structure of an algebraic curve and an abelian group in a compatible way.

Curves of genus g and Abelian varieties

- Two ways to generalize elliptic curves:
  - Curves of genus g (No group structure unless $g = 1$)
  - Abelian varieties (AVs) of dimension g (Not curves unless $g = 1$)
- How are these two generalizations related?

The Jacobian

To a curve C of genus g, we can canonically attach an AV of dimension g containing the curve. This is always canonically principally polarized.

- The space $\mathcal{M}_g$ of genus g curves has dimension $3g - 3$
- The space A_g of dimension g PPAVs has dimension $\frac{g(g+1)}{2}$.
- The Jacobian construction yields an injective map $\mathcal{M}_g \to A_g$
- J is generally not a surjection (even for $g = 2$)
- Many attempts to try and understand the image.

Zeta functions of curves

- Given a "nice" curve C of genus g defined over $\mathbb{F}_q$, we can define the zeta function

$$Z_C(T) = \exp\left(\sum_{k\geq 0} \#C(F_{q^k})\frac{X^k}{k}\right)$$

- The Riemann Hypothesis for curves (Proven!) implies that

$$Z_C(T) = \frac{P_C(T)}{(1-T)(1-qT)}$$

where

$$P_C(T) = \det(1 - T\,\mathrm{Frob})$$

all of whose roots have absolute value $q^{-1/2}$.

Weil q-polynomials

- Let A be an abelian variety over $\mathbb{F}_q$.
- Two abelian varieties are isogenous iff the characteristic polynomials of Frobenius match.
- This characteristic polynomial is called the Weil-q polynomial of the isogeny class.

Main question

Given a Weil q-polynomial, can we determine if it corresponds to the Jacobian of a curve?

Proven cases

Main question

Given a Weil q-polynomial, can we determine if it corresponds to the Jacobian of a curve?

- If $g = 1$, every abelian variety is an elliptic curve.
- If $g = 2$, a general Weil-q polynomial is

$$x^4 + a_1 x + a_2 x^2 + q a_1 + q^2.$$

Howe-Nart-Ritzenthaler

There exist elementary and explicit necessary and sufficient conditions on the integers a_1, a_2 for the above polynomial to be realized by a Jacobian.

Key ingredient

Every genus 2 curve is hyperelliptic, so has an order 2 automorphism!

The data for $g = 3, q = 3$

Sutherland enumerated both the set of isogeny classes of abelian varieties and curves of genus g for small p, g.

- For $q = 3$, there are 677 Weil q-polynomials
- For $q = 3$, there are 479 that arise from curves.

Question

What is wrong with the remaining 198 polynomials?

- Of the 677 polynomials, 24 would yield a generating function with negative coefficients.

Question

What is wrong with the remaining 174 polynomials?

Curves of genus 3

Curves of genus 3 come in two flavors:

- Hyperelliptic curves: Curves with affine model

$$y^2 = f(x) \text{ with } \deg(f) = 2g + 1 \text{ or } 2g + 2.$$

- Smooth plane quartics: Smooth curves with projective model

$$F(x, y, z) = 0 \text{ for } F \text{ homogenous of degree 4}$$

The former always have an involution $(x, y) \to (x, -y)$ but the latter generically have no non-trivial automorphisms.
So we study when a Weil-q polynomial cannot arise from the Jacobian of a hyperelliptic curve.

Nonexistence result

Theorem (CDFKSW)

Let q be an odd prime power. The isogeny classes of three-dimensional abelian varieties corresponding to Weil q-polynomials of the form

$$x^6 + a_1x^5 + a_2x^4 + a_3x^3 + qa_2x^2 + q^2a_1x + q^3$$

with $a_2 \equiv 0 \pmod 2$ and $a_3 \equiv 1 \pmod 2$ do not contain the Jacobian of any hyperelliptic curve over $\mathbb{F}_q$.

Theorem (CDFKSW)

As $q \to \infty$ along odd prime powers, at least $\frac{1}{4}$ of isogeny classes of of abelian varieties of dimension 3 over $\mathbb{F}_q$ do not contain a hyperelliptic Jacobian.

Toy Example

How does the form of an (even) hyperelliptic curve affect the number of points over field extensions?

- Points come in pairs $(x, y), (x, -y)$, unless $y = 0$.
- An irreducible polynomial $f \in \mathbb{F}_q[x]$ acquires (all) roots in $\mathbb{F}_{q^k}$ if and only if $k | \deg(f)$.

Example: Let $k = \mathbb{F}_q$ and consider the following curve :

- C is defined by $y^2 = f_1(x)f_2(x)$, where f_1, f_2 are irreducible of degrees 3 and 5 respectively.
- $\#C(\mathbb{F}_{q^k})$ is even unless
  - $3|k$ and $5 \nmid k$
  - $3 \nmid k$ and $5|k$

This is generalizable to any other factorization of of $f(x)$, where $y^2 = f(x)$

General Approach

- Let $C/\mathbb{F}_q$ a genus g hyperelliptic curve and $\pi : C \to \mathbb{P}^1$ the canonical (degree 2) map.
- Let W be the set of $2g+2$ points of C where π ramifies.
- The action of the Frobenius on W partitions it into orbits W_i, each of size d_i.

Key Proposition

Let C be a hyperelliptic curve of genus g defined over $\mathbb{F}_q$ and $\{d_i\}_{i=1}^r$ it's corresponding partition. Then the characteristic polynomial of Frobenius acting on Jacobian is congruent to

$$\Big(\prod_{i=1}^{r} t^{d_i} - 1\Big)/(t-1)^2 \pmod 2$$

Procedure for $g = 3$

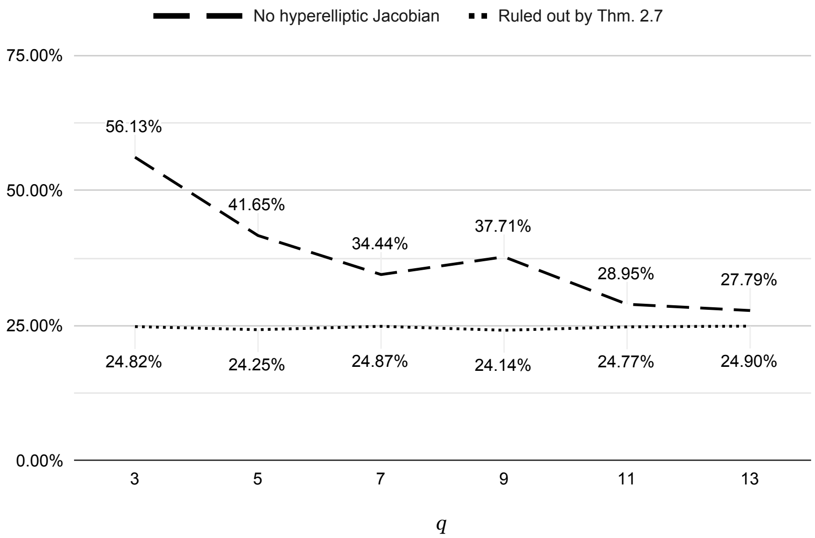
Let $g = 3$.

$(a_1, a_2, a_3) \pmod 2$	Partition of $2g + 2 = 8$
$(0, 1, 1)$	$\{3, 5\}$
$(1, 1, 0)$	$\{1, 1, 1, 1, 1, 3\}$, $\{1, 1, 1, 2, 3\}$, $\{1, 2, 2, 3\}$, $\{1, 3, 4\}$
$(1, 0, 0)$	$\{1, 1, 1, 5\}$, $\{1, 2, 5\}$
$(0, 0, 0)$	$\{1, 1, 3, 3\}$, $\{1, 1, 6\}$, $\{2, 3, 3\}$, $\{2, 6\}$
$(0, 1, 0)$	$\{1, 1, 1, 1, 1, 1, 1, 1\}$, $\{1, 1, 1, 1, 1, 1, 2\}$, $\{1, 1, 1, 1, 2, 2\}$, $\{1, 1, 1, 1, 4\}$, $\{1, 1, 2, 2, 2\}$, $\{1, 1, 2, 4\}$, $\{2, 2, 2, 2\}$, $\{2, 2, 4\}$, $\{4, 4\}$, $\{8\}$
$(1, 1, 1)$	$\{1, 7\}$

Table: Weil coefficients modulo 2 and corresponding partitions for threefolds.

The patterns $(1, 0, 1)$ and $(0, 0, 1)$ do not appear.

Statistics for $g = 3$



The q-limit

Theorem (CDFKSW)

Let $h(q,g)$ be the proportion of isogeny classes of g-dimensional abelian varieties over $\mathbb{F}_q$ which contain a hyperelliptic Jacobian.
For any $g \geq 2$ we have

$$\limsup_{q\to\infty} h(q,g) \leq \frac{Q(2g+2)}{2^g},$$

where $Q(2g+2)$ is the number of partitions of $2g+2$ into distinct parts.
In particular,

$$\lim_{g\to\infty} \limsup_{q\to\infty} h(q,g) = 0.$$

In both q-limits, the integer q ranges over odd prime powers.

Asymptotic result on Weil-q polynomials

Theorem (Holden+ϵ)

Fix a positve integer D and elements $b_1, b_2 \cdots, b_g \subset \mathbb{Z}/D\mathbb{Z}$. As $q \to \infty$ along odd prime powers, the proportion of isogeny classes of g-dimensional abelian varieties corresponding to Weil q-polynomials

$$x^{2g} + a_1 x^{2g-1} + \cdots q^{g-1} a_1 x + q^g$$

with $a_i \equiv b_i \pmod{D}$ approaches

$$\frac{1}{D^g}$$

.

Congruence restrictions on coefficients are "asymptotically independent".

Summary

- We explain why certain Weil-q polynomials do not arise as hyperelliptic Jacobians.
- Hyperelliptic curves have an involution whose effect on the point counts and zeta function is easily examinable.
- In the large q limit, at least 25% of all isogeny classes of abelian varieties of dimension 3 over $\mathbb{F}_q$ do not contain a hyperelliptic Jacobian.
- As g grows, hyperelliptic Jacobians occupy only a rapidly diminishing proportion of all isogeny classes.
- Lower bounds? Plane quartics? Much remains to be explored!