Polarizations of abelian varieties over finite fields via canonical liftings

Stefano Marseglia

Utrecht University

SU Wednesday Zoom - 21 April 2021

joint work with

Jonas Bergström (SU) and Valentijn Karemaker (UU).

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 $\operatorname{char} k \neq 2,3$

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

- 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

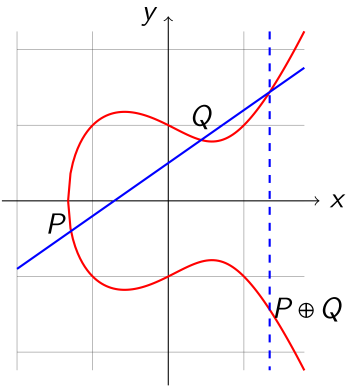
$$\lambda = \begin{cases} \frac{3x_P^2+B}{2A} & \text{if } P = Q \\ \frac{y_P-y_Q}{x_P-x_Q} & \text{if } P \neq Q \end{cases}$$

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 ker.
- Put $\deg \varphi = \mathrm{rank} \ker(\varphi)$.
- 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.
- Moreover, V admits a non-degenerate Riemann form $\longleftrightarrow$ polarization.
- Actually,

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

  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.

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, the association

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

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

Canonical Liftings

- Pick $A_0/\mathbb{F}_q$ of dim g.
- A canonical lifting of A_0 is an abelian scheme $\mathscr{A}$ over a local domain $\mathscr{R}$ of char. zero with residue field $\mathbb{F}_q$ such that $\mathscr{A}\otimes\mathbb{F}_q \simeq A_0$ and $\mathrm{End}(\mathscr{A}) = \mathrm{End}(A_0)$.
- If $\mathscr{R}$ is normal then $\mathrm{End}(\mathscr{A}) = \mathrm{End}(A)$, where $A = \mathscr{A}\otimes Q(\mathscr{R})$.
- For $A_0/\mathbb{F}_q$ of dim g, there is $0 \le f \le g$ (p-rank) such that $|A_0[p](\overline{\mathbb{F}}_p)| = p^f$.
- If $f = g$ then A_0 is ordinary and admits a canonical lifting to the ring of Witt vectors $W(\mathbb{F}_q)$.
- If $f = g-1$ then A_0 is almost-ordinary. If $\mathrm{End}(A_0)$ is commutative, A_0 admits a canonical lifting to a quadratic extension of $W(\mathbb{F}_q)$.
- In general, no canonical lifting: eg. supersingular elliptic curves (quaternions).

Complex Multiplication

- Let A_0 be an AV over $\mathbb{F}_q$ of dim g, with h_{A_0} squarefree.
- Put $L = \mathbb{Q}[F] = \mathbb{Q}[x]/h_{A_0}$ and $V = q/F$.
- L has an involution: $F \mapsto \overline{F} = V$.
- Also $\mathbb{Z}[F, V] \hookrightarrow \mathrm{End}(A_0)$...
- ... i.e. $\mathrm{End}(A_0) \otimes \mathbb{Q}$ contains a CM-algebra L of degree $[L : \mathbb{Q}] = 2g$.
- We say that AVs over $\mathbb{F}_q$ have Complex Multiplication (CM).

Complex Multiplication II

- A CM-type Φ of L is a choice of g homs $L \to \overline{\mathbb{Q}}$, one per each conjugate pair:
$$\mathrm{Hom}(L, \overline{\mathbb{Q}}) = \Phi \sqcup \overline{\Phi}.$$

- The reflex field E of (L, Φ) is the num. field s.t. $\mathrm{Gal}(\overline{\mathbb{Q}}/E)$ stabilizes Φ.
- If L is a field :
$$E = \mathbb{Q}\left(\sum_{\varphi \in \Phi} \varphi(\alpha) : \alpha \in L\right).$$

- Fix once and for all
$$\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p \simeq \mathbb{C}$$
so that we can talk about and identify p-adic and complex CM-types and reflex fields (with the completion).

Residual Reflex Condition (RRC)

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 RRC 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 $\mathbb{F}_q$.*

Theorem (Chai-Conrad-Oort)

Fix an isogeny class over $\mathbb{F}_q$ with CM by $L = \mathbb{Q}(F)$ through Φ determined by an irreducible characteristic polynomial of Frobenius h. Assume (L,Φ) satisfies RRC w.r.t. F. Then this isogeny class contains an abelian variety $A_0/\mathbb{F}_q$ such that $\mathscr{O}_L = \mathrm{End}(A_0)$ which has a canonical lifting A over a number field E' (a finite extension of the reflex field E of (L,Φ)).

- Can generalize: h irreducible $\rightsquigarrow$ h squarefree.
- Define $\mathscr{S}_\Phi$ as the set of orders S in L s.t. S is Gorenstein, $S = \overline{S}$ and there is in the isogeny class an A_0' with $S = \mathrm{End}(A_0')$ admitting a canonical lifting.
- By the Theorem: if (L,Φ) satisfies RRC then $\mathscr{O}_L \in \mathscr{S}_\Phi$.
- Also: if $\mathrm{End}(A_0) = \mathscr{O}_L$ and there is a separable isogeny $A_0 \to A_0'$ then $\mathrm{End}(A_0') \in \mathscr{S}_\Phi$.
- From now on we assume that $\mathscr{S}_\Phi \neq \emptyset$.

Complex Uniformization

- Let A be the canonical lifting of A_0.
- $A^\vee$ is the (canonical) lifting of $A_0^\vee$.
- Then $A(\mathbb{C}) \simeq \mathbb{C}^g/\Phi(I)$ (vector notation), for a fractional $\mathbb{Z}[F,V]$-ideal I in L.
- Define $\mathscr{H}(A) := I$.
- We have $\mathscr{H}(A^\vee) = \bar{I}^t = \{\bar{x} : \mathrm{Tr}_{L/\mathbb{Q}}(xI) \subseteq \mathbb{Z}\}$.
- In particular $\mathscr{H}(\mathrm{Hom}(A, A^\vee)) = (\bar{I}^t : I) = \left\{ x \in L : xI \subseteq \bar{I}^t \right\}$.

Centeleghe-Stix I : the functor

Theorem (Centeleghe-Stix)

Let $\mathrm{AV}_h(p)$ be the isogeny class over the prime field $\mathbb{F}_p$ determined by a squarefree h. Put $L = \mathbb{Q}[x]/h = \mathbb{Q}[F]$ and $V = p/F$. There is an equivalence of categories between $\mathrm{AV}_h(p)$ and the category of fractional $\mathbb{Z}[F,V]$-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.
- C-S prove that one can choose A_h in such a way that functors 'glue' together and form an equivalence from the category of AVs$/\mathbb{F}_p$ with no real roots and the category of free f.g. $\mathbb{Z}$-modules with a Frobenius-like endomorphism.

Centeleghe-Stix II : choices and duality

- In general one can prove that there exists an invertible $\mathbb{Z}[F,V]$-ideal H such that for any $B_0 \in \mathrm{AV}_h(p)$ we have $\mathscr{G}(B_0^\vee) = H\overline{\mathscr{G}(B_0)}^t$.
- Hence $\mathscr{G}(\mathrm{Hom}(B_0, B_0^\vee) = H\overline{H}(\mathscr{G}(B_0) : \overline{\mathscr{G}(B_0)}^t)$.
- The functor $\mathscr{G}$ depends on the choice of A_h with minimal End.
- More precisely there is an action of $\mathrm{Pic}(\mathbb{Z}[F,V])$ on such AVs.
- Therefore we can 'modify' $\mathscr{G}$ to obtain $\mathscr{G}(B_0^\vee) = \overline{\mathscr{G}(B_0)}^t$
- Hence
$$\mathscr{G}(\mathrm{Hom}(B_0, B_0^\vee)) = (\mathscr{G}(B_0) : \overline{\mathscr{G}(B_0)}^t),$$
- and that $\mathscr{G}(f^\vee) = \overline{\mathscr{G}(f)}$, for any $f : B_0 \to B_0'$.

Comparison I : Hom's

Proposition

Let $A_0 \in \mathrm{AV}_h(p)$ such that $S = \mathrm{End}(A_0) \in \mathscr{S}_\Phi$. In particular A_0 has a canonical lifting A. Then there exists a totally real $\alpha \in S^*$ such that the reduction map $\mathrm{Hom}_L(A, A^\vee) \to \mathrm{Hom}_L(A_0, A_0^\vee)$ *is multiplication by $\alpha \in S^*$.*

$$\begin{tikzcd}
\mathrm{Hom}(A, A^\vee) \arrow[d, "\mathrm{red}"'] \arrow[dr, "\mathscr{H}"] & \\
\mathrm{Hom}(A_0, A_0^\vee) \arrow[d, "\mathscr{G}"] & (\bar{I}^t : I) \arrow[d, "\alpha"'] \\
(\mathscr{G}(A_0) : \overline{\mathscr{G}(A_0)}^t) \arrow[r, equal] & (\bar{I}^t : I)
\end{tikzcd}$$

- In general $I = \mathscr{H}(A)$ is not $\mathscr{G}(A_0)$!
- But $(\bar{I}^t, I) = \mathscr{H}(\mathrm{Hom}(A, A^\vee))$ and $\mathscr{G}(\mathrm{Hom}(A_0, A_0^\vee))$ are the same ...
- ... and $\mathscr{G}(\mathrm{red}(f)) = \alpha\mathscr{H}(f)$.
- By the choices made above, $\mathscr{G}$ respects symmetric homomorphisms, that is, α is totally real $\alpha = \bar{\alpha}$.

Comparison II : Polarizations

- We understand polarizations over $\mathbb{C}$! Indeed:
- Let $\mu : A \to A^\vee$ an isogeny. Then μ is a polarization if and only if $\lambda := \mathscr{H}(\mu)$ satisfies
  1. $\lambda = -\overline{\lambda}$ (totally imaginary), and
  2. for every $\varphi \in \Phi$ we have $Im(\varphi(\lambda)) > 0$ (Φ-positive).

Theorem ("lift and spread")

Let $\mathrm{End}(A_0) = S \in \mathscr{S}_\Phi$ and $\alpha \in S^*$ totally real as above. For any abelian variety $B_0 \in \mathrm{AV}_h(p)$, and any isogeny $\mu : B_0 \to B_0^\vee$, the following are equivalent:

1. *The isogeny μ is a polarization of B_0;*
2. *The element $\alpha^{-1}\mathscr{G}(\mu) \in L$ is totally imaginary and Φ-positive.*

Moreover, we have $\deg \mu = \#(\mathscr{G}(B_0)/\mathscr{G}(\mu)\mathscr{G}(B_0^\vee))$.

Proof.

Let $f: A_0 \to B_0$ be an isogeny. Consider $f^* := f^\vee \circ - \circ f$:

$$\begin{tikzcd}
 & \mathrm{Hom}(A, A^\vee) \arrow[d, "\mathrm{red}"'] \arrow[dr, "\mathscr{H}"] & \\
\mathrm{Hom}(B_0, B_0^\vee) \arrow[r, "f^*"] \arrow[d, "\mathscr{G}"] & \mathrm{Hom}(A_0, A_0^\vee) \arrow[d, "\mathscr{G}"] & (\bar{I}^t : I) \arrow[d, "\alpha"'] \\
(\mathscr{G}(B_0) : \mathscr{G}(B_0^\vee)) \arrow[r, "\mathscr{G}(f^*)"] & (\mathscr{G}(A_0) : \mathscr{G}(A_0^\vee)) \arrow[r, equal] & (\bar{I}^t : I)
\end{tikzcd}$$

Note that $\mathscr{G}(f^*)$ is multiplication by the total real element $\overline{\mathscr{G}(f)}\mathscr{G}(f)$. So it sends totally imaginary elements to totally imaginary elements and Φ-positive elements to Φ-positive elements. □

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 transversal of $T^* / < v\overline{v} : v \in T^* >$.
- Then

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

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

Effective Results I

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

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

which does not depend on α.

Corollary

If $\mathbb{Z}[F, V] \in \mathscr{S}_{\Phi}$ (eg. $\mathrm{AV}_h(p)$ is ordinary or almost-ordinary) then we can ignore α.

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.

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!

$\square$

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!

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

<table>
<tr><td colspan="3">squarefree dimension 3</td><td>$p=2$</td><td>$p=3$</td><td>$p=5$</td><td>$p=7$</td></tr>
<tr><td colspan="3">total</td><td>185</td><td>621</td><td>2863</td><td>7847</td></tr>
<tr><td colspan="3">ordinary</td><td>82</td><td>390</td><td>2280</td><td>6700</td></tr>
<tr><td colspan="3">almost ordinary</td><td>58</td><td>170</td><td>474</td><td>996</td></tr>
<tr><td rowspan="3">p-rank 1</td><td colspan="2">no RRC</td><td>0</td><td>0</td><td>0</td><td>0</td></tr>
<tr><td rowspan="2">yes RRC</td><td>Thm 1 yes</td><td>20</td><td>26</td><td>76</td><td>118</td></tr>
<tr><td>Thm 1 no</td><td>4</td><td>16</td><td>12</td><td>8</td></tr>
<tr><td rowspan="3">p-rank 0</td><td colspan="2">no RRC</td><td>0</td><td>3</td><td>2</td><td>1</td></tr>
<tr><td rowspan="2">yes RRC</td><td>Thm 1 yes</td><td>20</td><td>15</td><td>17</td><td>23</td></tr>
<tr><td>Thm 1 no</td><td>1</td><td>1</td><td>2</td><td>1</td></tr>
</table>

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!