Polarizations of abelian varieties over finite fields via canonical liftings

Stefano Marseglia

Utrecht University

AGCCT 2021 - 1 June 2021

Polarizations of abelian varieties over finite fields via canonical liftings

Stefano Marseglia

Utrecht University

AGCCT 2021 - 1 June 2021

joint work with

Jonas Bergström and **Valentijn Karemaker**.

Canonical Liftings

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

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 $\mathrm{End}(\mathscr{A}_{\mathrm{can}}) = \mathrm{End}(A_0)$.

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 $\mathrm{End}(\mathscr{A}_{\mathrm{can}}) = \mathrm{End}(A_0)$.

- Example: ordinary abelian variety; almost-ordinary abelian variety.

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 $\mathrm{End}(\mathscr{A}_{\mathrm{can}}) = \mathrm{End}(A_0)$.

- Example: ordinary abelian variety; almost-ordinary abelian variety.
- Non-example: supersingular EC (quaternions).

Complex Uniformization

- Assume that A_0 admits a canonical lifting $\mathscr{A}_{\text{can}}$.

Complex Uniformization

- Assume that A_0 admits a canonical lifting $\mathscr{A}_{\mathrm{can}}$.
- Fix $\mathscr{R} \hookrightarrow \mathbb{C}$ and put $A_{\mathrm{can}} := \mathscr{A}_{\mathrm{can}} \otimes \mathbb{C}$.

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 reducing to Frobenius and Verschiebung.

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 reducing to Frobenius and Verschiebung.
- By **complex uniformization**:

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

- I : a fractional $\mathbb{Z}[F,V]$-ideal in $L := \mathbb{Q}[F]$,
- Φ : a CM-type of L.

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 reducing to Frobenius and Verschiebung.
- By **complex uniformization**:

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

- I : a fractional $\mathbb{Z}[F,V]$-ideal in $L := \mathbb{Q}[F]$,
- Φ : a CM-type of L.

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

Complex Uniformization

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

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

- I : a fractional $\mathbb{Z}[F,V]$-ideal in $L := \mathbb{Q}[F]$,
- Φ : a CM-type of L.

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

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

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 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.

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

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

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

Complex Uniformization : Polarizations

- We have:

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

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

- We have:

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

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

- What about **polarizations**? We understand them over $\mathbb{C}$!

Complex Uniformization : Polarizations

- We have:

$$A_{\text{can}}(\mathbb{C}) \simeq \mathbb{C}^g/_{\Phi(I)}, \quad A^\vee_{\text{can}}(\mathbb{C}) \simeq \mathbb{C}^g/_{\Phi(\bar{I}^t)},$$

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

- What about **polarizations**? We understand them over $\mathbb{C}$!
- Let $\mu : A_{\text{can}} \to A^\vee_{\text{can}}$ an isogeny. Then μ is a polarization if and only if $\lambda := \mathscr{H}(\mu) \in (\bar{I}^t : I)$ satisfies

Complex Uniformization : Polarizations

- 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

Complex Uniformization : Polarizations

- We have:

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

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

- 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).

Complex Uniformization : Polarizations

- We have:

$$A_{\text{can}}(\mathbb{C}) \simeq \mathbb{C}^g \big/ \Phi(I), \quad A^\vee_{\text{can}}(\mathbb{C}) \simeq \mathbb{C}^g \big/ \Phi(\bar{I}^t),$$

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

- What about **polarizations**? We understand them over $\mathbb{C}$!
- Let $\mu : A_{\text{can}} \to A^\vee_{\text{can}}$ 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).

The Centeleghe-Stix equivalence

The Centeleghe-Stix equivalence

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* $V = p/F$.

The Centeleghe-Stix equivalence

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:*

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

The Centeleghe-Stix equivalence

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 Centeleghe-Stix equivalence

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:

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

- 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.

The Centeleghe-Stix equivalence

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:

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

- 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 $B_0 \in \mathrm{AV}_h(p)$:

$$\mathscr{G}(B_0^\vee) = \overline{\mathscr{G}(B_0)}^t$$

The Centeleghe-Stix equivalence

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 $B_0 \in \mathrm{AV}_h(p)$:

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

The Centeleghe-Stix equivalence

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.

Comparison

- Assume that A_0 admits a canonical lifting A_{can}.
- We have two description using fractional ideals. Let's compare them.

$$\begin{tikzcd}
\mathrm{Hom}(A_{\mathrm{can}}, A_{\mathrm{can}}^\vee) \arrow[d, "\mathrm{red}"] \arrow[dr, "\text{complex unif.}"] & \\
\mathrm{Hom}(A_0, A_0^\vee) & (\overline{I}^t : I)
\end{tikzcd}$$

Comparison

- Assume that A_0 admits a canonical lifting A_{can}.
- We have two description using fractional ideals. Let's compare them.

$$
\begin{tikzcd}
\mathrm{Hom}(A_{\mathrm{can}}, A_{\mathrm{can}}^\vee) \arrow[d, "\mathrm{red}"] \arrow[drr, "\text{complex unif.}"] & & \\
\mathrm{Hom}(A_0, A_0^\vee) \arrow[d, "\mathscr{G}"] & & (\overline{I}^t : I) \arrow[d] \\
(\mathscr{G}(A_0) : \overline{\mathscr{G}(A_0)}^t) \arrow[rr, equal] & & (\overline{I}^t : I)
\end{tikzcd}
$$

Comparison

- Assume that A_0 admits a canonical lifting A_{can}.
- We have two description using fractional ideals. Let's compare them.

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

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.

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

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.

- 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:

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

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

Comparison : Polarizations

we WANT
to understand
pols. here

we DO
understand
pols. here

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

we WANT to understand pols. here

we DO understand pols. here

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

By chasing the diagram, we get:

Comparison : Polarizations

we WANT to understand pols. here

we DO understand pols. here

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

By chasing the diagram, we get:

Theorem ("lift and spread")

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

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

Principal Polarizations up to isomorphism

- Let $B_0 \in \mathrm{AV}_h(p)$. Put $T = \mathrm{End}(B_0)$ and $\mathscr{G}(B_0) = J$.

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 $i_0 \in L^*$.

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 $\mathscr{G}(\mu) = v\overline{v}\mathscr{G}(\mu')$.

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 $T^* / < v\overline{v} : v \in T^* >$.

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.

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 $T = \mathrm{End}(B_0)$.

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).

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

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

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!)

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

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.

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

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

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

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

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

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* $k_E \subseteq \mathbb{F}_q$*.*

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* $\mathscr{O}_L = \mathrm{End}(A_0)$*.*

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).

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

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

<table>
<tr><td colspan="3">squarefree dimension 4</td><td>$p = 2$</td><td>$p = 3$</td></tr>
<tr><td colspan="3">total</td><td>1431</td><td>10453</td></tr>
<tr><td colspan="3">ordinary</td><td>656</td><td>6742</td></tr>
<tr><td colspan="3">almost ordinary</td><td>392</td><td>2506</td></tr>
<tr><td rowspan="3">p-rank 2</td><td colspan="2">no RRC</td><td>0</td><td>0</td></tr>
<tr><td rowspan="2">yes RRC</td><td>Thm 1 yes</td><td>149</td><td>500</td></tr>
<tr><td>Thm 1 no</td><td>49</td><td>312</td></tr>
<tr><td rowspan="3">p-rank 1</td><td colspan="2">no RRC</td><td>6</td><td>36</td></tr>
<tr><td rowspan="2">yes RRC</td><td>Thm 1 yes</td><td>80</td><td>184</td></tr>
<tr><td>Thm 1 no</td><td>14</td><td>40</td></tr>
<tr><td rowspan="3">p-rank 0</td><td colspan="2">no RRC</td><td>3</td><td>6</td></tr>
<tr><td rowspan="2">yes RRC</td><td>Thm 1 yes</td><td>73</td><td>88</td></tr>
<tr><td>Thm 1 no</td><td>9</td><td>39</td></tr>
</table>

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

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	Thm 1 yes	149	500
		Thm 1 no	49	312
p-rank 1	no RRC		6	36
	yes RRC	Thm 1 yes	80	184
		Thm 1 no	14	40
p-rank 0	no RRC		3	6
	yes RRC	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 $391/\mathbb{F}_3$.

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

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	Thm 1 yes	149	500
		Thm 1 no	49	312
p-rank 1	no RRC		6	36
	yes RRC	Thm 1 yes	80	184
		Thm 1 no	14	40
p-rank 0	no RRC		3	6
	yes RRC	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 have **other methods** for $20/\mathbb{F}_2$ and $214/\mathbb{F}_3$.

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

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	Thm 1 yes	149	500
		Thm 1 no	49	312
p-rank 1	no RRC		6	36
	yes RRC	Thm 1 yes	80	184
		Thm 1 no	14	40
p-rank 0	no RRC		3	6
	yes RRC	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 have **other methods** 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).

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

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	Thm 1 yes	149	500
		Thm 1 no	49	312
p-rank 1	no RRC		6	36
	yes RRC	Thm 1 yes	80	184
		Thm 1 no	14	40
p-rank 0	no RRC		3	6
	yes RRC	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 have **other methods** 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.

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 $I_1, \dots, I_r$. 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!