Combinatorial Approaches to Finite Field Geometry

Ravi Kiran Donepudi

University of Illinois at Urbana-Champaign

November 3 , 2019

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 1

An elliptic curve over k is a smooth projective geometrically connected curve of genus 1 with a choice of k-rational point.

Definition 2

An elliptic curve over k "is" the variety defined by $y^2 = f(x)$, where $f(x)$ is a cubic, squarefree polynomial in $k[x]$.

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

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.

- The space $\mathcal{M}_g$ of genus g curves has dimension $3g - 3$
- The space A_g of g dimensional (PP)[1] AVs has dimension $\frac{g(g+1)}{2}$.
- The Jacobian construction yields an injective map:

$$J : \mathcal{M}_g \to A_g$$

- J is generally not a surjection, (even for $g = 2$)

[1] Principally Polarized

Zeta functions of curves

- Given a 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
$$P_C(T) = \prod_{i=1}^{2g}(1-\omega_i T) \in \mathbb{Z}[T]$$
and
$$|\omega_i| = q^{1/2} \text{ for all } 1 \leq i \leq 2g$$

Weil q-polynomials

There is a canonical bijection between the following sets:

- AVs of dimension g defined over $\mathbb{F}_q$, up to isogeny,
- Monic integer polynomials of degree $2g$ all of whose roots have absolute value $q^{\frac{1}{2}}$. (Weil q-polynomials)

For the Jacobian of a curve C of genus g, under this correspondance, the associated polynomial is simply

$$T^{2g} P_C(\frac{q}{T}).$$

Main question

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

When is something that looks like a generating function actually counting points on 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 give elementary necessary and sufficient conditions on the integers a_1, a_2 for the polynomial to be realized by a Jacobian.

Key Point

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:

$$x^6 + a_1 x^5 + a_2 x^4 + a_3 x^3 + q a_2 x^2 + q^2 a_1 x + q^3$$

  where $a_i \in \mathbb{Z}$, and all roots have absolute value $q^{\frac{1}{2}}$
- For $q = 3$, there are 479 generating functions of all curves of genus 3.
- Of the 677 polynomials, 24 would yield a generating function with negative coefficients.

Sutherland's 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

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

- 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.

Main Idea

How does the form of the hyperelliptic curve affect the number of points over field extensions?

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

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

- Example 1: C_i is defined by $y^2 = f(x)$ where $f(x) \in k[x]$ is irreducible of degree 8.
- $\#C_1(\mathbb{F}_{q^k})$ is always even.
- Example 2: C_i is defined by $y^2 = f(x)$ where $f(x) = p(x)q(x) \in k[x]$, where p, q are irreducible of degrees 3 and 5 respectively.
- $\#C_2(\mathbb{F}_{q^k})$ is even unless
    - $3 \mid k$ and $5 \nmid k$
    - $3 \nmid k$ and $5 \mid k$

Main Idea

- Assume the curve C has a model of the form $y^2 = f(x)$ and $deg(f) = 8$. No loss of generality for $q \geq 8$.
- The degrees of the irreducible factors of f can be encoded as a partition of 8.
- For each partition, we can study the possible binary sequences appearing as
$$\#C(\mathbb{F}_{q^k}) \pmod 2$$
- The set $C(\mathbb{F}_{q^k})$ also has an action of $\mathrm{Gal}(\mathbb{F}_{q^k}/\mathbb{F}_q) \simeq \mathbb{Z}/k\mathbb{Z}$.
- Studying the joint $\mathbb{Z}/k\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$-action places further restrictions on the sequence.

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 $\mathbb{F}_q$.

Asymptotic result on Weil-q polynomials

Theorem (Holden)

Fix a positve integer D and subsets $S_1, S_2 \cdots, S_g \subset \mathbb{Z}/D\mathbb{Z}$. As $q \to \infty$ along odd prime powers, the proportion of isogeny classes of g abelian varieties corresponding to Weil q-polynomials

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

with $a_i \in S_i$ approaches

$$\prod_{i=1}^{g} \frac{|S_i|}{D}$$

.

Asymptotic non-existence result

Applying Holden's result and using our congruence restriction, we get

Corollary (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.

Summary

- Our main goal is to determine which Weil-q polynomials describe point counts of genus 3 curves.
- Hyperelliptic curves have an involution whose effect on the point counts is easily examinable.
- We found congruence conditions on $a_1, a_2 \pmod 2$ for which

$$x^6 + a_1x^5 + a_2x^4 + a_3x^3 + qa_2x^4 + qa_1x^5 + q^3$$

  does not arise from a hyperelliptic curve.
- We use geometry of numbers to show that these congruence conditions are independant of each other.
- Thus, 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.