Isomorphism classes of abelian varieties over finite fields

Marseglia Stefano

Utrecht University

ICERM - January 31, 2019

Plan for the talk

Plan for the talk

(a) equivalence of categories
- Deligne (ordinary over $\mathbb{F}_q$)
- Centeleghe-Stix (over $\mathbb{F}_p$ away from real primes)

Plan for the talk

a. equivalence of categories
   - Deligne (ordinary over $\mathbb{F}_q$)
   - Centeleghe-Stix (over $\mathbb{F}_p$ away from real primes)
b. isomorphism classes of AV
   - square-free case : ideal class monoid
   - power of a sq-free : only Bass orders

Plan for the talk

(a) equivalence of categories
- Deligne (ordinary over $\mathbb{F}_q$)
- Centeleghe-Stix (over $\mathbb{F}_p$ away from real primes)

(b) isomorphism classes of AV
- square-free case : ideal class monoid
- power of a sq-free : only Bass orders

(c) polarizations
- square-free ordinary case : working algorithm
- square-free Centeleghe-Stix case : working algorithm (conjectural)
- power of a sq-free : no algorithm :(

Plan for the talk

a. equivalence of categories
   - Deligne (ordinary over $\mathbb{F}_q$)
   - Centeleghe-Stix (over $\mathbb{F}_p$ away from real primes)
b. isomorphism classes of AV
   - square-free case : ideal class monoid
   - power of a sq-free : only Bass orders
c. polarizations
   - square-free ordinary case : working algorithm
   - square-free Centeleghe-Stix case : working algorithm (conjectural)
   - power of a sq-free : no algorithm :(
d. bottle-necks
   - over-orders (Tommy Hofmann?)
   - weak eq. classes (I have a conjecture)
   - CM-type (need to compute a splitting field)
   - polarizations (it should be possible to spread them)

Deligne's equivalence

Theorem (Deligne '69)

Let $q = p^r$, with p a prime. There is an equivalence of categories:

$$\{\textit{Ordinary abelian varieties over } \mathbb{F}_q\} \qquad\qquad A$$

Deligne's equivalence

Theorem (Deligne '69)

Let $q = p^r$, with p a prime. There is an equivalence of categories:

$$\begin{array}{ccc}
\{\textit{Ordinary abelian varieties over } \mathbb{F}_q\} & & A \\
\updownarrow & & \mapsto \\
\left\{\begin{array}{l}
\textit{pairs } (T, F)\textit{, where } T \simeq_{\mathbb{Z}} \mathbb{Z}^{2g} \textit{ and } T \xrightarrow{F} T \textit{ s.t.} \\
\textit{- } F \otimes \mathbb{Q} \textit{ is semisimple} \\
\textit{- the roots of } \mathrm{char}_{F\otimes\mathbb{Q}}(x) \textit{ have abs. value } \sqrt{q} \\
\textit{- half of them are p-adic units} \\
\textit{- } \exists V : T \to T \textit{ such that } FV = VF = q
\end{array}\right\} & & (T(A), F(A))
\end{array}$$

Deligne's equivalence

Theorem (Deligne '69)

Let $q = p^r$, with p a prime. There is an equivalence of categories:

$$\begin{array}{cc}
\{\text{Ordinary abelian varieties over } \mathbb{F}_q\} & A \\
\updownarrow & \downarrow \\
\left\{\begin{array}{l}
\text{pairs } (T,F), \text{ where } T \simeq_{\mathbb{Z}} \mathbb{Z}^{2g} \text{ and } T \xrightarrow{F} T \text{ s.t.} \\
\text{- } F \otimes \mathbb{Q} \text{ is semisimple} \\
\text{- the roots of } \mathrm{char}_{F\otimes\mathbb{Q}}(x) \text{ have abs. value } \sqrt{q} \\
\text{- half of them are } p\text{-adic units} \\
\text{- } \exists V : T \to T \text{ such that } FV = VF = q
\end{array}\right\} & (T(A), F(A))
\end{array}$$

Remark

- *If* $\dim(A) = g$ *then* $\mathrm{Rank}(T(A)) = 2g$;
- $\mathrm{Frob}(A) \rightsquigarrow F(A)$.

Centeleghe-Stix' equivalence

Theorem (Centeleghe-Stix '15)

Let p be a prime. There is an equivalence of categories:

$$\{\text{abelian varieties over } \mathbb{F}_p \text{ away from real primes}\} \qquad A$$

Centeleghe-Stix' equivalence

Theorem (Centeleghe-Stix '15)

Let p be a prime. There is an equivalence of categories:

$$
\begin{array}{ccc}
\{\text{abelian varieties over } \mathbb{F}_p \text{ away from real primes}\} & & A \\
\updownarrow & & \downarrow \\
\left\{\begin{array}{l}
\text{pairs } (T,F), \text{ where } T \simeq_{\mathbb{Z}} \mathbb{Z}^{2g} \text{ and } T \xrightarrow{F} T \text{ s.t.} \\
\text{- } F \otimes \mathbb{Q} \text{ is semisimple} \\
\text{- the roots of } \mathrm{char}_{F\otimes\mathbb{Q}}(x) \text{ have abs. value } \sqrt{p} \\
\text{- } \mathrm{char}_{F\otimes\mathbb{Q}}(\sqrt{p}) \neq 0 \\
\text{- } \exists V : T \to T \text{ such that } FV = VF = p
\end{array}\right\} & & (T(A), F(A))
\end{array}
$$

Centeleghe-Stix' equivalence

Theorem (Centeleghe-Stix '15)

Let p be a prime. There is an equivalence of categories:

$$\begin{array}{ccc}
\{\text{abelian varieties over } \mathbb{F}_p \text{ away from real primes}\} & & A \\
\updownarrow & & \downarrow \\
\left\{\begin{array}{l}
\text{pairs } (T,F), \text{ where } T \simeq_{\mathbb{Z}} \mathbb{Z}^{2g} \text{ and } T \xrightarrow{F} T \text{ s.t.} \\
\text{- } F \otimes \mathbb{Q} \text{ is semisimple} \\
\text{- the roots of } \mathrm{char}_{F\otimes\mathbb{Q}}(x) \text{ have abs. value } \sqrt{p} \\
\text{- } \mathrm{char}_{F\otimes\mathbb{Q}}(\sqrt{p}) \neq 0 \\
\text{- } \exists V : T \to T \text{ such that } FV = VF = p
\end{array}\right\} & & (T(A), F(A))
\end{array}$$

Remark

- *If* $\dim(A) = g$ *then* $\mathrm{Rank}(T(A)) = 2g$;
- $\mathrm{Frob}(A) \rightsquigarrow F(A)$.

equivalences in the square-free case

Let h be a square-free characteristic q-Weil polynomial.
Assume that h is **ordinary** or, $q = p$ and $\mathbf{h}(\sqrt{\mathbf{p}}) \neq \mathbf{0}$.

$$\rightsquigarrow \text{an isogeny class } \mathscr{C}_h \text{ (by Honda-Tate).}$$

equivalences in the square-free case

Let h be a square-free characteristic q-Weil polynomial.
Assume that h is **ordinary** or, $q = p$ and $\mathbf{h}(\sqrt{\mathbf{p}}) \neq \mathbf{0}$.

$$\rightsquigarrow \text{an isogeny class } \mathscr{C}_h \text{ (by Honda-Tate).}$$

Put

$$K := \mathbb{Q}[x]/(h)$$
$$F := x \bmod (h)$$
$$R := \mathbb{Z}[F, q/F] \subset K$$

equivalences in the square-free case

Let h be a square-free characteristic q-Weil polynomial.
Assume that h is **ordinary** or, $q = p$ and $\mathbf{h}(\sqrt{\mathbf{p}}) \neq \mathbf{0}$.

$\rightsquigarrow$ an isogeny class $\mathscr{C}_h$ (by Honda-Tate).

Put

$$K := \mathbb{Q}[x]/(h)$$
$$F := x \bmod (h)$$
$$R := \mathbb{Z}[F, q/F] \subset K$$

We get:

Theorem (M.)

$$\textit{an equivalence } \mathscr{C}_h \longleftrightarrow \{\textit{fractional } R\textit{-ideals}\}$$

$$\textit{and } {}^{\mathscr{C}_h}/_{\simeq} \longleftrightarrow {}^{\{\textit{fractional } R\textit{-ideals}\}}/_{\simeq_R} =: \mathrm{ICM}(R) \textit{ ideal class monoid}$$

The case "power of a square-free"

Consider $\mathscr{C}_h$ for $h = g^r$ with g a square-free q-Weil polynomial. Assume that g is **ordinary** or, $q = p$ and $\mathbf{g(\sqrt{p}) \neq 0}$.

The case "power of a square-free"

Consider $\mathscr{C}_h$ for $h = g^r$ with g a square-free q-Weil polynomial. Assume that g is **ordinary** or, $q = p$ and $\mathbf{g(\sqrt{p}) \neq 0}$.
Put

$$K := \mathbb{Q}[x]/(g)$$
$$F := x \bmod (g)$$
$$R := \mathbb{Z}[F, q/F] \subset K$$

The case "power of a square-free"

Consider $\mathscr{C}_h$ for $h = g^r$ with g a square-free q-Weil polynomial. Assume that g is **ordinary** or, $q = p$ and $\mathbf{g}(\sqrt{\mathbf{p}}) \neq \mathbf{0}$.
Put

$$\begin{aligned} K &:= \mathbb{Q}[x]/(g) \\ F &:= x \bmod (g) \\ R &:= \mathbb{Z}[F, q/F] \subset K \end{aligned}$$

We get:

Theorem (M.)

We have an equivalence

$$\mathscr{C}_h \longleftrightarrow \{\textit{fin. gen. torsion-free } R\textit{-modules } M \textit{ s.t. } M \otimes_R K \simeq K^r\} =: \mathscr{B}(g^r)$$

The category $\mathscr{B}(g^r)$

Recall that an R-module M is **torsion-free** if the canonical morphism

$$M \to M \otimes_R K$$

is injective.

The category $\mathscr{B}(g^r)$

Recall that an R-module M is **torsion-free** if the canonical morphism

$$M \to M \otimes_R K$$

is injective.
We can think of modules $M \in \mathscr{B}(g^r)$ as **embedded** in K^r.

The category $\mathscr{B}(g^r)$

Recall that an R-module M is **torsion-free** if the canonical morphism

$$M \to M \otimes_R K$$

is injective.
We can think of modules $M \in \mathscr{B}(g^r)$ as **embedded** in K^r.
The category $\mathscr{B}(g^r)$ becomes more explicit and computable under certain assumption on the order R.
An order R is called Bass if one of the following equivalent conditions holds:

The category $\mathscr{B}(g^r)$

Recall that an R-module M is **torsion-free** if the canonical morphism

$$M \to M \otimes_R K$$

is injective.

We can think of modules $M \in \mathscr{B}(g^r)$ as **embedded** in K^r.

The category $\mathscr{B}(g^r)$ becomes more explicit and computable under certain assumption on the order R.

An order R is called Bass if one of the following equivalent conditions holds:

- every over-order $R \subseteq S \subseteq \mathscr{O}_K$ is Gorenstein (i.e. S^t is invertible in S).

The category $\mathscr{B}(g^r)$

Recall that an R-module M is **torsion-free** if the canonical morphism

$$M \to M \otimes_R K$$

is injective.
We can think of modules $M \in \mathscr{B}(g^r)$ as **embedded** in K^r.
The category $\mathscr{B}(g^r)$ becomes more explicit and computable under certain assumption on the order R.
An order R is called Bass if one of the following equivalent conditions holds:

- every over-order $R \subseteq S \subseteq \mathscr{O}_K$ is Gorenstein (i.e. S^t is invertible in S).
- every fractional R-ideal I is invertible in $(I : I)$.

The category $\mathscr{B}(g^r)$

Recall that an R-module M is **torsion-free** if the canonical morphism

$$M \to M \otimes_R K$$

is injective.
We can think of modules $M \in \mathscr{B}(g^r)$ as **embedded** in K^r.
The category $\mathscr{B}(g^r)$ becomes more explicit and computable under certain assumption on the order R.
An order R is called Bass if one of the following equivalent conditions holds:

- every over-order $R \subseteq S \subseteq \mathscr{O}_K$ is Gorenstein (i.e. S^t is invertible in S).
- every fractional R-ideal I is invertible in $(I:I)$.
- $\mathrm{ICM}(R) = \bigsqcup_{R \subseteq S \subseteq \mathscr{O}_K} \mathrm{Pic}(S)$.

$\mathscr{B}(g^r)$ in the Bass case

Corollary

Assume that R is Bass. Then for every $M \in \mathscr{B}(g^r)$ there are over orders $S_1 \subseteq \ldots \subseteq S_r$ of R and a fractional ideal I invertible in S_r such that

$$M \simeq S_1 \oplus \ldots \oplus S_{r-1} \oplus I$$

$\mathscr{B}(g^r)$ in the Bass case

Corollary

Assume that R is Bass. Then for every $M \in \mathscr{B}(g^r)$ there are over orders $S_1 \subseteq \ldots \subseteq S_r$ of R and a fractional ideal I invertible in S_r such that

$$M \simeq S_1 \oplus \ldots \oplus S_{r-1} \oplus I$$

We have a simple description of morphisms in $\mathscr{B}(g^r)$.
For example, for M as above:

$\mathscr{B}(g^r)$ in the Bass case

Corollary

Assume that R is Bass. Then for every $M \in \mathscr{B}(g^r)$ there are over orders $S_1 \subseteq \ldots \subseteq S_r$ of R and a fractional ideal I invertible in S_r such that

$$M \simeq S_1 \oplus \ldots \oplus S_{r-1} \oplus I$$

We have a simple description of morphisms in $\mathscr{B}(g^r)$.
For example, for M as above:

$$\mathrm{End}_R(M) = \begin{pmatrix} S_1 & S_2 & \ldots & S_{r-1} & I \\ (S_1 : S_2) & S_2 & \ldots & S_{r-1} & I \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ (S_1 : S_{r-1}) & (S_2 : S_{r-1}) & \ldots & S_{r-1} & I \\ (S_1 : I) & (S_2 : I) & \ldots & (S_{r-1} : I) & (I : I) \end{pmatrix}$$

and

$\mathscr{B}(g^r)$ in the Bass case

Corollary

Assume that R is Bass. Then for every $M \in \mathscr{B}(g^r)$ there are over orders $S_1 \subseteq \ldots \subseteq S_r$ of R and a fractional ideal I invertible in S_r such that

$$M \simeq S_1 \oplus \ldots \oplus S_{r-1} \oplus I$$

We have a simple description of morphisms in $\mathscr{B}(g^r)$.
For example, for M as above:

$$\mathrm{End}_R(M) = \begin{pmatrix} S_1 & S_2 & \ldots & S_{r-1} & I \\ (S_1 : S_2) & S_2 & \ldots & S_{r-1} & I \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ (S_1 : S_{r-1}) & (S_2 : S_{r-1}) & \ldots & S_{r-1} & I \\ (S_1 : I) & (S_2 : I) & \ldots & (S_{r-1} : I) & (I : I) \end{pmatrix}$$

and

$$\mathrm{Aut}_R(M) = \left\{ A \in \mathrm{End}_R(M) \cap \mathrm{GL}_r(K) : A^{-1} \in \mathrm{End}_R(M) \right\}.$$

Consequences for $\mathscr{C}_h$

Corollary

Assume $R = \mathbb{Z}[F, q/F]$ *is Bass. Then*

Consequences for $\mathscr{C}_h$

Corollary

Assume $R = \mathbb{Z}[F, q/F]$ *is Bass. Then*

- $$ {\mathscr{C}_h}/_{\simeq} \longleftrightarrow \left\{ (S_1 \subseteq S_2 \subseteq \ldots \subseteq S_r, [I]_{\simeq}) : \begin{array}{c} R \subseteq S_1, \\ I \text{ a frac. } R\text{-ideal} \\ \text{with } (I:I) = S_r \end{array} \right\} $$

Consequences for $\mathscr{C}_h$

Corollary

Assume $R = \mathbb{Z}[F, q/F]$ is Bass. Then

- $$\mathscr{C}_h/_{\simeq} \longleftrightarrow \left\{ (S_1 \subseteq S_2 \subseteq \ldots \subseteq S_r, [I]_{\simeq}) : \begin{array}{c} R \subseteq S_1, \\ I \text{ a frac. } R\text{-ideal} \\ \text{with } (I:I) = S_r \end{array} \right\}$$
- *for every $A \in \mathscr{C}_h$, say $A \sim B^r$ with $h_B = g$, there are*
  $$C_1, \ldots, C_r \sim B \text{ such that } A \simeq C_1 \times \ldots \times C_r$$
  everything is a product

Consequences for $\mathscr{C}_h$

Corollary

Assume $R=\mathbb{Z}[F,q/F]$ is Bass. Then

- $$\mathscr{C}_h/_{\simeq} \longleftrightarrow \left\{ (S_1\subseteq S_2\subseteq\ldots\subseteq S_r,[I]_{\simeq}) : \begin{array}{c} R\subseteq S_1, \\ I \text{ a frac. } R\text{-ideal} \\ \text{with } (I:I)=S_r \end{array} \right\}$$

- *for every $A\in\mathscr{C}_h$, say $A\sim B^r$ with $h_B=g$, there are*

  $C_1,\ldots,C_r\sim B$ *such that* $A\simeq C_1\times\ldots\times C_r$ *everything is a product*

- *if*
  $$A\longleftrightarrow\bigoplus_k I_k \text{ and } B\longleftrightarrow\bigoplus_k J_k$$

  then $\mu\in\operatorname{Hom}(A,B)\longleftrightarrow\Lambda\in\operatorname{Mat}_{r\times r}(K)$ *s.t.* $\Lambda_{h,k}\in(J_h:I_k)$

Consequences for $\mathscr{C}_h$

Corollary

Assume $R = \mathbb{Z}[F, q/F]$ is Bass. Then

- $$\mathscr{C}_h/_{\simeq} \longleftrightarrow \left\{ (S_1 \subseteq S_2 \subseteq \ldots \subseteq S_r, [I]_{\simeq}) : \begin{array}{c} R \subseteq S_1, \\ I \text{ a frac. } R\text{-ideal} \\ \text{with } (I:I) = S_r \end{array} \right\}$$
- *for every $A \in \mathscr{C}_h$, say $A \sim B^r$ with $h_B = g$, there are*
  $$C_1, \ldots, C_r \sim B \text{ such that } A \simeq C_1 \times \ldots \times C_r$$
  everything is a product
- *if*
  $$A \longleftrightarrow \bigoplus_k I_k \text{ and } B \longleftrightarrow \bigoplus_k J_k$$
  then
  $$\mu \in \mathrm{Hom}(A, B) \longleftrightarrow \Lambda \in \mathrm{Mat}_{r\times r}(K) \text{ s.t. } \Lambda_{h,k} \in (J_h : I_k)$$
  Moreover, μ is an isogeny if and only if $\det(\Lambda) \in K^\times$

dual variety and polarizations

Using Howe ('95) in the ordinary square-free case:

Theorem (M.)

If $A \leftrightarrow I$, then:

dual variety and polarizations

Using Howe ('95) in the ordinary square-free case:

Theorem (M.)

If $A \leftrightarrow I$, then:

- $A^{\vee} \leftrightarrow \overline{I}^{t}$.

dual variety and polarizations

Using Howe ('95) in the ordinary square-free case:

Theorem (M.)

If $A \leftrightarrow I$, then:

- $A^\vee \leftrightarrow \bar{I}^t$.
- *a polarization μ of A corresponds to a $\lambda \in K^\times$ such that*
  - $\lambda I \subseteq \bar{I}^t$ *(isogeny);*
  - λ *is totally imaginary* ($\bar{\lambda} = -\lambda$)*;*
  - λ *is Φ-positive, where Φ is a specific CM-type of K.* Bottleneck 3

  Also: $\deg \mu = [\bar{I}^t : \lambda I]$.

dual variety and polarizations

Using Howe ('95) in the ordinary square-free case:

Theorem (M.)

If $A \leftrightarrow I$, then:

- $A^\vee \leftrightarrow \overline{I}^t$.
- *a polarization μ of A corresponds to a $\lambda \in K^\times$ such that*
  - $\lambda I \subseteq \overline{I}^t$ *(isogeny);*
  - λ *is totally imaginary* $(\overline{\lambda} = -\lambda)$*;*
  - λ *is* Φ*-positive, where* Φ *is a specific CM-type of* K. *Bottleneck 3*

  Also: $\deg \mu = [\overline{I}^t : \lambda I]$.
- *if* $(A, \mu) \leftrightarrow (I, \lambda)$ *and* $S = (I : I)$ *then*

$$\left\{\begin{matrix} \text{non-isomorphic} \\ \text{polarizations of } A \end{matrix}\right\} \longleftrightarrow \frac{\{\text{totally positive } u \in S^\times\}}{\{v\overline{v} : v \in S^\times\}}.$$

" Bottleneck" 4

dual variety and polarizations

Using Howe ('95) in the ordinary square-free case:

Theorem (M.)

If $A \leftrightarrow I$, then:

- $A^\vee \leftrightarrow \overline{I}^t$.
- *a polarization μ of A corresponds to a $\lambda \in K^\times$ such that*
  - $\lambda I \subseteq \overline{I}^t$ *(isogeny);*
  - λ *is totally imaginary* ($\overline{\lambda} = -\lambda$);
  - λ *is Φ-positive, where Φ is a specific CM-type of K.* Bottleneck 3

  Also: $\deg \mu = [\overline{I}^t : \lambda I]$.
- *if $(A,\mu) \leftrightarrow (I,\lambda)$ and $S = (I : I)$ then*

$$\left\{ \begin{matrix} \text{non-isomorphic} \\ \text{polarizations of } A \end{matrix} \right\} \longleftrightarrow \frac{\{\text{totally positive } u \in S^\times\}}{\{v\overline{v} : v \in S^\times\}}.$$ "Bottleneck" 4

- *and* $\mathrm{Aut}(A,\mu) = \{\text{torsion units of } S\}$.

Work in progress and Bottlenecks

Work in progress

- 1: polarizations in the non-ordinary (Centeleghe-Stix) square-free case (with Jonas Bergström)
- 2: group of rational points (and level structure)

Work in progress and Bottlenecks

Work in progress

- 1: polarizations in the non-ordinary (Centeleghe-Stix) square-free case (with Jonas Bergström)
- 2: group of rational points (and level structure)

Bottlenecks

- 1: over-orders (Tommy Hoffman ?)
- 2: weak equivalence class monoid (I have a conjecture)
- 3: CM-type (need to compute a splitting field. can be done locally?)
- 4: polarizations (it should be possible to "spread" them)