Polarisations of abelian varieties over finite fields via canonical liftings

arXiv 2101.05531, joint w/ J. Bergström & S. Marseglia

Definition An abelian variety is a non-singular connected projective group variety.

e.g. an elliptic curve

Definition The dual variety $A^\vee$ of an abelian variety A over K is such that $A^\vee(\bar{K}) = \mathrm{Pic}^0(A_{\bar{K}})$.

any field

e.g. for an elliptic curve E, $E^\vee \simeq E$.

Definition A polarisation of an abelian variety A is an isogeny $\mu: A \to A^\vee$ such that there exists an ample line bundle $\mathcal{L}$ on $A_{\bar{K}}$ such that $\mu_{\bar{K}} = \varphi_{\mathcal{L}}$,

where
$$\varphi_{\mathcal{L}}: A \to A^\vee$$
$$x \mapsto [t_x^* \mathcal{L} \otimes \mathcal{L}^{-1}]$$

$\Rightarrow$ So $\{\text{polarisations of } A\} \subseteq \mathrm{Hom}(A, A^\vee)$.

$\boxed{\text{Goal}}$ Describe and compute polarisations of AV's when $K = \mathbb{F}_q$.

§ Preliminaries: Complex Multiplication

<u>Definition</u> A CM-field $L/\mathbb{Q}$ is such that

$$\begin{array}{rcl} & L & \\ \deg 2 & | & \text{tot. imaginary} \\ & L' & \\ \deg g & | & \text{totally real} \\ & \mathbb{Q} & \end{array}$$

It has a canonical involution $x \mapsto \bar{x}$.

A CM-algebra is a finite product of CM-fields.

<u>Definition</u> An abelian variety A over k of dimension g has CM (by L) if $L \subseteq \mathrm{End}^\circ(A) := \mathrm{End}(A) \otimes \mathbb{Q}$.

<u>Fact</u> Every abelian variety over a finite field has CM.

<u>Definition</u> A CM-type for L is a subset $\Phi \subseteq \mathrm{Hom}(L, \bar{\mathbb{Q}})$ such that $\mathrm{Hom}(L, \bar{\mathbb{Q}}) = \Phi \sqcup \bar{\Phi}$.

We often say an abelian variety "has CM by (L, Φ)".

§ Polarisations in characteristic zero

Consider an abelian variety A over $\mathbb{C}$ of dimension g.

Complex uniformisation: $A(\mathbb{C}) \simeq \mathbb{C}^g/\Lambda$, $\Lambda \simeq_{\mathbb{Z}} \mathbb{Z}^{2g}$

When A has CM by (L, Φ), we can say more:

$\exists$ fractional ideal I in L s.t. $A(\mathbb{C}) \simeq \mathbb{C}^g/\Phi(I)$

Then also $A^\vee(\mathbb{C}) \simeq \mathbb{C}^g/\Phi(\bar{I}^t)$ ($\bar{I}^t$ involution, trace dual)

and hence $\mathrm{Hom}_L(A, A^\vee) \overset{1:1}{\longleftrightarrow} (\bar{I}^t : I) = \{x \in L : xI \subseteq \bar{I}^t\}$

Recall: $\{\text{polarisations of } A\} \subseteq \mathrm{Hom}(A, A^\vee)$.

Definition / construction: Let A be a g-dimensional abelian variety over a p-adic field K and with CM by (L, Φ).

Form $A_{\mathbb{C}} = A \otimes \mathbb{C}$; then $A_{\mathbb{C}}(\mathbb{C}) \simeq \mathbb{C}^g/\Phi(I)$.

write $\boxed{\mathscr{L}(A) := I}$.

Then $\mathscr{L}(A^\vee) = \bar{I}^t$ and

$$\mathscr{L}(\mathrm{Hom}_L(A, A^\vee)) = \mathrm{Hom}_L(\mathscr{L}(A), \mathscr{L}(A^\vee)) = (\bar{I}^t : I).$$

(well-defined up to L-isomorphism; we are free to choose an embedding into L)

§ Polarisations in characteristic zero

Have $\mathfrak{a}(A) = I$ and $\mathfrak{a}(\mathrm{Hom}(A, A^\vee)) = (\bar{I}^t : I)$.

<u>Proposition</u> Let A be a g-dimensional abelian variety over a p-adic field K and with CM by (L, Φ).

An L-linear isogeny $\mu : A \to A^\vee \in \mathrm{Hom}(A, A^\vee)$ is a polarisation if and only if:

- $\mathfrak{a}(\mu) = \lambda \in L$ is <u>totally imaginary</u> $(\bar{\lambda} = -\lambda)$
- λ is <u>Φ-positive</u> $(\mathrm{Im}(\varphi(\lambda)) > 0 \ \forall \varphi \in \Phi)$

$$\boxed{\begin{tikzcd} \mathrm{Hom}(A, A^\vee) \arrow[dr, "\mathfrak{a}"] & \\ & (\bar{I}^t : I) \end{tikzcd}}$$

§ (towards) polarisations in characteristic p

Goal Describe and compute polarisations of AV's when $K = \mathbb{F}_q$.

Every $A/\mathbb{F}_q$ has a Frobenius endomorphism π_A
which has a characteristic polynomial $h_A(x) \in \mathbb{Z}[x]$,
which is an isogeny invariant:
By Honda-Tate theory, $\{\text{isogeny classes}\} \xleftrightarrow{1:1} \{\text{charpoly's } h_A\}$

Idea Want analogous construction to $\mathbb{C}$ for AV's in char p
to describe $\mathrm{Hom}(A, A^\vee) \supseteq \{\text{polarisations of } A\}$

$\Rightarrow$ We use the Centeleghe-Stix equivalence.

For this, we need to restrict to:
Abelian varieties A_0 over $\mathbb{F}_p$ s.t. h_{A_0} is squarefree.

N.B. h_{A_0} squarefree $\Leftrightarrow$ $\mathrm{End}(A_0)$ commutative

C-S equivalence: Fix such an $h \xleftrightarrow{HT}$ isogeny class AV_h
Let $L := \mathbb{Q}[x]/(h) = \mathbb{Q}[F]$ and $V := p/F$.
Any $A_0 \in AV_h$ has $\mathrm{End}(A_0) \supseteq \mathbb{Z}[F, V]$.
Choose $A_h \in AV_h$ with $\mathrm{End}(A_h) = \mathbb{Z}[F, V]$

Then $\forall A_0 \in AV_h$, $\mathcal{G}$: $AV_h \longrightarrow \{\text{fractional } \mathbb{Z}[F,V]\text{-ideals}\}$
$A_0 \longmapsto \mathrm{Hom}(A_0, A_h)$, embedded into L

§ (towards) polarisations in characteristic p

Goal Describe and compute polarisations of AV's when $k = \mathbb{F}_p$

C-S equivalence: Choose $A_h \in AV_h$ with $\mathrm{End}(A_h) = \mathbb{Z}[F,V]$

Then $\forall A_0 \in AV_h$, $\mathcal{G}: AV_h \longrightarrow \{\text{fractional } \mathbb{Z}[F,V]\text{-ideals}\}$

$$A_0 \longmapsto \mathrm{Hom}(A_0, A_h) \text{, embedded into } L$$

There are some choices involved here:

- Choosing A_h; these form a $\mathrm{Pic}(\mathbb{Z}[F,V])$-orbit
- Choosing embedding into L

Choosing well, we can ensure that $\mathcal{G}(A_0^\vee) = \overline{\mathcal{G}(A_0)}^t$ and hence

$$\mathcal{G}(\mathrm{Hom}_L(A_0, A_0^\vee)) := (\mathcal{G}(A_0) : \mathcal{G}(A_0^\vee)) = (\mathcal{G}(A_0) : \overline{\mathcal{G}(A_0)}^t)$$

$$\left[\text{compare: } \mathcal{F}(\mathrm{Hom}(A, A^\vee)) = (\bar{I}^t : I)\right]$$

In particular, for $f: A_0 \to B_0$ and $f^\vee: B_0^\vee \to A_0^\vee$ we have $\mathcal{G}(f^\vee) = \overline{\mathcal{G}(f)}$.

$$\boxed{\begin{tikzcd} \mathrm{Hom}(B_0, B_0^\vee) \arrow[r, "f^*"] \arrow[d, "\mathcal{G}"'] & \mathrm{Hom}(A_0, A_0^\vee) \arrow[d, "\mathcal{G}"] & \\ (\mathcal{G}(B_0) : \mathcal{G}(B_0^\vee)) \arrow[r, "\mathcal{G}(f^*)"'] & (\mathcal{G}(A_0) : \mathcal{G}(A_0^\vee)) & = (\mathcal{G}(A_0) : \overline{\mathcal{G}(A_0)}^t) \end{tikzcd}}$$

where $f^*: \varphi \longmapsto f^\vee \circ \varphi \circ f$

so $\mathcal{G}(f^*)$ is multiplication with $\mathcal{G}(f)\overline{\mathcal{G}(f)}$ in L.

§ Characteristic p versus characteristic zero

Goal Describe and compute polarisations of AV's when $K = \mathbb{F}_p$

We now have $\mathcal{G}(\mathrm{Hom}(A_0, A_0^\vee)) \supset \mathcal{G}(\text{polarisations})$

$$\underset{(\mathcal{G}(A_0) : \overline{\mathcal{G}(A_0)}^t)}{\parallel} \qquad \underset{???}{\parallel}$$

Idea Lift to characteristic 0 to access description of polarisations.

N.B. $\mathrm{Hom}(A_0, A_0^\vee)$ should be preserved by the lifting process.

Definition A canonical lifting of $A_0/\mathbb{F}_q$ to a local domain $\mathcal{R}$ of characteristic 0 with residue field $\mathbb{F}_q$ and fraction field K is an abelian scheme $\mathcal{A}/\mathcal{R}$ such that $\mathrm{End}(A_0) = \mathrm{End}(\mathcal{A})$ and $\mathcal{A} \otimes \mathbb{F}_q \simeq A_0$, $\mathcal{A} \otimes K \simeq A$.

(Later, we will talk about when canonical liftings are known to exist.)

(N.B. Since $L \simeq \mathrm{End}^0(A_0)$ we may view $\mathrm{End}(A_0)$ as an order in L; we show these identifications can be made compatibly with $\mathcal{G}$ and $\mathcal{H}$.)

Moreover:

Proposition If $A_0/\mathbb{F}_q$ has a canonical lifting to A/K, or equivalently if A/K with CM by L has good reduction to $A_0/\mathbb{F}_q$, and if $\mathrm{End}(A_0) \simeq \mathrm{End}(A_0^\vee)$ $(= \overline{\mathrm{End}(A_0)})$ or equivalently if $\mathrm{End}(A) \simeq \mathrm{End}(A^\vee)$ $(= \overline{\mathrm{End}(A)})$ [with $\mathrm{End}(A_0) \simeq \mathrm{End}(A)$ and $\mathrm{End}(A_0^\vee) \simeq \mathrm{End}(A^\vee)$]

and if "$\mathrm{End}(A_0) \simeq \mathrm{End}(A)$ is Gorenstein",

then the reduction map $\mathrm{Hom}_L(A, A^\vee) \longrightarrow \mathrm{Hom}_L(A_0, A_0^\vee)$ is multiplication by $\alpha \in \mathrm{End}(A_0)^*$.

§ Characteristic p versus characteristic zero

Goal Describe and compute polarisations of AV's when $K = \mathbb{F}_p$

Let A be an abelian variety over a p-adic field K with CM by (L, Φ) with good reduction to $A_0/\mathbb{F}_p \in AV_h$,
where h is squarefree and has no real roots, and $L \simeq \mathbb{Q}[x]/(h)$,
such that $\mathrm{End}(A_0) = \mathrm{End}(A) = (I:I) = S$ is Gorenstein and satisfies $S = \bar{S}$.
Then we can make compatible choices to obtain

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

Also:

Lemma Let $f: A_0 \to B_0$ and $\mu_0: B_0 \to B_0^\vee$ be isogenies.
Then μ_0 is a polarisation $\Longleftrightarrow$ $f^*\mu_0 = f^\vee \circ \mu_0 \circ f$ is a polarisation

Lemma Let $\mu: A \to A^\vee$ be an isogeny and $\mu_0: A_0 \to A_0^\vee$ its reduction.
Then μ is a polarisation $\Longleftrightarrow$ μ_0 is a polarisation.

Lemma The element $\alpha \in S^*$ is totally real: $\alpha = \bar{\alpha}$.

§ Characteristic p versus characteristic zero

Goal Describe and compute polarisations of AV's when $K = \mathbb{F}_p$

Reformulating the above, we can now describe $\{\text{polarisations}\} \subseteq \mathrm{Hom}(A_0, A_0^\vee)$!

Theorem Let h be a squarefree char. poly. without real roots corresponding to the isogeny class AV_h over $\mathbb{F}_p$.
Let $L \simeq \mathbb{Q}[x]/(h)$ and choose a CM-type Φ for L.
Let $S = \bar{S}$ be a Gorenstein order in L such that $\exists A_0 \in AV_h$ with $\mathrm{End}(A_0) = S$ which admits a canonical lifting to a p-adic field K.

Then there exists a totally real $\alpha \in S^*$ such that for <u>any</u> $B_0 \in AV_h$ and any isogeny $\mu_0 : B_0 \to B_0^\vee$,

μ_0 is a polarisation $\iff \alpha^{-1}\mathcal{G}(\mu) \in L$ is totally imaginary and Φ-positive.

$$\begin{tikzcd}
 & \underset{\mathrm{Hom}(A, A^\vee)}{\mathrm{red}^{-1}(f^*\mu) \in} \arrow[d, "\mathrm{red}"] \arrow[dr, "\mathcal{H}"] & \\
\underset{\mathrm{Hom}(B_0, B_0^\vee)}{\mu \in} \arrow[r, "f^*"] \arrow[d, "\mathcal{G}"'] & \underset{\mathrm{Hom}(A_0, A_0^\vee)}{f^*\mu \in} \arrow[d, "\mathcal{G}"] & \underset{(\bar{I}^t : I)}{\mathcal{H}(\mathrm{red}^{-1}(f^*\mu)) = \frac{1}{\alpha}\mathcal{G}(f^*\mu) \in} \arrow[d, "\alpha"] \\
(\mathcal{G}(B_0) : \mathcal{G}(B_0^\vee)) \arrow[r, "\mathcal{G}(f^*)"'] & \underset{\mathcal{G}(f^*\mu)}{(\mathcal{G}(A_0) : \mathcal{G}(A_0^\vee)) \ni} & \underset{\mathcal{G}(f^*\mu)}{= (\bar{I}^t : I) \ni}
\end{tikzcd}$$

[Recall: $\mathcal{G}(f^*\mu) = \mathcal{G}(f)\overline{\mathcal{G}(f)}\mathcal{G}(\mu)$]

§ When do canonical liftings exist?

Definition A canonical lifting of $A_0/\mathbb{F}_q$ to a local domain $\mathcal{R}$ of characteristic 0 with residue field $\mathbb{F}_q$ and fraction field K is an abelian scheme $\mathcal{A}/\mathcal{R}$ such that $\mathrm{End}(A_0) = \mathrm{End}(\mathcal{A})$ and
$$\mathcal{A} \otimes \mathbb{F}_q \simeq A_0, \quad \mathcal{A} \otimes K \simeq A.$$

Proposition 1) (Serre-Tate) Every ordinary AV has a canonical lifting.

2) (Oswal-Shankar (& BKM)) Every almost-ordinary AV with commutative End has a canonical lifting

Theorem (Chai-Conrad-Oort)
Let h be an irreducible char. poly, $L = \mathbb{Q}[x]/(h) = \mathbb{Q}(\pi)$, and Φ a CM-type of L, such that (L, Φ) satisfies the

residual reflex condition (RRC):

a) (Shimura-Taniyama formula) For every v of L above p,
$$\frac{\mathrm{ord}_v(\pi)}{\mathrm{ord}_v(q)} = \frac{\#\{\varphi \in \Phi : \varphi \text{ induces } v\}}{[L_v : \mathbb{Q}_p]}$$

b) Let $E = \mathbb{Q}\left(\sum_{\varphi \in \Phi} \varphi(\alpha) : \alpha \in L\right)$ be the reflex field of (L, Φ) with induced p-adic place v. Then the residue field k_v of $\mathcal{O}_{E,v}$ satisfies $k_v \subseteq \mathbb{F}_q$.

Then the isogeny class corresponding to h contains an AV $A_0/\mathbb{F}_q$ s.t. $\mathrm{End}(A_0) = \mathcal{O}_L$ which has a canonical lifting.

Remarks
- We generalised this to h squarefree
- Any AV separably isogenous to A_0 then also has a canonical lifting
- We implemented the (generalised) RRC in Magma

§ Computations of polarisations

Theorem (under a bunch of assumptions...)
... there exists a totally real $\alpha \in S^*$ such that for <u>any</u> $B_0 \in AV_h$ and any isogeny $\mu_0 : B_0 \to B_0^\vee$,

μ_0 is a polarisation $\iff \alpha^{-1}\mathcal{G}(\mu_0) \in L$ is totally imaginary and Φ-positive.

Lemma $(B_0, \mu_0) \simeq (B_0, \mu_0') \iff \exists v \in \mathrm{End}(B_0)^* \text{ s.t. } \mathcal{G}(\mu_0) = v\bar{v}\,\mathcal{G}(\mu_0')$

So to find all (principal) polarisations of B_0, starting with a given $\mathcal{G}(\mu_0) = i_0 \in L^*$, we need to compute

$$\{ i_0 \cdot u : u \in \mathrm{End}(B_0)^* / \langle v\bar{v} \rangle \text{ s.t. } \alpha^{-1} i_0 \cdot u \text{ is totally imaginary \& } \Phi\text{-positive} \}$$

In practice, we can often ignore α!

This happens e.g. when an AV with $\mathrm{End} = \mathbb{Z}[F, V]$ lifts, like for (almost)-ordinary.

We also implemented the above in Magma.
Aggregate examples for dimensions 2, 3, 4:

squarefree dimension 2			$p=2$	$p=3$	$p=5$	$p=7$
total			29	55	119	195
ordinary			14	36	94	168
almost ordinary			8	14	20	24
p-rank 0	no RRC		0	0	0	0
	yes RRC	5.5.2(R_w) yes	6	2	5	3
		5.5.2(R_w) no	1	3	0	0

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	no RRC		0	0	0	0
	yes RRC	5.5.2(R_w) yes	20	26	76	118
		5.5.2(R_w) no	4	16	12	8
p-rank 0	no RRC		0	3	2	1
	yes RRC	5.5.2(R_w) yes	20	15	17	23
		5.5.2(R_w) no	1	1	2	1

squarefree dimension 4			$p=2$	$p=3$
total			1431	10453
ordinary			656	6742
almost ordinary			392	2506
p-rank 2	no RRC		0	0
	yes RRC	5.5.2(R_w) yes	149	500
		5.5.2(R_w) no	49	312
p-rank 1	no RRC		6	36
	yes RRC	5.5.2(R_w) yes	80	184
		5.5.2(R_w) no	14	40
p-rank 0	no RRC		3	6
	yes RRC	5.5.2(R_w) yes	73	88
		5.5.2(R_w) no	9	39