Polarizations of abelian varieties over finite fields via canonical liftings

Stefano Marseglia

Utrecht University

KIAS Number Theory Seminar - 12 May 2022

joint work with

Jonas Bergström and **Valentijn Karemaker**.

Abelian Varieties

- An **abelian variety** A over a field k is a projective geometrically connected group variety over k.
  We have **morphisms** $\oplus : A \times A \to A$, $\ominus : A \to A$ and a k-rational point $e \in A(k)$ such that $(A, \oplus, \ominus, e)$ is a group object in the category of projective geom. connected varieties over k.
- In practice, we have diagrams $\rightsquigarrow$ **"natural" group structure** on $A(\overline{k})$.
- eg. ($\ominus$ is the "inverse" morphism)

$$\begin{tikzcd}
A \times_k A \arrow[rr, "(\ominus,\mathrm{id})"] & & A \times_k A \arrow[d, "\oplus"] \\
A \arrow[u, "\Delta"] \arrow[r] & \mathrm{Spec}(k) \arrow[r, "e"] & A
\end{tikzcd}
\qquad
\begin{tikzcd}
A \times_k A \arrow[rr, "(\mathrm{id},\ominus)"] & & A \times_k A \arrow[d, "\oplus"] \\
A \arrow[u, "\Delta"] \arrow[r] & \mathrm{Spec}(k) \arrow[r, "e"] & A
\end{tikzcd}$$

Example : $\dim A = 1$ elliptic curves

- AVs of dimension 1 are called **elliptic curves**.
- They admit a plane model: if $\operatorname{char} k \neq 2, 3$

$$Y^2 Z = X^3 + AXZ^2 + BZ^3 \quad A, B \in k \text{ and } e = [0:1:0]$$

- The groups law is explicit:
  if $P = (x_P, y_P)$ then $\ominus P = (x_P, -y_P)$ and
  if $Q = (x_Q, y_Q) \neq \ominus P$ then $P \oplus Q = (x_R, y_R)$ where

$$x_R = \lambda^2 - x_P - x_Q, \quad y_R = y_P + \lambda(x_R - x_P),$$

  where

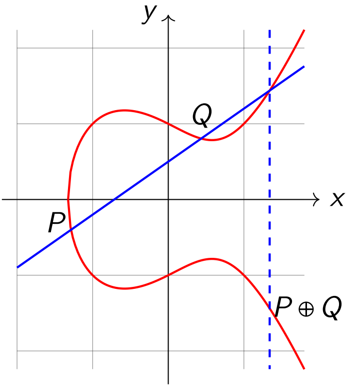
$$\lambda = \begin{cases} \frac{3x_P^2 + B}{2A} & \text{if } P = Q \\ \frac{y_P - y_Q}{x_P - x_Q} & \text{if } P \neq Q \end{cases}$$

Example : EC over $\mathbb{R}$

Over $\mathbb{R}$:
consider the abelian variety:

$$y^2 = x^3 - x + 1$$

Addition law: $P, Q \rightsquigarrow P \oplus Q$



Duals and Polarizations

- A hom. $\varphi : A \to B$ is an **isogeny** if $\dim A = \dim B$ and φ is surjective.
- Isogenies have finite kernel: $\deg \varphi = \mathrm{rank}(\ker(\varphi))$
- Pic^0_A is also an AV, called the **dual** of A and denoted $A^\vee$.
- An isogeny $\mu : A \to A^\vee$ (over k) is called a **polarization** if there are an $k \subseteq k'$ and an ample line bundle $\mathscr{L}$ such that (on points)

$$\varphi_{k'} : x \mapsto [t_x^* \mathscr{L} \otimes \mathscr{L}^{-1}].$$

- A polarization μ is **principal** if $\deg \mu = 1 \iff \mu$ is an isomorphism.
- Why do we care about polarizations?
  1. $\mathrm{Aut}(A, \mu)$ is finite $\rightsquigarrow$ moduli space $\mathscr{A}_{g,d}$
  2. proper smooth curve $C/k \rightsquigarrow \mathrm{Pic}^0_C =: \mathrm{Jac}(C)$ a PPAV.

$\mathbb{C}$ vs $\mathbb{F}_q$

- Pick $A/\mathbb{C}$ of dimension g.
- $A(\mathbb{C}) \simeq V := \mathbb{C}^g/\Lambda$, where $\Lambda \simeq_{\mathbb{Z}} \mathbb{Z}^{2g}$. It is a torus.
- V admits a non-degenerate **Riemann form** $\longleftrightarrow$ polarization.
- Actually,

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

  induced by $A \mapsto A(\mathbb{C})$ is an equivalence of categories.
- In char. $p > 0$ such an equivalence cannot exist : there are (supersingular) elliptic curves with quaternionic endomorphism algebras.

Canonical Liftings

- Let A_0 be an abelian variety over $\mathbb{F}_q$ of dim g.

Definition

A **canonical lifting** of A_0 is an abelian scheme over a normal local domain $\mathscr{R}$ of characteristic zero with residue field $\mathbb{F}_q$ with:

1. special fiber A_0, and
2. general fiber $\mathscr{A}_{\mathrm{can}}$ satisfying $\mathrm{End}(\mathscr{A}_{\mathrm{can}}) = \mathrm{End}(A_0)$.

- A_0 comes with a Frobenius endomorphism induced by $x \mapsto x^q$ on coordinates rings (we are in $\mathrm{char}(\mathbb{F}_q) = p > 0$!)
- Example: ordinary abelian variety; almost-ordinary abelian variety (with commutative $\mathbb{F}_q$-endomorphism algebra).
- Non-example: supersingular EC with quaternionic end. algebra.

Complex Uniformization

- Assume that A_0 admits a canonical lifting $\mathscr{A}_{\mathrm{can}}$.
- Fix $\mathscr{R} \hookrightarrow \mathbb{C}$ and put $A_{\mathrm{can}} := \mathscr{A}_{\mathrm{can}} \otimes \mathbb{C}$.
- A_{can} has morphisms F (and $V = \frac{q}{F}$) reducing to Frobenius (and Verschiebung).
- By **complex uniformization**:

$$A_{\mathrm{can}}(\mathbb{C}) \simeq {}^{\mathbb{C}^g} \big/ {}_{\Phi(I)}$$

- I : a fractional $\mathbb{Z}[F,V]$-ideal in $L := \mathbb{Q}[F]$,
- Φ : a **CM-type** of L (g maps $L \to \mathbb{C}$, one per conjugate pair).

- Define $\mathscr{H}(A_{\mathrm{can}}) := I$.
- By the same construction:

$$\begin{tikzcd} \text{char.0}: & \mathscr{A}_{\mathrm{can}}^{\vee} \arrow[r, "\otimes\mathbb{C}"] & A_{\mathrm{can}}^{\vee} \arrow[r, "\mathscr{H}"] & \bar{I}^{t} = \{\bar{x} : \mathrm{Tr}_{L/\mathbb{Q}}(xI) \subseteq \mathbb{Z}\} \\ \mathbb{F}_q : A_0^{\vee} \arrow[ur] & & & \end{tikzcd}$$

- In particular: $\mathscr{H}(\mathrm{Hom}(A_{\mathrm{can}}, A_{\mathrm{can}}^{\vee})) = (\bar{I}^{t} : I) = \left\{x \in L : xI \subseteq \bar{I}^{t}\right\}$.

- We have:

$$A_{\mathrm{can}}(\mathbb{C}) \simeq {}^{\mathbb{C}^g}\!\big/_{\Phi(I)}, \quad A^{\vee}_{\mathrm{can}}(\mathbb{C}) \simeq {}^{\mathbb{C}^g}\!\big/_{\Phi(\bar{I}^t)},$$

$$\mathscr{H}(\mathrm{Hom}(A_{\mathrm{can}}, A^{\vee}_{\mathrm{can}})) = (\bar{I}^t : I).$$

- What about **polarizations**? We understand them over $\mathbb{C}$!
- Let $\mu : A_{\mathrm{can}} \to A^{\vee}_{\mathrm{can}}$ an isogeny. Then μ is a polarization if and only if $\lambda := \mathscr{H}(\mu) \in (\bar{I}^t : I)$ satisfies
  1. $\lambda = -\bar{\lambda}$ (totally imaginary), and
  2. for every $\varphi \in \Phi$ we have $Im(\varphi(\lambda)) > 0$ (Φ-positive).

Isogeny classification over $\mathbb{F}_q$

- The Frobenius endomorphism $A/\mathbb{F}_q$ comes 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, the association

$$A \longmapsto h_A(x)$$

  is injective up-to-isogeny and allows us to list all isogeny classes.
- One can prove that $h_A(x)$ is squarefree $\iff$ $\mathrm{End}(A)$ is commutative.

Isomorphism classification over $\mathbb{F}_p$

Theorem (Centeleghe-Stix)

Let $\mathrm{AV}_h(p)$ *be the isogeny class over the* **prime field** $\mathbb{F}_p$ *determined by a* **squarefree** *characteristic polynomial of Frobenius* h*.*
Let $L = \mathbb{Q}[x]/h = \mathbb{Q}[F]$ *be the endomorphism algebra, and put* $V = p/F$*.*
There is an equivalence of categories:

$$\mathrm{AV}_h(p) \xrightarrow{\mathscr{G}} \{\textit{fractional } \mathbb{Z}[F,V]\textit{-ideals in } L\}.$$

- Let A_h be an AV in $\mathrm{AV}_h(p)$ with $\mathrm{End}(A_h) = \mathbb{Z}[F,V]$.
- The functor $\mathscr{G}(-) := \mathrm{Hom}(-, A_h)$ induces the equivalence.
- We can **choose** A_h so that for every $B_0 \in \mathrm{AV}_h(p)$:

$$\mathscr{G}(B_0^\vee) = \overline{\mathscr{G}(B_0)}^t \text{ and } \mathscr{G}(f^\vee) = \overline{\mathscr{G}(f)}, \text{ for any } f : B_0 \to B_0' \text{ in } \mathrm{AV}_h(p).$$

- In particular:
$$\mathscr{G}(\mathrm{Hom}(B_0, B_0^\vee)) = (\mathscr{G}(B_0) : \overline{\mathscr{G}(B_0)}^t).$$

Comparison

- Assume that A_0 admits a canonical lifting A_{can}.
- We have two description using fractional ideals. Let's compare them.
- Let $f : A_0 \to B_0$ be an isogeny.

$$\begin{tikzcd}
 & \mathrm{Hom}(A_{\mathrm{can}}, A_{\mathrm{can}}^\vee) \arrow[d, "\mathrm{red}"] \arrow[dr, "\text{complex unif.}"] & \\
\mathrm{Hom}(B_0, B_0^\vee) \arrow[r, "f^* := f^\vee \circ - \circ f"] \arrow[d, "\mathscr{G}"] & \mathrm{Hom}(A_0, A_0^\vee) \arrow[d, "\mathscr{G}"] & (\overline{I}^t : I) \arrow[d, "\cdot\alpha"', "\substack{\text{tot. real } (\alpha=\overline{\alpha}) \\ \text{unit in } \mathrm{End}(A_0)}"] \\
(\mathscr{G}(B_0) : \overline{\mathscr{G}(B_0)}^t) \arrow[r, "\mathscr{G}(f^*)"] & (\mathscr{G}(A_0) : \overline{\mathscr{G}(A_0)}^t) \arrow[r, equal] & (\overline{I}^t : I)
\end{tikzcd}$$

- f^* sends polarizations to polarizations.
- $\mathscr{G}(f^*) = \overline{\mathscr{G}(f)}\mathscr{G}(f)$ is a totally positive element:
  it sends totally imaginary elements to totally imaginary elements and Φ-positive elements to Φ-positive elements.

Comparison : Polarizations

we WANT to understand pols. here

we DO understand pols. here

$$
\begin{tikzcd}
 & & \mathrm{Hom}(A_{\mathrm{can}}, A_{\mathrm{can}}^\vee) \arrow[d, "\mathrm{red}"] \arrow[drr] & & \\
\mu \in & \mathrm{Hom}(B_0, B_0^\vee) \arrow[r, "f^*:=f^\vee\circ - \circ f"] \arrow[d, "\mathscr{G}"] & \mathrm{Hom}(A_0, A_0^\vee) \arrow[d, "\mathscr{G}"] & & (\bar{I}^t : I) \ni \alpha^{-1}\mathscr{G}(f^*)\mathscr{G}(\mu) \arrow[d, "\cdot\alpha"'] \\
 & (\mathscr{G}(B_0) : \overline{\mathscr{G}(B_0)}^t) \arrow[r, "\mathscr{G}(f^*)"] & (\mathscr{G}(A_0) : \overline{\mathscr{G}(A_0)}^t) \arrow[rr, equal] & & (\bar{I}^t : I)
\end{tikzcd}
$$

By chasing the diagram, we get:

Theorem ("lift and spread")

Let $\mu : B_0 \to B_0^\vee$ be an isogeny. Then

$$\mu \text{ is a } \textit{polarization} \iff \alpha^{-1}\mathscr{G}(\mu) \text{ is totally imaginary and } \Phi\text{-positive}$$

Principal Polarizations up to isomorphism

- Let $B_0 \in \mathrm{AV}_h(p)$. Put $T = \mathrm{End}(B_0)$ and $\mathscr{G}(B_0) = J$.
- Assume that $B_0 \simeq B_0^\vee$, i.e. $J = i_0 \overline{J}^t$ for some $i_0 \in L^*$.
- If μ and μ' are principal polarizations of B_0 then $(B_0, \mu) \simeq (B_0, \mu')$ (as PPAVs) if and only if there is $v \in T^*$ such that $\mathscr{G}(\mu) = v\overline{v}\mathscr{G}(\mu')$.
- Let $\mathscr{T}$ be a transversal of $T^* / < v\overline{v} : v \in T^* >$.
- Then

$$\mathscr{P}_\Phi^\alpha(J) := \{ i_0 \cdot u : u \in \mathscr{T} \text{ s.t. } \alpha^{-1} i_0 u \text{ is tot. imaginary and } \Phi\text{-positive} \}$$

  is a set or representatives of the PPs of B_0 up to isomorphism.
- It depends on α!

Effective Results : when can we ignore α?

Assume A_0 admits a canonical lifting. Put $S := \mathrm{End}(A_0)$
Let B_0 be isogenous to A_0. Put $T = \mathrm{End}(B_0)$.

Theorem (1)

Denote by $S^*_{\mathbb{R}}$ (resp. $T^*_{\mathbb{R}}$) the group of totally real units of S (resp. T). If $S^*_{\mathbb{R}} \subseteq T^*_{\mathbb{R}}$, then the set

$$\mathscr{P}^{\alpha}_{\Phi}(J) := \{ i_0 \cdot u : u \in \mathscr{T} \text{ s.t. } \alpha^{-1} i_0 u \text{ is tot. imaginary and } \Phi\text{-positive} \}$$

is in bijection with the set (which does not depend on α!)

$$\mathscr{P}^{1}_{\Phi}(J) = \{ i_0 \cdot u : u \in \mathscr{T} \text{ such that } i_0 u \text{ is totally imaginary and } \Phi\text{-positive} \}.$$

Corollary

If $S = \mathbb{Z}[F, V]$ (eg. $\mathrm{AV}_h(p)$ is ordinary or almost-ordinary) then we can ignore α. We recover Deligne+Howe and Oswal-Shankar

We run computations over all squarefree isogeny classes over small prime fields of dim 2,3 and 4. For example:

squarefree dimension 3			$p = 2$	$p = 3$	$p = 5$	$p = 7$
total			185	621	2863	7847
ordinary			82	390	2280	6700
almost ordinary			58	170	474	996
p-rank 1	cannot lift		0	0	0	0
	can lift	Thm 1 yes	20	26	76	118
		Thm 1 no	4	16	12	8
p-rank 0	cannot lift		0	3	2	1
	can lift	Thm 1 yes	20	15	17	23
		Thm 1 no	1	1	2	1

Among the 45 isogeny classes which we cannot 'handle' with Thm 1, we can compute the number of PPAV for 32 of them using Thm 2. For the remaining 13 (all over $\mathbb{F}_2$ and $\mathbb{F}_3$) we only get partial info.

Thank you!

Effective Results II

Theorem (2)

Assume that there are r isomorphism classes of abelian varieties in $\mathrm{AV}_h(p)$ with endomorphism ring T, represented under $\mathscr{G}$ by the fractional ideals $I_1,\ldots,I_r$. For any CM-type Φ', we put

$$\mathscr{P}^1_{\Phi'}(I_i) = \{ i_0 \cdot u : u \in \mathscr{T} \text{ such that } i_0 u \text{ is totally imaginary and } \Phi'\text{-positive} \}.$$

If there exists a non-negative integer N such that for every CM-type Φ' we have

$$|\mathscr{P}^1_{\Phi'}(I_1)| + \ldots + |\mathscr{P}^1_{\Phi'}(I_r)| = N$$

then there are exactly N isomorphism classes of principally polarized abelian varieties with endomorphism ring T.

Effective Results II

Proof.

- Consider the association $\Phi' \mapsto b$ where $b \in L^*$ is tot. imaginary and Φ'-positive.
- We can go back: for every b tot. imaginary there exists a unique CM-type Φ_b s.t. b is Φ_b-positive.
- Hence the totally real elements of L^* acts on the set of CM-types.
- If $\Phi = \Phi_b$ is the CM-type for which we have a canonical lift (as before) then $\mathscr{P}^{\alpha}_{\Phi_b}(I_i) \longleftrightarrow \mathscr{P}^{1}_{\Phi_{\alpha b}}(I_i)$.
- If the we get the 'same sum' (over the I_i's) for every CM-type we know that the result must be the correct one!

□

Note: even if the sum is not the same for all Φ''s then we know that one of the outputs is the correct one!

When can we lift up to isogeny?

Definition (Chai-Conrad-Oort)

Let Φ be a p-adic CM-type for a CM-field $L = \mathbb{Q}(F)$. The pair (L,Φ) satisfies the Residual Reflex Condition *w.r.t. F if the following conditions are met:*

1. *The* **Shimura-Taniyama formula** *holds for F: for every place v of L above p, we have*

$$\frac{\mathrm{ord}_v(F)}{\mathrm{ord}_v(q)} = \frac{\#\{\varphi\in\Phi \text{ s.t. } \varphi \text{ induces } v\}}{[L_v:\mathbb{Q}_p]}.$$

2. *Let E be the reflex field attached to (L,Φ), and let v be the induced p-adic place of E. Then the* **residue field** *k_v of $\mathcal{O}_{E,v}$ can be realized as a* **subfield** *of $\mathbb{F}_q$.*

When can we lift up to isogeny?

Theorem (Chai-Conrad-Oort)

Assume that (L,Φ) satisfies the **Residual Reflex Condition** *w.r.t. F, that is,*

1. *Φ satisfies the Shimura-Taniyama formula for F, and*
2. *the reflex field E has residue field $k_E \subseteq \mathbb{F}_q$.*

Then we can canonically lift an abelian variety A_0 with $\mathcal{O}_L = \mathrm{End}(A_0)$.

- If there is a separable isogeny $A_0 \to A_0'$ then A_0' admits a canonical lifting (useful in combination with Thm 1).

squarefree dimension 4			$p=2$	$p=3$
total			1431	10453
ordinary			656	6742
almost ordinary			392	2506
p-rank 2	cannot lift		0	0
	can lift	Thm 1 yes	149	500
		Thm 1 no	49	312
p-rank 1	cannot lift		6	36
	can lift	Thm 1 yes	80	184
		Thm 1 no	14	40
p-rank 0	cannot lift		3	6
	can lift	Thm 1 yes	73	88
		Thm 1 no	9	39

Thm 1 ($S_{\mathbb{R}}^* \subseteq T_{\mathbb{R}}^*$) doesn't handle $72/\mathbb{F}_2$ and $391/\mathbb{F}_3$. Out of these, we can use Thm 2 for $20/\mathbb{F}_2$ and $214/\mathbb{F}_3$. For the remaining $52/\mathbb{F}_2$ and $171/\mathbb{F}_3$ we can only get information about certain endomorphism rings (723 out of 946 and 3481 out of 4636, respectively). Also there are $9/\mathbb{F}_3$ for which the computations of the isomorphism classes of unpolarized abelian varieties is not over yet.