

# 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  $g$ .

## Definition

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

- 1 special fiber  $A_0$ , and
  - 2 general fiber  $\mathcal{A}_{\text{can}}$  satisfying  $\text{End}(\mathcal{A}_{\text{can}}) = \text{End}(A_0)$ .
- Example: ordinary abelian variety; almost-ordinary abelian variety.
  - Non-example: supersingular EC (quaternions).

# Complex Uniformization

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

$$A_{\text{can}}(\mathbb{C}) \simeq \mathbb{C}^g / \Phi(I) \quad \begin{array}{l} - I : \text{a fractional } \mathbb{Z}[F, V]\text{-ideal in } L := \mathbb{Q}[F], \\ - \Phi : \text{a CM-type of } L. \end{array}$$

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

$$\begin{array}{c} \text{char.0 :} \\ \nearrow \\ \mathbb{F}_q : A_0^\vee \end{array} \quad \mathcal{A}_{\text{can}}^\vee \xrightarrow{\otimes \mathbb{C}} A_{\text{can}}^\vee \xrightarrow{\mathcal{H}} \bar{I}^t = \{\bar{x} : \text{Tr}_{L/\mathbb{Q}}(xI) \subseteq \mathbb{Z}\}$$

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

# Complex Uniformization : Polarizations

- We have:

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

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

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

# The Centeleghe-Stix equivalence

## Theorem (Centeleghe-Stix)

Let  $AV_h(p)$  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:

$$AV_h(p) \xrightarrow{\mathcal{G}} \{\text{fractional } \mathbb{Z}[F, V]\text{-ideals in } L\}.$$

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

$$\mathcal{G}(B_0^\vee) = \overline{\mathcal{G}(B_0)}^t \text{ and } \mathcal{G}(f^\vee) = \overline{\mathcal{G}(f)}, \text{ for any } f: B_0 \rightarrow B_0' \text{ in } AV_h(p).$$

- In particular:

$$\mathcal{G}(\text{Hom}(B_0, B_0^\vee)) = (\mathcal{G}(B_0) : \overline{\mathcal{G}(B_0)}^t).$$

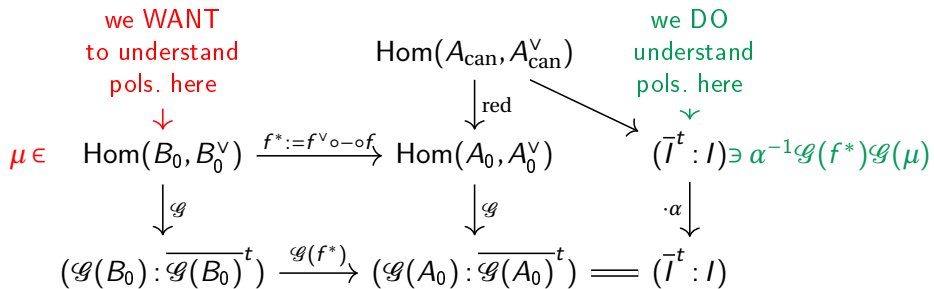
# Comparison

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

$$\begin{array}{ccccc}
 & & \text{Hom}(A_{\text{can}}, A_{\text{can}}^{\vee}) & & \\
 & & \downarrow \text{red} & \searrow \text{complex unif.} & \\
 \text{Hom}(B_0, B_0^{\vee}) & \xrightarrow{f^* := f^{\vee} \circ \circ f} & \text{Hom}(A_0, A_0^{\vee}) & & (\bar{I}^t : I) \\
 \downarrow \mathcal{G} & & \downarrow \mathcal{G} & & \downarrow \cdot \alpha \begin{array}{l} \text{tot. real } (\alpha = \bar{\alpha}) \\ \text{unit in End}(A_0) \end{array} \\
 (\mathcal{G}(B_0) : \overline{\mathcal{G}(B_0)})^t & \xrightarrow{\mathcal{G}(f^*)} & (\mathcal{G}(A_0) : \overline{\mathcal{G}(A_0)})^t & = & (\bar{I}^t : I)
 \end{array}$$

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

# Comparison : Polarizations



By chasing the diagram, we get:

Theorem ("lift and spread")

Let  $\mu : B_0 \rightarrow B_0^{\vee}$  be an isogeny. Then

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

# Principal Polarizations up to isomorphism

- Let  $B_0 \in AV_h(p)$ . Put  $T = \text{End}(B_0)$  and  $\mathcal{G}(B_0) = J$ .
- Assume that  $B_0 \simeq B_0^\vee$ , i.e.  $J = i_0 \bar{J}^t$  for some  $i_0 \in L^*$ .
- If  $\mu$  and  $\mu'$  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  $\mathcal{G}(\mu) = v \bar{v} \mathcal{G}(\mu')$ .
- Let  $\mathcal{T}$  be a transversal of  $T^* / \langle v \bar{v} : v \in T^* \rangle$ .
- Then

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

is a set of representatives of the PPs of  $B_0$  up to isomorphism.

- It depends on  $\alpha$ !



## Effective Results : when can we ignore $\alpha$ ?

Assume  $A_0$  admits a canonical lifting. Put  $S := \text{End}(A_0)$

Let  $B_0$  be isogenous to  $A_0$ . Put  $T = \text{End}(B_0)$ .

### 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

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

is in bijection with the set (which does not depend on  $\alpha$ !)

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

### Corollary

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

# When can we lift up to isogeny?

## Theorem (Chai-Conrad-Oort)

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

- 1  $\Phi$  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  $\mathcal{O}_L = \text{End}(A_0)$ .

- If there is a separable isogeny  $A_0 \rightarrow A'_0$  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.

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  $AV_h(p)$  with endomorphism ring  $T$ , represented under  $\mathcal{G}$  by the fractional ideals  $I_1, \dots, I_r$ . For any CM-type  $\Phi'$ , we put*

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

*If there exists a non-negative integer  $N$  such that for every CM-type  $\Phi'$  we have*

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

*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  $\Phi'$ -positive.
- We can go back: for every  $b$  tot. imaginary there exists a unique CM-type  $\Phi_b$  s.t.  $b$  is  $\Phi_b$ -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  $\mathcal{P}_{\Phi_b}^\alpha(l_i) \longleftrightarrow \mathcal{P}_{\Phi_{ab}}^1(l_i)$ .
- If the we get the 'same sum' (over the  $l_i$ '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  $\Phi'$ 's then we know that one of the outputs is the correct one!