Computing isomorphism classes of abelian varieties over finite fields

Stefano Marseglia

Utrecht University

VaNTAGe

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 $\Lambda \simeq_{\mathbb{Z}} \mathbb{Z}^{2g}$.
- Also, T admits a non-degenerate **Riemann form** $\longleftrightarrow$ polarization.
- The functor $A \mapsto A(\mathbb{C})$ induces an equivalence of categories:

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

- 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

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

  where $T_\ell(A) = \varprojlim A[\ell^n] \simeq \mathbb{Z}_\ell^{2g}$.
- $h_A(x) := \mathrm{char}(\mathrm{Frob}_A)$ is a q-Weil polynomial and **isogeny invariant**.
- By **Honda-Tate** theory ([Tat66]-[Hon68]), 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 $\iff$ $\mathrm{End}(A)$ 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 [Del69])

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

$$\left\{ \textbf{Ordinary } \textit{abelian varieties over } \mathbb{F}_q \right\} \qquad\qquad A$$

$$\updownarrow \qquad\qquad\qquad\qquad \mapsto$$

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

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

Squarefree case

- Fix an **ordinary squarefree** q-Weil polynomial h :
- $\rightsquigarrow$ an isogeny class $\mathscr{C}_h/\mathbb{F}_q$.
- 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

$$\left\{\textit{abelian varieties over } \mathbb{F}_q \textit{ in } \mathscr{C}_h\right\}_{/\simeq}$$

$$\updownarrow$$

$$\left\{\textit{fractional ideals of } \mathbb{Z}[F,V] \subset K\right\}_{/\simeq} \quad =: \mathrm{ICM}(\mathbb{Z}[F,V])$$

ideal class monoid

- 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

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

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

- ...and actually

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

- Hofmann-Sircana [HS20]: computation of over-orders.

simplify the problem

First, locally: Dade-Taussky-Zassenhaus [DTZ62].

- **weak equivalence**:

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

$$\Updownarrow$$

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

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

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

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

Compute $\mathrm{ICM}(R)$

Partition w.r.t. the multiplicator ring:

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

$$\mathrm{ICM}(R) = \bigsqcup_{R \subseteq S \subseteq \mathscr{O}_K} \mathrm{ICM}_S(R)$$

the "pedix" $-_S$ means "only classes with multiplicator ring S"

Theorem ([Mar20b])

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

$$\mathscr{W}_S(R) = \mathrm{ICM}_S(R)/\mathrm{Pic}(S)$$

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

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

To sum up:

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

Dual varieties and Polarizations

Howe [How95] : **dual** varieties and **polarizations** on Deligne modules.

Theorem ([Mar21])

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

- $A^\vee \leftrightarrow \overline{I}^t := \{\overline{x} \in K : \mathrm{Tr}(xI) \subseteq \mathbb{Z}\}$.
- *a polarization μ of A corresponds to a $\lambda \in K^\times$ such that*
  - $\lambda I \subseteq \overline{I}^t$ *(isogeny of $\deg \mu = [\overline{I}^t : \lambda I]$);*
  - λ *is totally imaginary ($\overline{\lambda} = -\lambda$);*
  - λ *is Φ-positive ($\Im\varphi(\lambda) > 0$ for all $\varphi \in \Phi$),*

  where Φ is a CM-type of K satisf. the Shimura-Taniyama formula.
- *if $(A,\mu) \leftrightarrow (I,\lambda)$ is a princ. polarized ab. var. and $S = (I : I)$ then*

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

similar statement for $\deg \mu > 1$

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

Principal Polarizations

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

1. Compute i_0 such that $i_0 I = \overline{I}^t$.
2. Loop over the representatives u of the finite quotient
$$\frac{S^\times}{\{v\overline{v} : v \in S^\times\}}.$$
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.

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.
- $\#\mathrm{ICM}(R) = 18 \rightsquigarrow 18$ isom. classes of AV in the isogeny class.
- 5 are not invertible in their multiplicator ring.
- 8 classes admit principal polarizations.
- 10 isomorphism classes of princ. polarized AV.

Example

Concretely:

$$
\begin{aligned}
I_1 =& 2645633792595191\mathbb{Z} \oplus (F + 836920075614551)\mathbb{Z} \oplus (F^2 + 1474295643839839)\mathbb{Z}\oplus \\
&\oplus (F^3 + 1372829830503387)\mathbb{Z} \oplus (F^4 + 1072904687510)\mathbb{Z}\oplus \\
&\oplus \frac{1}{3}(F^5 + F^4 + F^3 + 2F^2 + 2F + 670480698614361 0)\mathbb{Z}\oplus \\
&\oplus \frac{1}{9}(F^6 + F^5 + F^4 + 8F^3 + 2F^2 + 2991665243621169)\mathbb{Z}\oplus \\
&\oplus \frac{1}{27}(F^7 + F^6 + F^5 + 17F^4 + 20F^3 + 9F^2 + 6801531251872220 1)\mathbb{Z}
\end{aligned}
$$

principal polarizations:

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

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

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

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:

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

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

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

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

The Power-of-a-Bass case

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

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

- Recall: an order R is **Bass** if all its over-orders S are **Gorenstein**, ...
- ... or equivalently $\mathrm{ICM}(R) = \bigsqcup_S \mathrm{Pic}(S)$. (see [Bas63])
- 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 frac.R-ideals.

The Power-of-a-Bass case

Theorem ([Mar19])

If $R = \mathbb{Z}[F,V]$ is Bass then

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

we have a classification:

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

Corollary

If $A \in \mathscr{C}_{g^r}$ then $A \simeq C_1 \times \ldots \times C_r$, for $C_j \in \mathscr{C}_g$.

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 [KNRR21].

Outside of the ordinary...

Theorem (Centeleghe-Stix [CS15])

There is an equivalence of categories:

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

- Now, $T(A) := \mathrm{Hom}(A, A_w)$, 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 $\mathbb{F}_p$.
- 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: jt. Jonas Bergström and Valentijn Karemaker [BKM21].
- Consider $\mathscr{C}_h$ 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 residuel field k_E of the reflex field E of (K, Φ) satisfies: $k_E \subseteq \mathbb{F}_q$.

Theorem ([CCO14])

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

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

Outside of the ordinary...polarizations

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

$$\begin{tikzcd}
 & \mathrm{Hom}(\mathscr{A},\mathscr{A}^\vee) \arrow[d, "\text{red}"] \arrow[dr, "\text{complex unif.}"] & \\
\mathrm{Hom}(B,B^\vee) \arrow[r, "f^*:=f^\vee\circ - \circ f"] \arrow[d, "\mathscr{G}"] & \mathrm{Hom}(A,A^\vee) \arrow[d, "\mathscr{G}"] & (\bar{I}^t : I) \arrow[d, "\alpha", "\simeq"'] \\
(\mathscr{G}(B):\mathscr{G}(B^\vee)) \arrow[r, "\mathscr{G}(f^*)"] & (\mathscr{G}(A):\mathscr{G}(A^\vee)) \arrow[r, equal] & (\bar{I}^t : I)
\end{tikzcd}$$

Note that $\mathscr{G}(f^*)$ is multiplication by the totally positive element $\overline{\mathscr{G}(f)}\mathscr{G}(f)$: 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' $\alpha = 1$.

Some related work

- Base field extensions and **twists** (ordinary case) [Mar20a].
- **Period matrices** of the canonical lift (ordinary case) [Mar21].
- with Caleb Springer [MS21]: every finite abelian group occur as the **group of points** of an ordinary AV over $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_5$.
- Magma implementations of the algorithms are on GitHub!
- Results of computations will appear on the LMFDB.

Summary

We group isogeny classes into:
square-free (SQ), pure-power (PP) and 'mixed' (eg. $E_1^2 \times E_2$).

		ordinary	$\mathbb{F}_p$ and no real roots	$\mathbb{F}_{p^k}$ or real roots
functor		[Del69]	[CS15]	[CS21] new!
isomorphism classes	SQ	[Mar21]		work in prog.
	PP	[Mar19] (Bass)		?
	mixed	?	?	?
polarizations	SQ	[How95]+[Mar21]	[BKM21]	?
	PP	[KNRR21] (E^r), [Mar19] (descr. but no algorithm)	?	?
	mixed	?	?	?

More comments:
- in [JKP$^+$18]: a functor for isogeny classes of the form E^r.
- in [OS20]+[BKM21]: almost-ordinary SQ with polarizations .
- in [CS21]: they use $\mathrm{Hom}_{\mathbb{F}_{p^k}}(-, A_w)$ as in [CS15], but A_w is more complicated.

[Bas63] Hyman Bass, *On the ubiquity of Gorenstein rings*, Math. Z. 82 (1963), 8–28. MR 0153708 (27 #3669)

[BKM21] Jonas Bergström, Valentijn Karemaker, and Stefano Marseglia, *Polarizations of Abelian Varieties Over Finite Fields via Canonical Liftings*, International Mathematics Research Notices (2021), rnab333.

[CCO14] Ching-Li Chai, Brian Conrad, and Frans Oort, *Complex multiplication and lifting problems*, Mathematical Surveys and Monographs, vol. 195, American Mathematical Society, Providence, RI, 2014. MR 3137398

[CS15] Tommaso Giorgio Centeleghe and Jakob Stix, *Categories of abelian varieties over finite fields, I: Abelian varieties over $\mathbb{F}_p$*, Algebra Number Theory 9 (2015), no. 1, 225–265. MR 3317765

[CS21] Tommaso Giorgio Centeleghe and Jakob Stix, *Categories of abelian varieties over finite fields II: Abelian varieties over finite fields and Morita equivalence*, arXiv e-prints (2021), arXiv:2112.14306.

[Del69] Pierre Deligne, *Variétés abéliennes ordinaires sur un corps fini*, Invent. Math. 8 (1969), 238–243. MR 0254059

[DTZ62] E. C. Dade, O. Taussky, and H. Zassenhaus, *On the theory of orders, in particular on the semigroup of ideal classes and genera of an order in an algebraic number field*, Math. Ann. 148 (1962), 31–64. MR 0140544 (25 #3962)

[Hon68] Taira Honda, *Isogeny classes of abelian varieties over finite fields*, J. Math. Soc. Japan 20 (1968), 83–95. MR 0229642

[How95] Everett W. Howe, *Principally polarized ordinary abelian varieties over finite fields*, Trans. Amer. Math. Soc. 347 (1995), no. 7, 2361–2401. MR 1297531

[HS20] Tommy Hofmann and Carlo Sircana, *On the computation of overorders*, Int. J. Number Theory 16 (2020), no. 4, 857–879. MR 4093387

[JKP+18] Bruce W. Jordan, Allan G. Keeton, Bjorn Poonen, Eric M. Rains, Nicholas Shepherd-Barron, and John T. Tate, *Abelian varieties isogenous to a power of an elliptic curve*, Compos. Math. 154 (2018), no. 5, 934–959. MR 3798590

[KNRR21] Markus Kirschmer, Fabien Narbonne, Christophe Ritzenthaler, and Damien Robert, *Spanning the isogeny class of a power of an elliptic curve*, Math. Comp. **91** (2021), no. 333, 401–449. MR 4350544

[Mar19] Stefano Marseglia, *Computing abelian varieties over finite fields isogenous to a power*, Res. Number Theory **5** (2019), no. 4, Paper No. 35, 17. MR 4030241

[Mar20a] Stefano Marseglia, *Computing base extensions of ordinary abelian varieties over finite fields*, arXiv:2003.09977, 2020.

[Mar20b] Stefano Marseglia, *Computing the ideal class monoid of an order*, J. Lond. Math. Soc. (2) **101** (2020), no. 3, 984–1007. MR 4111932

[Mar21] ______, *Computing square-free polarized abelian varieties over finite fields*, Math. Comp. **90** (2021), no. 328, 953–971. MR 4194169

[MS21] Stefano Marseglia and Caleb Springer, *Every finite abelian group is the group of rational points of an ordinary abelian variety over* $\mathbb{F}_2$, $\mathbb{F}_3$ *and* $\mathbb{F}_5$, arXiv e-prints (2021), arXiv:2105.08125.

[OS20] Abhishek Oswal and Ananth N. Shankar, *Almost ordinary abelian varieties over finite fields*, J. Lond. Math. Soc. (2) **101** (2020), no. 3, 923–937. MR 4111929

[Tat66] John Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. 2 (1966), 134–144. MR 0206004

Thank you!