Deducing information about a curve over a finite field from its Weil polynomial

Everett W. Howe

Unaffiliated mathematician, San Diego, California

VaNTAGe Seminar
1 March 2022
(corrected slides)

Email: however@alumni.caltech.edu Web site: ewhowe.com Twitter: @howe

Land acknowledgement

As we work on our mathematics, it is important to remember:

- We are human beings, connected to one another.
- What we do, and how we do it, affects society.

For many of us, even our *location* connects us to ongoing injustice.

- I am giving this talk on land that is unceded territory of the Kumeyaay people.
- For more than 10,000 years this land has been — and continues to be — their home.
- I recognize the violent history of colonization in California, and honor the legacy of the continuing presence of the Kumeyaay Nation.

Visit https://native-land.ca to learn about the land where you live and work.

Where to find out more

This talk is based on my paper
"Deducing information about curves over finite fields from their Weil polynomials."

This is available at arXiv:2110.04221.

Eventually (?) part of the proceedings volume of the 2021 conference *Curves over finite fields: Past, present, and future*, which celebrated the publication of the notes for Serre's 1985 Harvard course on curves with many points.

In particular: further details, and all references, can be found there.

Motivation

Sometimes you want to know:

Is there a genus-g curve over a finite field $\mathbb{F}_q$ with certain properties?

For example: many points, or no points, or large gonality, or...

If there does exist such a curve, can you find an example?

Sometimes, the properties you are interested in tell you something about the number of points on the curve...

...possibly over several extensions of the base field.

Weil polynomials of abelian varieties

A — a g-dimensional abelian variety over a finite field $\mathbb{F}_q$

f — the characteristic polynomial of the Frobenius endomorphism on A

Properties of f

- Monic element of $\mathbb{Z}[x]$ of degree $2g$
- All roots of f in $\mathbb{C}$ have magnitude $\sqrt{q}$, all real roots have even multiplicity
- Can be written $f = x^g h(x + q/x)$ for a polynomial h:
  - h is monic element of $\mathbb{Z}[x]$ of degree g
  - All roots of h are real, and lie in $[-2\sqrt{q}, 2\sqrt{q}]$

We call f the *Weil polynomial* of A, and h the *real Weil polynomial* of A.

Define the Weil polynomial of a curve to be the Weil polynomial of its Jacobian.

Weil polynomials and numbers of points

Let f be the Weil polynomial of a genus-g curve $C/\mathbb{F}_q$, with roots $\pi_1, \ldots, \pi_{2g}$ in $\mathbb{C}$.

We have $\#C(\mathbb{F}_{q^n}) = q^n + 1 - \sum \pi_i^n$.

We also have $\#C(\mathbb{F}_{q^n}) = \sum_{d|n} d \cdot (\text{number of places of degree } d)$.

Möbius inversion gives:
$a_n(C) := (\text{number of places of degree } n \text{ on } C) = (1/n) \sum_{d|n} \mu(n/d) \cdot \#C(\mathbb{F}_{q^d})$

Basic facts

The Weil polynomial determines the number of degree-n places on C.

The Weil polynomial is determined by $(a_1(C), \ldots, a_g(C))$.

Weil polynomials, isogeny classes, and Jacobians

Theorem (Tate 1966)

Two abelian varieties over a finite field are isogenous if and only if they have the same Weil polynomial.

Motivating problems, rephrased

1. Given the Weil polynomial of an isogeny class of abelian varieties over $\mathbb{F}_q$, determine whether there's a curve whose Jacobian lies in the isogeny class.
2. Determine properties of the hypothetical curve that can help you construct it.

First part of the talk: Conditions that show there is no Jacobian in an isogeny class.

Second part of the talk: Properties that can help you construct a curve.

Part I: Showing an isogeny class contains no Jacobian

Principal polarizations of abelian varieties and Jacobians

~~Definition~~ Vague description:

A *principal polarization* of an abelian variety A is an isomorphism $\lambda\colon A \to \widehat{A}$ from A to its dual variety $\widehat{A}$ satisfying symmetry and positivity conditions:

- λ is equal to its own dual under the canonical isomorphism $A \cong \widehat{\widehat{A}}$, and
- λ "comes from" an ample invertible sheaf.

Fact

The Jacobian variety of a curve has a canonical principal polarization.

Consequence

An isogeny class with no principally polarized varieties also has no Jacobians.

Most isogeny classes contain principally polarized varieties

Let f be a Weil polynomial of an isogeny class $\mathcal{C}$ of simple varieties over $\mathbb{F}_q$.
Then $f = g^e$ for some irreducible g. Let K be the number field defined by g.
K is either real or CM. Let $\pi \in K$ be a root of g, and let $\overline{\pi}$ be its complex conjugate.

Theorem (H. 1995, H. 1996)

1. *If K is totally real then $\mathcal{C}$ contains a PPAV.*
2. *Suppose K is CM, with real subfield K^+. If K/K^+ is ramified at a finite prime, or if $\pi - \overline{\pi}$ is divisible by a prime of K inert in K/K^+, then $\mathcal{C}$ contains a PPAV.*
3. *Suppose the middle coefficient c of f is coprime to q, and that $\mathcal{C}$ does not satisfy the conditions in* (2)*. Then there is an integer $s > 0$ with $N_{K/\mathbb{Q}}(\pi - \overline{\pi}) = s^2$, and $\mathcal{C}$ contains a PPAV if and only if $c \equiv s \bmod m$, where m is the prime divisor of q if q is odd, and $m = 4$ if q is even.*

Most isogeny classes contain a PPAV, but not all

Corollary (H. 1996)

Every simple odd-dimensional isogeny class over a finite field contains a PPAV.

(Class field theory: if K is CM of degree 2·odd, K/K^+ is ramified at a finite prime.)

Example

Let $f = x^8 + 13x^7 + 90x^6 + 414x^5 + 1369x^4 + 3312x^3 + 5760x^2 + 6656x + 4096$.

Then f corresponds to an isogeny class $\mathcal{C}$ of abelian fourfolds over $\mathbb{F}_8$.

The Weil polynomial predicts nonnegative place counts, so maybe a Jacobian?

But we check: K is unramified over K^+, and $N_{K/\mathbb{Q}}(\pi - \overline{\pi}) = 199^2$.

Since $199 \not\equiv 1369 \bmod 4$, $\mathcal{C}$ does not contain a PPAV... or a Jacobian.

Decomposable and indecomposable polarizations

Definition

Suppose A is an abelian variety over a field k with a principal polarization λ.

1. (A, λ) is *decomposable* if there are nontrivial (A_1, λ_1) and (A_2, λ_2) and an isomorphism $A \to A_1 \times A_2$ that identifies λ with $\lambda_1 \times \lambda_2$.
2. (A, λ) is *geometrically decomposable* if it is decomposable over $\overline{k}$.

Fact

The canonical polarization of a Jacobian variety is geometrically indecomposable.

Consequence

An isogeny class with no geometrically indecomposable principally polarized varieties also has no Jacobians.

Analyzing how varieties split

Question

How can we tell whether every principally polarized variety in an isogeny class is decomposable?

Let h be the real Weil polynomial of an abelian variety A.

Suppose $h = h_1 h_2$ with $h_1, h_2 \in \mathbb{Z}[x]$ coprime to one another.

Then A is isogenous to $A_1 \times A_2$, where A_i has real Weil polynomial h_i.

Question

How big is the smallest isogeny from A to a product of this form?

Reduced resultants help us analyze splittings

Reduced resultants let us bound the degree of the smallest splitting $A \to A_1 \times A_2$.

Definition

Let f be a monic polynomial in $\mathbb{Z}[x]$.

The *radical* of f is the product of its irreducible factors, each taken once.

Definition

Let h_1 and h_2 be coprime monic polynomials in $\mathbb{Z}[x]$, with radicals H_1 and H_2.

Let I be the ideal of $\mathbb{Z}[x]$ generated by H_1 and H_2.

The *reduced resultant* of h_1 and h_2 is the positive generator of $I \cap \mathbb{Z}$.

Note: the reduced resultant of h_1 and h_2 is a $\mathbb{Z}[x]$-linear combination of H_1 and H_2.

Minimal splittings

Let A have real Weil polynomial $h = h_1 h_2$, with h_1 and h_2 coprime.

Theorem

There are unique abelian varieties A_1 and A_2 with real Weil polynomials h_1 and h_2, and a unique finite group scheme Δ, such that there is an exact sequence

$$0 \longrightarrow \Delta \longrightarrow A_1 \times A_2 \longrightarrow A \longrightarrow 0$$

where the induced maps $A_1 \to A$ and $A_2 \to A$ injective.

In addition, the induced maps $\Delta \to A_1$ and $\Delta \to A_2$ are embeddings, and Δ is annihilated by the reduced resultant r of h_1 and h_2.

The idea of the proof

(Goal: $\exists!$ A_1, A_2, Δ with $0 \to \Delta \to A_1 \times A_2 \to A \to 0$ and $A_i \hookrightarrow A$, and we have $r\Delta = 0$.)

- Take any isogeny $B_1 \times B_2 \to A$. Find the largest product $\Delta_1 \times \Delta_2$ in its kernel.
- Let $A_i = B_i/\Delta_i$, and write $0 \to \Delta \to A_1 \times A_2 \to A \to 0$.
- Then $\Delta \hookrightarrow A_i$ and $A_i \hookrightarrow A$ for both i.
- Let F and V be the Frobenius and Verschiebung endomorphisms on A.
- We have $H(F + V) = 0$, and $H_i(F + V) = 0$ on A_i.
- Since Δ embeds in both A_1 and A_2, we have $H_i(F + V) = 0$ on Δ.
- The reduced resultant is a $\mathbb{Z}[x]$-linear combination of the H_i, so $r = 0$ on Δ.

Application: The “resultant 1” method

If the reduced resultant r is equal to 1, then $\Delta = 0$ and $A \cong A_1 \times A_2$.

The only maps between A_1 and A_2 are 0, so every polarization on A is a product.

Fact: the reduced resultant of h_1 and h_2 is 1 if and only if the usual resultant is ± 1.

Theorem (Serre 1985)

If the real Weil polynomial h of an isogeny class can be written $h = h_1 h_2$, where the resultant of h_1 and h_2 is ± 1, then the isogeny class contains no Jacobians.

A genus-8 curve over $\mathbb{F}_4$ with 24 points?

Over $\mathbb{F}_4$, the real Weil polynomial

$$h = x^8 + 19x^7 + 152x^6 + 664x^5 + 1713x^4 + 2618x^3 + 2212x^2 + 824x + 32$$

gives one of 26 isogeny classes that might contain the Jacobian of a genus-8 curve with 24 points.

Example

We have $h = h_1 h_2$ with $h_1 = (x+2)^3(x+4)$ and $h_2 = (x^4 + 9x^3 + 26x^2 + 24x + 1)$.

We compute that $\mathrm{Res}(h_1, h_2) = 1$.

Therefore, there is no Jacobian in this isogeny class.

Hermitian modules

Suppose E is an elliptic curve over $\mathbb{F}_q$ with trace t, where $\Delta := t^2 - 4q$ is a fundamental discriminant of a quadratic order $\mathcal{O}$.

Principal polarizations on E^n correspond to $n \times n$ positive definite unimodular Hermitian matrices over $\mathcal{O}$.

If $\mathcal{O}$ has class number 1, then for all n, the only variety isogenous to E^n is E^n itself!

Indecomposable Hermitian forms

Theorem

Assume $\Delta \neq 0$.

There's an indecomposable PPAV isog. to E^2 *if and only if* $\Delta \notin \{-3, -4, -7\}$.

There's an indecomposable PPAV isog. to E^3 *if and only if* $\Delta \notin \{-3, -4, -8, -11\}$.

Serre proves this in his 1985 Harvard course notes. Follows from Hoffmann 1991.

Theorem

Assume $\Delta \neq 0$. *If* $n = 8$, $n = 12$, *or* $n > 13$, *then there is a variety isogenous to* E^n *with an indecomposable principal polarization.*

O'Meara 1975 shows there are indecomposable unimodular $\mathbb{Z}$-lattices of rank n. Smith 1978 shows: tensored with $\mathcal{O}$, they give indecomposable Hermitian forms.

Counting arguments

Let f be the Weil polynomial of a simple ordinary isogeny class $\mathcal{C}$.

Let K be the number field defined by f, with $\pi \in K$ a root of f.

Definition

An order $\mathcal{O} \subset K$ is *convenient* if

1. $\pi \in \mathcal{O}$ and $\mathcal{O}$ is stable under complex conjugation;
2. the maximal real suborder $\mathcal{O}^+$ is Gorenstein;
3. the trace dual of $\mathcal{O}$ is generated as an $\mathcal{O}$-module by its totally imaginary elements.

If $\mathcal{O} \subset K$ is convenient, there is a formula for the number of principally polarized varieties in $\mathcal{C}$ with endomorphism ring $\mathcal{O}$:

PPAVs with convenient endomorphism rings

Theorem

If $\mathcal{O}$ is convenient and the norm map $\operatorname{Pic}\mathcal{O} \to \operatorname{Pic}^+\mathcal{O}^+$ is surjective, the number of PPAVs in $\mathcal{C}$ with endomorphism ring $\mathcal{O}$ is equal to

$$\frac{1}{[N(U):(U^+)^2]}\,\frac{\#\operatorname{Pic}\mathcal{O}}{\#\operatorname{Pic}\mathcal{O}^+},$$

where U is the unit group of $\mathcal{O}$ and U^+ is the unit group of $\mathcal{O}^+$.

For maximal orders, this is due to Shimura and Taniyama (1961).
In this generality, Howe 2020.

Application to abelian surfaces

Theorem (H. 2004)

Let q be an odd prime power. There are no geometrically irreducible principally polarized varieties with Weil polynomial $x^4 + (2 - 2q)x^2 + q^2$.

Let $\mathcal{C}$ be the isogeny class with this Weil polynomial. To prove the statement:

1. Show that every PPAV in $\mathcal{C}$ has convenient endomorphism ring.
2. Count the number of PPAVs.
3. Count the number of $E/\mathbb{F}_{q^2}$ with Weil polynomial $x^2 + (2 - 2q)x + q^2$.
4. Weil restriction: Each such E gives a geometrically decomposable PPAV in $\mathcal{C}$.
5. Show that these Weil restrictions account for all of the PPAVs in $\mathcal{C}$.

Supersingular factors

Suppose q is a square, and let $s = \pm\sqrt{q}$.

Let $\mathcal{C}$ be an isogeny class over $\mathbb{F}_q$ with real Weil polynomial $h = h_0 \cdot (x - 2s)^n$, where h_0 is ordinary.

Theorem (H.–Lauter 2012)

If $h_0(2s)$ is squarefree, every principally polarized variety in $\mathcal{C}$ is decomposable.

Idea of proof: For every A in $\mathcal{C}$ there is an ordinary A_0 and supersingular E with

$$0 \longrightarrow \Delta \longrightarrow A_0 \times E^n \longrightarrow A \longrightarrow 0$$

as earlier, with Δ embedding into E^n and into A_0.

Frobenius and Verschiebung both act as the integer s on E^n and hence on Δ.

Frobenius and Verschiebung *don't* act as an integer on A_0, and this is visible in the group scheme Δ if it is nontrivial. This depends on additional properties of Δ and on $h_0(2s)$ being squarefree.

Another genus-8 curve over $\mathbb{F}_4$ with 24 points?

Over $\mathbb{F}_4$, the real Weil polynomial

$$h = x^8 + 19x^7 + 152x^6 + 664x^5 + 1716x^4 + 2652x^3 + 2351x^2 + 1065x + 180$$

gives one of 26 isogeny classes that might contain the Jacobian of a genus-8 curve with 24 points.

Example

We have $h = h_0 \cdot (x+4)$ with $h_0 = (x+1)(x+3)^2(x^2+3x+1)(x^2+5x+5)$.

We compute that $h_0(-4) = (-3) \cdot (-1)^2 \cdot 5 \cdot 1 = 15$.

This is squarefree, so there is no Jacobian in this isogeny class.

No Jacobians: Summary

We have seen the following techniques for showing that an isogeny class contains no Jacobians:

1. Using H. 1995 to show there are no PPAVs in an isogeny class
2. The resultant 1 method
3. Special Hermitian modules
4. Counting arguments to show every PPAV is geometrically decomposable
5. Supersingular factors

Let's move on to the next section.

Part II: Deducing information about curves

Nontrivial automorphisms

Theorem (Torelli's theorem)

Let C be a curve with polarized Jacobian (J, λ).

There's a homomorphism $\operatorname{Aut} C \to \operatorname{Aut}(J, \lambda)$ given by $\varepsilon \mapsto (\varepsilon^{-1})^*$.

If C is hyperelliptic, this is an isomorphism. Otherwise, we have

$$\operatorname{Aut}(J, \lambda) \cong \{\pm 1\} \times \operatorname{Aut} C.$$

Nontrivial automorphisms when $h = h_1 h_2$

If (A, λ) is a PPAV with real Weil polynomial h with $h = h_1 h_2$ for coprime h_i, then

$$0 \longrightarrow \Delta \longrightarrow A_1 \times A_2 \longrightarrow A \longrightarrow 0$$

for some A_1, A_2, and Δ as before. Furthermore, if

- A_2 has an automorphism $\alpha \ldots$
- $\ldots$ with $\alpha\alpha^\dagger = 1$ for every positive involution $\dagger$ on $\mathrm{End}\, A_2 \ldots$
- $\ldots$ and if $\alpha - 1$ kills the image of Δ in A_2,

then the automorphism $(1, \alpha)$ of $A_1 \times A_2$ descends to an automorphism of (A, λ).

Main example: $\alpha = -1$. The "resultant 2" method

Theorem

If C is a curve with real Weil polynomial $h_1 h_2$ with h_1 and h_2 having reduced resultant 2, then C has an involution ε that defines a double cover $C \to D$, where D has real Weil polynomial h_1 or h_2.

Example

Let $h_1 = (x+2)^3$ and $h_2 = (x+4)^2(x^3+5x^2+6x+1)$. The real Weil polynomial $h_1 h_2$ could belong to a genus-8 curve $C/\mathbb{F}_4$ with 24 points.

The reduced resultant of the factors is 2, so we would have a double cover $C \to D$, where D has real Weil polynomial h_1 or h_2.

Can't be h_2, because a genus-8 curve can't cover a genus-5 curve.
Can't be h_1, because then D would have only 11 points while C has 24.

Therefore, no such C exists.

Nontrivial automorphisms when $h = h_0^e$ with h_0 irreducible

If $h = h_0^e$ then the corresponding Weil polynomial f satisfies $f = f_0^e$.

Let K be the number field defined by f_0, and let π be a root of h_0 in K.

Suppose $\mathbb{Z}[\pi, \overline{\pi}]$ contains a root of unity ζ. If C is a curve with real Weil polynomial $h = h_0^e$, then C has an automorphism ε with $\varepsilon^* = \pm\zeta$.

Application to genus-2 curves

Theorem (Maisner–Nart–H. 2002)

There is no curve over $\mathbb{F}_q$ with Weil polynomial $f = x^4 + (1 - 2q)x^2 + q^2$.

Idea of proof (for odd q):

- We check that f is irreducible, and that $\pi - \overline{\pi}$ is a primitive fourth root of 1.
- If C had Weil polynomial f, it would have an automorphism ε of order 4.
- Analysis of the action of ε on the Weierstrass points shows that all six of them are rational over $\mathbb{F}_{q^4}$.
- Non-Weierstrass points come in ε-orbits of size 4, so $\#C(\mathbb{F}_{q^4}) \equiv 2 \bmod 4$.
- But Weil polynomial predicts $q^4 - 4q^2 + 8q - 1$ points over $\mathbb{F}_{q^4}$.
- Contradiction, because $q^4 - 4q^2 + 8q - 1 \equiv 0 \bmod 4$.

Nontrivial automorphisms when $h = (x - t)^e$

Suppose $h = (x - t)^n$, where $\Delta = t^2 - 4q$ is the discriminant of a maximal order $\mathcal{O}$.

Alexander Schiemann has computed all unimodular Hermitian forms on rank-n lattices over maximal orders $\mathcal{O}$ for various smallish n and $\mathcal{O}$.

https://www.math.uni-sb.de/ag/schulze/Hermitian-lattices/

He computes the automorphism groups of all of the lattices.

Example: Genus-5 curves over $\mathbb{F}_{17}$ meeting the Weil–Serre bound

Example

No genus-5 curve $C/\mathbb{F}_{17}$ attains the Weil–Serre bound of 53 points.

1. A curve meeting the bound would have real Weil polynomial $(x+7)^5$, so $\Delta = -19$. Let $\mathcal{O}$ be the quadratic order of discriminant Δ.
2. Schiemann: Every rank-5 unimodular Hermitian $\mathcal{O}$-lattice has an automorphism of order 4.
3. Therefore every genus-5 curve $C/\mathbb{F}_{17}$ with 53 points has an involution.
4. Only possibility: Double cover of a curve with real Weil polynomial $(x+7)^2$.
5. Only one such genus-2 curve: $y^2 = x^6 + 3x^4 + 2x^2 + 15$.
6. Enumerate its genus-5 double covers. None has 53 points.

Maps to elliptic curves

Suppose C is a curve whose real Weil polynomial is divisible by the real Weil polynomial of an elliptic curve of trace t; that is, h is divisible by $x - t$.

Then there is a nonzero map $E \to \operatorname{Jac} C$. The principal polarization on $\operatorname{Jac} C$ pulls back to a polarization on E of degree d^2, for some d.

Embedding C into $\operatorname{Jac} C$, and then applying the dual map $\operatorname{Jac} C \to E$, gives a degree-$d$ map from C to E.

Bounding the degrees of maps to elliptic curves

Various methods for bounding d, based on reduced resultants and theorems about short vectors in lattices. Example:

Theorem (H.–Lauter 2012)

Suppose $C/\mathbb{F}_q$ has real Weil polynomial $h = h_0 \cdot (x - t)$, where t is the trace of an elliptic curve over $\mathbb{F}_q$.

Let r be the reduced resultant of h_0 and $x - t$.

Then there is a map from C to some elliptic curve of trace t, with degree dividing r.

Other results deal with cases when h is divisible by a *power* of $x - t$.

Genus-12 curves over $\mathbb{F}_2$ with 15 points

After applying all the elimination techniques we can think of, we are left with three possible real Weil polynomials for a genus-12 curve over $\mathbb{F}_2$ with 15 points.

One of them is $(x+1)^2(x+2)^2(x^2-2)(x^2+2x-2)^3$. We can show that there is a map of degree at most 4 from C to the elliptic curve $E/\mathbb{F}_2$ of trace -1.

Since $\#E(\mathbb{F}_2) = 4$ and $\#C(\mathbb{F}_2) = 15$, the map $C \to E$ must have degree 4.

Open problem

How do we enumerate degree-4 covers of E by curves of genus 12?

Deducing information about curves: Summary

We have seen the following techniques for finding useful properties of curves from their real Weil polynomials:

1. The resultant 2 method of producing double covers
2. Other methods of deducing the existence of automorphisms
3. Finding maps of bounded degree to an elliptic curve

This list feels very sparse! Are there other techniques that we are missing?