ICERM: Cyclic covers with isogenous Jacobians

Vishal Arul, Jeremy Booher, Steven Groen, Everett W. Howe,
Wanlin Li, Vlad Matei, Rachel Pries, Caleb Springer

June 2020

Set-up

- Z_s is a genus 2 curve over $\mathbb{F}_q$ with $D_4 \subseteq \mathrm{Aut}(Z_s)$:
$$Z_s : y^2 = r(x^2+1)(x^4+sx^2+1),$$
where either $r = 1$ or r is a fixed nonsquare.
- This parametrizes the Moonen family M[4].
- $\mathrm{Jac}\, Z_s \sim E_s^2$, where E_s is the elliptic curve
$$E_s : y^2 = r(x+1)(x^2+sx+1).$$
- Consider the degree 16 unramified cover given by the pullback
$$\begin{array}{ccc} Z_{s_i}^{(2)} & \longrightarrow & \mathrm{Jac}\, Z_{s_i} \\ \downarrow & & \downarrow 2 \\ Z_{s_i} & \longrightarrow & \mathrm{Jac}\, Z_{s_i} \end{array}$$
- We call Z_{s_1} and Z_{s_2} *doubly isogenous* if $\mathrm{Jac}\, Z_{s_1} \sim \mathrm{Jac}\, Z_{s_2}$ and $\mathrm{Jac}\, Z_{s_1}^{(2)} \sim \mathrm{Jac}\, Z_{s_2}^{(2)}$.

Lemma: Up to isogeny, Jac $Z_{s_i}^{(2)}$ decomposes into 17 elliptic curves, including two copies of E_s. The 15 others are in six orbits under the D_4-action; five of these orbits depend on s.

Question: Describe the heuristics of doubly isogenous curves which are not Galois conjugate.

(Naive) heuristics

What one would roughly expect:

- $\#\{\text{curves } Z_s/\mathbb{F}_q\} \sim q$.
- Isogeny classes have size roughly $\sqrt{q}$.
- $\#\{\text{pairs } (Z_{s_1}, Z_{s_2})\} \sim q^2/2$.
- $\#\{\text{pairs } (Z_{s_1}, Z_{s_2}) \text{ isogenous Jacobians}\} \sim C_1 q^{3/2}$.
- Question: what is C_1?
- There are five additional conditions to be doubly isogenous coming from the five non-constant orbits of 2-torsion points so $\#\{\text{pairs } (Z_{s_1}, Z_{s_2}) \text{ doubly isogenous}\} \sim C_2 q^{-1}$.
- Or can we hope for more?

Data

Curves with isogenous Jacobians:

- For many primes p, $\#\{\text{pairs } (Z_{s_1}, Z_{s_2}) \text{ isogenous}\} \sim 0.41q^{3/2}$.
- The constant $C_1 \approx 0.41$ is subtle to explain, since we lack information about the distribution of isogeny class sizes conditional on being in this family.

Doubly isogenous curves:

- We found more doubly isogeny curves than expected, indicating that more collisions occur than expected for isogeny classes.
- We have an explanation for this.

A family of coincidences

A one parameter family of pairs.

- We consider pairs (Z_s, Z_{-s}).
- In that case, three of the six orbits already match up (coincidentally).
- Two other orbits match up simultaneously.

Heuristics:

- $\#\{\text{pairs } (Z_s, Z_{-s})\} \sim q$.
- $\#\{\text{pairs } (Z_s, Z_{-s}) \text{ isogenous Jacobians}\} \sim q^{1/2}$.
- $\#\{\text{pairs } (Z_s, Z_{-s}) \text{ doubly isogenous}\} \sim q^{-1/2}$.

Discussion

Topics to investigate

- Explain the constant C_1?
- Could the collisions in $\mathbb{F}_q$ come from collisions in characteristic 0?
- There are additional families of collisions which appear in positive characteristic; we have found two extra genus 1 families, and there might possibly be more. We think that the majority of the collisions might come from positive characteristic families of collisions rather than characteristic 0 collisions.
- $\sim q$ collisions are found if we pull back along multiplication by $1 \pm i$ instead of multiplication by 2, this might be more fruitful.
- Do similar phenomena occur for other Moonen families?