

Computing isomorphism classes of abelian varieties over finite fields.

Stefano Marseglia

Utrecht University

Curves over Finite Fields:
Past, Present and Future

Abelian varieties over \mathbb{C} vs \mathbb{F}_q

- Let A/\mathbb{C} be an abelian variety of dimension g .
- Then $A(\mathbb{C})$ is a **torus**: $T := \mathbb{C}^g / \Lambda$, where $\Lambda \simeq_{\mathbb{Z}} \mathbb{Z}^{2g}$.
- Moreover, T admits a non-degenerate **Riemann form** \longleftrightarrow polarization.
- Actually, $A \mapsto A(\mathbb{C})$ induces an **equivalence** of categories:

$$\{\text{abelian varieties } / \mathbb{C}\} \longleftrightarrow \left\{ \mathbb{C}^g / \Lambda \text{ with } \Lambda \simeq \mathbb{Z}^{2g} \text{ admitting a Riemann form} \right\}.$$

- In **char. $p > 0$** such an equivalence **cannot exist**: there are (supersingular) elliptic curves with quaternionic endomorphism algebras.
- Nevertheless, over finite fields, we obtain analogous results if we restrict ourselves to certain **subcategories** of AVs.

Isogeny classification over \mathbb{F}_q

- A/\mathbb{F}_q comes with a **Frobenius** endomorphism, that induces an action

$$\text{Frob}_A : T_\ell A \rightarrow T_\ell A \text{ for any } \ell \neq p,$$

where $T_\ell(A) = \varprojlim A[\ell^n] \simeq \mathbb{Z}_\ell^{2g}$.

- $h_A(x) := \text{char}(\text{Frob}_A)$ is a **q -Weil** polynomial and **isogeny invariant**.
- By **Honda-Tate** theory, the association

$$\text{isogeny class of } A \longmapsto h_A(x)$$

is injective and allows us to **enumerate** all AVs up to isogeny.

- Also, $h_A(x)$ is squarefree $\iff \text{End}(A)$ is commutative.

Deligne's equivalence

Recall: A/\mathbb{F}_q is **ordinary** if half of the p -adic roots of h_A are units.

Theorem (Deligne '69)

Let $q = p^r$, with p a prime. There is an *equivalence* of categories:

$$\begin{array}{ccc}
 \{ \text{Ordinary abelian varieties over } \mathbb{F}_q \} & & A \\
 \updownarrow & & \downarrow \\
 \left\{ \begin{array}{l} \text{pairs } (T, F), \text{ where } T \simeq_{\mathbb{Z}} \mathbb{Z}^{2g} \text{ and } T \xrightarrow{F} T \text{ s.t.} \\
 - F \otimes \mathbb{Q} \text{ is semisimple} \\
 - \text{the roots of } \text{char}_{F \otimes \mathbb{Q}}(x) \text{ have abs. value } \sqrt{q} \\
 - \text{half of them are } p\text{-adic units} \\
 - \exists V : T \rightarrow T \text{ such that } FV = VF = q \end{array} \right\} & & (T(A), F(A))
 \end{array}$$

- Ordinary A/\mathbb{F}_q can be canonically lifted: $\rightsquigarrow \mathcal{A}_{\text{can}}/\text{Witt}(\mathbb{F}_q)\dots$
- ... characterized by: $\text{End}_{\mathbb{F}_q}(A) = \text{End}_W(\mathcal{A}_{\text{can}})$.
- Put $T(A) := H_1(\mathcal{A}_{\text{can}} \otimes \mathbb{C}, \mathbb{Z})$ and $F(A) :=$ the induced Frobenius.

Squarefree case

- Fix an **ordinary squarefree** q -Weil polynomial h :
- \rightsquigarrow an isogeny class $\mathcal{C}_h/\mathbb{F}_q$.
- Put $K := \mathbb{Q}[x]/(h) = \mathbb{Q}[F]$, an étale algebra = product of number fields.
- Put $V = q/F$. Deligne's equivalence induces:

Theorem

$$\begin{array}{ccc} \{ \text{abelian varieties over } \mathbb{F}_q \text{ in } \mathcal{C}_h \} / \simeq & & \\ \updownarrow & & \\ \{ \text{fractional ideals of } \mathbb{Z}[F, V] \subset K \} / \simeq & =: & \text{ICM}(\mathbb{Z}[F, V]) \\ & & \text{ideal class monoid} \end{array}$$

- **Problem:** $\mathbb{Z}[F, V]$ might not be maximal \rightsquigarrow **non-invertible** ideals.

ICM : Ideal Class Monoid

Let R be an **order** in an étale \mathbb{Q} -algebra K .

- Recall: for **fractional R -ideals** I and J

$$I \simeq_R J \iff \exists x \in K^\times \text{ s.t. } xI = J$$

- We have

$$\mathrm{ICM}(R) \supseteq \mathrm{Pic}(R) = \{\text{invertible fractional } R\text{-ideals}\} / \simeq_R$$

with equality \Updownarrow iff $R = \mathcal{O}_K$

- ...and actually

$$\mathrm{ICM}(R) \supseteq \bigsqcup_{\substack{R \subseteq S \subseteq \mathcal{O}_K \\ \text{over-orders}}} \mathrm{Pic}(S) \quad \text{with equality iff } R \text{ is Bass}$$

- Hofmann-Sircana '19: computation of over-orders.

simplify the problem

Study the isomorphism problem locally: (Dade, Taussky, Zassenhaus '62)

- **weak equivalence:**

$$I_{\mathfrak{p}} \simeq_{R_{\mathfrak{p}}} J_{\mathfrak{p}} \text{ for every } \mathfrak{p} \in \text{mSpec}(R)$$



$$1 \in (I : J)(J : I) \quad \text{easy to check!}$$

- Let $\mathcal{W}(R)$ be the set of weak eq. classes...
...whose representatives can be found in

$$\left\{ \text{sub-}R\text{-modules of } \mathcal{O}_K / \mathfrak{f}_R \right\} \quad \text{finite! and most of the time not-too-big ...}$$

where $\mathfrak{f}_R = (R : \mathcal{O}_K)$ is the conductor of R .

Compute $\text{ICM}(R)$

Partition w.r.t. the multiplier ring:

$$\mathcal{W}(R) = \bigsqcup_{R \subseteq S \subseteq \mathcal{O}_K} \mathcal{W}_S(R)$$

$$\text{ICM}(R) = \bigsqcup_{R \subseteq S \subseteq \mathcal{O}_K} \text{ICM}_S(R)$$

the “pedix” $-_S$ means
“only classes with multiplier ring S ”

Theorem (M.)

For every over-order S of R , $\text{Pic}(S)$ acts *freely* on $\text{ICM}_S(R)$ and

$$\mathcal{W}_S(R) = \text{ICM}_S(R) / \text{Pic}(S)$$

Repeat for every $R \subseteq S \subseteq \mathcal{O}_K$:

$$\rightsquigarrow \text{ICM}(R).$$

To sum up:

- To sum up:
- Given a **ordinary squarefree** q -Weil polynomial h ...
- ... \rightsquigarrow algorithm to **compute the isomorphism classes** of AVs in \mathcal{C}_h .
- We can actually get a lot more!

Dual varieties and Polarizations

Howe described **dual** varieties and **polarizations** on Deligne modules.

Theorem

Let $A \in \mathcal{C}_h$ with h ordinary and squarefree. If $A \leftrightarrow I$, then:

- $A^\vee \leftrightarrow \bar{I}^t := \{\bar{x} \in K : \text{Tr}(xI) \subseteq \mathbb{Z}\}.$
- a polarization μ of A corresponds to a $\lambda \in K^\times$ such that
 - $\lambda I \subseteq \bar{I}^t$ (isogeny);
 - λ is **totally imaginary** ($\bar{\lambda} = -\lambda$);
 - λ is Φ -positive, where Φ is a CM-type of K satisf. the **Shimura-Taniyama** formula.

Also: $\deg \mu = [\bar{I}^t : \lambda I].$

- if $(A, \mu) \leftrightarrow (I, \lambda)$ is a princ. polarized ab. var. and $S = (I : I)$ then

$$\left\{ \begin{array}{l} \text{non-isomorphic princ.} \\ \text{polarizations of } A \end{array} \right\} \longleftrightarrow \frac{\{\text{totally positive } u \in S^\times\}}{\{\bar{v}v : v \in S^\times\}},$$

- and $\text{Aut}(A, \mu) = \{\text{torsion units of } S\}.$

Principal Polarizations

We have an **algorithm** to enumerate principal polarizations up to isomorphism:

- 1 Compute i_0 such that $i_0 I = \bar{I}^t$.
- 2 Loop over the representatives u of the finite quotient

$$\frac{S^\times}{\{v\bar{v} : v \in S^\times\}}.$$

- 3 If $\lambda := i_0 u$ is totally imaginary and Φ -positive ...
- 4 ... then we have one principal polarization.
- 5 By the previous Theorem, we have all princ. polarizations up to isom.

Can modify to compute polarizations of any degree.

Example

- Let $h(x) = x^8 - 5x^7 + 13x^6 - 25x^5 + 44x^4 - 75x^3 + 117x^2 - 135x + 81$.
- \rightsquigarrow isogeny class of an simple ordinary abelian varieties over \mathbb{F}_3 of dimension 4.
- Let F be a root of $h(x)$ and put $R := \mathbb{Z}[F, 3/F] \subset \mathbb{Q}(F)$.
- 8 over-orders of R : two of them are not Gorenstein.
- $\#\text{ICM}(R) = 18 \rightsquigarrow 18$ isom. classes of AV in the isogeny class.
- 5 are not invertible in their multiplier ring.
- 8 classes admit principal polarizations.
- 10 isomorphism classes of princ. polarized AV.

Example

Concretely:

$$\begin{aligned} I_1 = & 2645633792595191\mathbb{Z} \oplus (F + 836920075614551)\mathbb{Z} \oplus (F^2 + 1474295643839839)\mathbb{Z} \oplus \\ & \oplus (F^3 + 1372829830503387)\mathbb{Z} \oplus (F^4 + 1072904687510)\mathbb{Z} \oplus \\ & \oplus \frac{1}{3}(F^5 + F^4 + F^3 + 2F^2 + 2F + 6704806986143610)\mathbb{Z} \oplus \\ & \oplus \frac{1}{9}(F^6 + F^5 + F^4 + 8F^3 + 2F^2 + 2991665243621169)\mathbb{Z} \oplus \\ & \oplus \frac{1}{27}(F^7 + F^6 + F^5 + 17F^4 + 20F^3 + 9F^2 + 68015312518722201)\mathbb{Z} \end{aligned}$$

principal polarizations:

$$\begin{aligned} x_{1,1} = & \frac{1}{27}(-121922F^7 + 588604F^6 - 1422437F^5 + \\ & + 1464239F^4 + 1196576F^3 - 7570722F^2 + 15316479F - 12821193) \\ x_{1,2} = & \frac{1}{27}(3015467F^7 - 17689816F^6 + 35965592F^5 - \\ & - 64660346F^4 + 121230619F^3 - 191117052F^2 + 315021546F - 300025458) \end{aligned}$$

$$\text{End}(I_1) = R$$

$$\# \text{Aut}(I_1, x_{1,1}) = \# \text{Aut}(I_1, x_{1,2}) = 2$$

Example

$$\begin{aligned} I_7 = & 2\mathbb{Z} \oplus (F+1)\mathbb{Z} \oplus (F^2+1)\mathbb{Z} \oplus (F^3+1)\mathbb{Z} \oplus (F^4+1)\mathbb{Z} \oplus \frac{1}{3}(F^5+F^4+F^3+2F^2+2F+3)\mathbb{Z} \oplus \\ & \oplus \frac{1}{36}(F^6+F^5+10F^4+26F^3+2F^2+27F+45)\mathbb{Z} \oplus \\ & \oplus \frac{1}{216}(F^7+4F^6+49F^5+200F^4+116F^3+105F^2+198F+351)\mathbb{Z} \end{aligned}$$

principal polarization:

$$x_{7,1} = \frac{1}{54}(20F^7 - 43F^6 + 155F^5 - 308F^4 + 580F^3 - 1116F^2 + 2205F - 1809)$$

$$\begin{aligned} \text{End}(I_7) = & \mathbb{Z} \oplus F\mathbb{Z} \oplus F^2\mathbb{Z} \oplus F^3\mathbb{Z} \oplus F^4\mathbb{Z} \oplus \frac{1}{3}(F^5+F^4+F^3+2F^2+2F)\mathbb{Z} \oplus \\ & \oplus \frac{1}{18}(F^6+F^5+10F^4+8F^3+2F^2+9F+9)\mathbb{Z} \oplus \\ & \oplus \frac{1}{108}(F^7+4F^6+13F^5+56F^4+80F^3+33F^2+18F+27)\mathbb{Z} \end{aligned}$$

$$\# \text{Aut}(I_7, x_{7,1}) = 2$$

I_1 is invertible in R , but I_7 is not invertible in $\text{End}(I_7)$.

The Power-of-a-Bass case

- Another case we understand well: $h = g^r$ for g square-free and ordinary.
- Every A in \mathcal{C}_{g^r} is $A \sim B^r$ for $B \in \mathcal{C}_g$.
- Put $R := \mathbb{Z}[F, V] \subset K_g := \mathbb{Q}[x]/(g) = \mathbb{Q}[F]$.
- Under these assumption, Deligne's theorem induces:

$$\{\text{abelian varieties in } \mathcal{C}_{g^r}\} \longleftrightarrow \{R\text{-modules } M \subseteq K_g^r\}.$$

- Recall: an order R is **Bass** if all its over-orders S are **Gorenstein**, ...
- ... or equivalently $\text{ICM}(R) = \bigsqcup_S \text{Pic}(S)$.
- Eg: quadratic orders are Bass \rightsquigarrow powers of ordinary elliptic curves E^r .
- If R is Bass, then M is isomorphic to a **direct sum** of $\text{frac.}R$ -ideals.

The Power-of-a-Bass case

Theorem

$$\{\text{abelian varieties in } \mathcal{C}_{g^r}\} / \simeq \longleftrightarrow \{I_1 \oplus \dots \oplus I_r : I_j \text{ a frac. } R\text{-ideal}\} / \simeq$$

we have a classification: $\longleftrightarrow \left\{ (S_1 \subseteq S_2 \subseteq \dots \subseteq S_r, [I]_{\simeq}) : \begin{array}{l} R \subseteq S_j \text{ orders,} \\ I \text{ a frac. } R\text{-ideal} \\ \text{with } (I : I) = S_r \end{array} \right\}$

Corollary

If $A \in \mathcal{C}_{g^r}$ then $A \simeq C_1 \times \dots \times C_r$, for $C_j \in \mathcal{C}_g$. *everything is a product!*

- Howe's results on polarizations carry over ...
- ... but computing them in general is harder!
- Solved for E^r by Kirschmer-Narbonne-Ritzenthaler-Robert '20. *next talk!*

Example

Let $g = x^6 - 3x^5 + 6x^4 - 10x^3 + 18x^2 - 27x + 27$. Note $\mathcal{C}(g)$ is an isogeny class of simple ordinary abelian varieties over \mathbb{F}_3 . Define

$K = \mathbb{Q}[x]/(g) = \mathbb{Q}(F)$ and $R = \mathbb{Z}[F, V]$. The only over-order of R is the maximal order \mathcal{O}_K of K and, since R is Gorenstein R is Bass. Observe

$$\text{Pic}(R) \simeq \mathbb{Z}/3\mathbb{Z} \text{ and } \text{Pic}(\mathcal{O}_K) = \{1\}.$$

Let I be a representatives of a generator of $\text{Pic}(R)$. We now list the representatives of the isomorphism classes in $\mathcal{C}(g^3)$:

$$\begin{array}{lll} M_1 = R \oplus R \oplus R & M_2 = R \oplus R \oplus I & M_3 = R \oplus R \oplus I^2 \\ M_4 = R \oplus R \oplus \mathcal{O}_K & M_5 = R \oplus \mathcal{O}_K \oplus \mathcal{O}_K & M_6 = \mathcal{O}_K \oplus \mathcal{O}_K \oplus \mathcal{O}_K \end{array}$$

$$\text{End}(M_1) = \text{Mat}_3(R) \text{ and } \text{End}(M_2) = \begin{pmatrix} R & R & I \\ R & R & I \\ (R:I) & (R:I) & R \end{pmatrix}$$

Outside of the ordinary...

Theorem (Centeleghe-Stix '15)

There is an equivalence of categories:

$$\begin{array}{ccc}
 \{\text{abelian varieties } A \text{ over } \mathbb{F}_p \text{ with } h_A(\sqrt{p}) \neq 0\} & & A \\
 \updownarrow & & \downarrow \\
 \left\{ \begin{array}{l} \text{pairs } (T, F), \text{ where } T \simeq_{\mathbb{Z}} \mathbb{Z}^{2g} \text{ and } T \xrightarrow{F} T \text{ s.t.} \\ - F \otimes \mathbb{Q} \text{ is semisimple} \\ - \text{the roots of } \text{char}_{F \otimes \mathbb{Q}}(x) \text{ have abs. value } \sqrt{p} \\ - \text{char}_F(\sqrt{p}) \neq 0 \\ - \exists V : T \rightarrow T \text{ such that } FV = VF = p \end{array} \right\} & & (T(A), F(A))
 \end{array}$$

- Now, $T(A) := \text{Hom}(A, A_w)$, where A_w has minimal End among the varieties with Weil support $w = w(A)$.
- $F(A)$ is the induced Frobenius.

Outside of the ordinary...isomorphism classes

- Everything I told so far about **isomorphism classes** works in the **same way** using the Centeleghe-Stix functor:
- both in the squarefree and Power-of-Bass cases, over \mathbb{F}_p .
- (There are there are other functors:
Oswal-Shankar for almost-ordinary abelian varieties, together with generalizations by Bergström-Karemaker-M.;
Serre and the work of Kani, Jordan-Keeton-Poonen-Rains-Shepherd-Barron-Tate for E^r ; **Isabel Vogt's talk**
... but we will not use them in this talk.)
- For polarizations, the results by Howe do **not apply immediately** to the Centeleghe-Strix case:
- in general we **cannot** lift canonically **each** abelian variety.

Outside of the ordinary...polarizations

- New strategy: with Jonas Bergström and Valentijn Karemaker '21.
- Consider \mathcal{C}_h with h squarefree $/\mathbb{F}_q \rightsquigarrow K = \mathbb{Q}[F]$.
- Chai-Conrad-Oort: A (p -adic) CM-type (K, Φ) satisfies the **Residual Reflex Condition** if:
 1. the **Shimura-Taniyama formula** holds for Φ .
 2. the residual field k_E of the reflex field E of (K, Φ) satisfies: $k_E \subseteq \mathbb{F}_q$.

Theorem (Chai-Conrad-Oort)

If (K, Φ) satisfies the RRC then in \mathcal{C}_h there exists an abelian variety A admitting a canonical lifting \mathcal{A} .

- If we understand the polarizations of A we can 'spread' them to the whole isogeny class.

Outside of the ordinary...polarizations

Now \mathcal{C}_h over \mathbb{F}_p : let \mathcal{G} be the Centeleghe-Stix functor.
 Assume that there exists A admitting a canonical lifting \mathcal{A} .
 Let $f : A \rightarrow B$ be an isogeny.

$$\begin{array}{ccccc}
 & & \mathrm{Hom}(\mathcal{A}, \mathcal{A}^\vee) & & \\
 & & \downarrow \text{red} & \searrow \text{complex unif.} & \\
 \mathrm{Hom}(B, B^\vee) & \xrightarrow{f^* := f^\vee \circ - \circ f} & \mathrm{Hom}(A, A^\vee) & & (\bar{I}^t : I) \\
 \downarrow \mathcal{G} & & \downarrow \mathcal{G} & & \simeq \downarrow \alpha \\
 (\mathcal{G}(B) : \mathcal{G}(B^\vee)) & \xrightarrow{\mathcal{G}(f^*)} & (\mathcal{G}(A) : \mathcal{G}(A^\vee)) & = & (\bar{I}^t : I)
 \end{array}$$

Note that $\mathcal{G}(f^*)$ is multiplication by the totally positive element $\overline{\mathcal{G}(f)}\mathcal{G}(f)$:
 it sends totally imaginary elements to totally imaginary elements and
 Φ -positive elements to Φ -positive elements. The only 'issue' is the α .
 We study when we can 'pretend' $\alpha = 1$.

Final remarks

- Base field extensions and **twists** (ordinary case).
- **Period matrices** of the canonical lift (ordinary case).
- with Caleb Springer '21, building on Howe-Kedlaya '21, we proved that every finite abelian group occur as the **group of points** of an ordinary AV over \mathbb{F}_2 . [check Wanlin Li's talk!](#)
- Magma implementations of the algorithms are on GitHub!
- Results of computations will appear on the LMFDB.

Thank you!