Computing isomorphism classes of abelian varieties over finite fields
CNTA XV

Marseglia Stefano

Stockholms Universitet

12 July 2018

Introduction

- Goal: compute **isomorphism classes** of (polarized) abelian varieties over a **finite field**.

Introduction

- Goal: compute **isomorphism classes** of (polarized) abelian varieties over a **finite field**.
- in dimension $g > 1$ is not easy to produce equations.

Introduction

- Goal: compute **isomorphism classes** of (polarized) abelian varieties over a **finite field**.
- in dimension $g > 1$ is not easy to produce equations.
- for $g > 3$ it is not enough to consider Jacobians.

Introduction

- Goal: compute **isomorphism classes** of (polarized) abelian varieties over a **finite field**.
- in dimension $g > 1$ is not easy to produce equations.
- for $g > 3$ it is not enough to consider Jacobians.
- over $\mathbb{C}$:

$$\{\text{abelian varieties } /\mathbb{C}\} \longleftrightarrow \left\{ \begin{array}{l} \mathbb{C}^g/L \text{ with } L \simeq \mathbb{Z}^{2g} \\ + \text{ Riemann form} \end{array} \right\}.$$

Introduction

- Goal: compute **isomorphism classes** of (polarized) abelian varieties over a **finite field**.
- in dimension $g > 1$ is not easy to produce equations.
- for $g > 3$ it is not enough to consider Jacobians.
- over $\mathbb{C}$:

$$\{\text{abelian varieties } /\mathbb{C}\} \longleftrightarrow \left\{ \begin{array}{l} \mathbb{C}^g/L \text{ with } L \simeq \mathbb{Z}^{2g} \\ + \text{ Riemann form} \end{array} \right\}.$$

- in positive characteristic we don't have such equivalence.

Deligne's equivalence

Theorem (Deligne '69)

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

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

Deligne's equivalence

Theorem (Deligne '69)

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

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

$$\updownarrow \qquad\qquad\qquad\qquad \mapsto$$

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

Deligne's equivalence

Theorem (Deligne '69)

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

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

Remark

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

Deligne's equivalence: square-free case

Fix a **ordinary square-free** characteristic q-Weil polynomial h.

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

Deligne's equivalence: square-free case

Fix a **ordinary square-free** characteristic q-Weil polynomial h.

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

Put

$$K := \mathbb{Q}[x]/(h) \text{ and } F := x \bmod h.$$

Deligne's equivalence: square-free case

Fix a **ordinary square-free** characteristic q-Weil polynomial h.

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

Put

$$K := \mathbb{Q}[x]/(h) \text{ and } F := x \bmod h.$$

Deligne's equivalence induces:

Theorem (M.)

$$\left\{ \textit{Ordinary abelian varieties over } \mathbb{F}_q \textit{ in } \mathscr{C}_h \right\}_{/\simeq}$$

$$\updownarrow$$

$$\left\{ \textit{fractional ideals of } \mathbb{Z}[F, q/F] \subset K \right\}_{/\simeq} \qquad =: \mathrm{ICM}(\mathbb{Z}[F, q/F])$$

ideal class monoid

ICM : Ideal Class Monoid

Let R be an order in a finite étale $\mathbb{Q}$-algebra K.

ICM : Ideal Class Monoid

Let R be an order in a finite étale $\mathbb{Q}$-algebra K.

- Recall: for fractional R-ideals I and J

$$I \simeq_R J \iff \exists x \in K^\times \text{ s.t. } xI = J$$

ICM : Ideal Class Monoid

Let R be an order in a finite étale $\mathbb{Q}$-algebra K.

- Recall: for fractional R-ideals I and J

$$I \simeq_R J \iff \exists x \in K^\times \text{ s.t. } xI = J$$

- Define the **ideal class monoid** of R as

$$\mathrm{ICM}(R) := {}^{\{\text{fractional } R\text{-ideals}\}}\!\big/_{\simeq_R}$$

ICM : Ideal Class Monoid

Let R be an order in a finite étale $\mathbb{Q}$-algebra K.

- Recall: for fractional R-ideals I and J

$$I \simeq_R J \Longleftrightarrow \exists x \in K^\times \text{ s.t. } xI = J$$

- Define the **ideal class monoid** of R as

$$\mathrm{ICM}(R) := {\{\text{fractional } R\text{-ideals}\}}\big/_{\simeq_R}$$

- We have

$$\mathrm{ICM}(R) \supseteq \mathrm{Pic}(R) \qquad \text{with equality iff } R = \mathcal{O}_K$$

ICM : Ideal Class Monoid

Let R be an order in a finite étale $\mathbb{Q}$-algebra K.

- Recall: for fractional R-ideals I and J

$$I \simeq_R J \iff \exists x \in K^\times \text{ s.t. } xI = J$$

- Define the **ideal class monoid** of R as

$$\mathrm{ICM}(R) := {}^{\{\text{fractional } R\text{-ideals}\}}\!\big/_{\simeq_R}$$

- We have

$$\mathrm{ICM}(R) \supseteq \mathrm{Pic}(R) \qquad \text{with equality iff } R = \mathcal{O}_K$$

- ...and actually

$$\mathrm{ICM}(R) \supseteq \bigsqcup_{\substack{R \subseteq S \subseteq \mathcal{O}_K \\ \text{over-orders}}} \mathrm{Pic}(S) \qquad \text{with equality iff } R \text{ is Bass}$$

Study the isomorphism problem locally: (Dade, Taussky, Zassenhaus '62)

simplify the problem

Study the isomorphism problem locally: (Dade, Taussky, Zassenhaus '62)

- **weak equivalence**:

$$I_{\mathfrak{p}} \simeq_{R_{\mathfrak{p}}} J_{\mathfrak{p}} \text{ for every } \mathfrak{p} \in \mathrm{mSpec}(R)$$

simplify the problem

Study the isomorphism problem locally: (Dade, Taussky, Zassenhaus '62)

- **weak equivalence**:

$$I_{\mathfrak{p}} \simeq_{R_{\mathfrak{p}}} J_{\mathfrak{p}} \text{ for every } \mathfrak{p} \in \mathrm{mSpec}(R)$$

$$\Updownarrow$$

$$1 \in (I : J)(J : I) \quad \text{easy to check!}$$

simplify the problem

Study the isomorphism problem locally: (Dade, Taussky, Zassenhaus '62)

- **weak equivalence**:

$$I_{\mathfrak{p}} \simeq_{R_{\mathfrak{p}}} J_{\mathfrak{p}} \text{ for every } \mathfrak{p} \in \mathrm{mSpec}(R)$$

$$\Updownarrow$$

$$1 \in (I : J)(J : I) \quad \text{easy to check!}$$

- Let $\mathscr{W}(R)$ be the set of weak eq. classes...

simplify the problem

Study the isomorphism problem locally: (Dade, Taussky, Zassenhaus '62)

- **weak equivalence**:

$$I_{\mathfrak{p}} \simeq_{R_{\mathfrak{p}}} J_{\mathfrak{p}} \text{ for every } \mathfrak{p} \in \mathrm{mSpec}(R)$$

$$\Updownarrow$$

$$1 \in (I:J)(J:I) \quad \text{easy to check!}$$

- Let $\mathscr{W}(R)$ be the set of weak eq. classes...
  ...whose representatives can be found in

$$\left\{ \text{sub-}R\text{-modules of } {}^{\mathcal{O}_K}\!\big/\!{}_{\mathfrak{f}_R} \right\} \quad \text{finite! and most of the time not-too-big ...}$$

Compute ICM(R)

Compute $\mathrm{ICM}(R)$

Partition w.r.t. the multiplicator ring:

$$\mathscr{W}(R) = \bigsqcup_{R\subseteq S\subseteq \mathscr{O}_K} \overline{\mathscr{W}}(S)$$

$$\mathrm{ICM}(R) = \bigsqcup_{R\subseteq S\subseteq \mathscr{O}_K} \overline{\mathrm{ICM}}(S)$$

Compute $\mathrm{ICM}(R)$

Partition w.r.t. the multiplicator ring:

$$\mathscr{W}(R) = \bigsqcup_{R \subseteq S \subseteq \mathscr{O}_K} \overline{\mathscr{W}}(S)$$

$$\mathrm{ICM}(R) = \bigsqcup_{R \subseteq S \subseteq \mathscr{O}_K} \overline{\mathrm{ICM}}(S)$$

the “bar” means “only classes with multiplicator ring S”

Compute $\mathrm{ICM}(R)$

Partition w.r.t. the multiplicator ring:

$$\mathcal{W}(R) = \bigsqcup_{R \subseteq S \subseteq \mathcal{O}_K} \overline{\mathcal{W}}(S)$$

$$\mathrm{ICM}(R) = \bigsqcup_{R \subseteq S \subseteq \mathcal{O}_K} \overline{\mathrm{ICM}}(S)$$

the "bar" means "only classes with multiplicator ring S"

Theorem (M.)

For every over-order S of R, $\mathrm{Pic}(S)$ acts freely on $\overline{\mathrm{ICM}(S)}$ and

$$\overline{\mathcal{W}}(S) = \overline{\mathrm{ICM}(S)} / \mathrm{Pic}(S)$$

Compute $\mathrm{ICM}(R)$

Partition w.r.t. the multiplicator ring:

$$\mathcal{W}(R) = \bigsqcup_{R\subseteq S\subseteq \mathcal{O}_K} \overline{\mathcal{W}}(S)$$

$$\mathrm{ICM}(R) = \bigsqcup_{R\subseteq S\subseteq \mathcal{O}_K} \overline{\mathrm{ICM}}(S)$$

the "bar" means "only classes with multiplicator ring S"

Theorem (M.)

For every over-order S of R, $\mathrm{Pic}(S)$ acts freely on $\overline{\mathrm{ICM}(S)}$ and

$$\overline{\mathcal{W}}(S) = \overline{\mathrm{ICM}(S)}/\mathrm{Pic}(S)$$

Repeat for every $R \subseteq S \subseteq \mathcal{O}_K$:

$$\rightsquigarrow \mathrm{ICM}(R).$$

back to AV's: Dual variety/Polarization

Howe ('95) defined a notion of **dual** module and of **polarization** in the category of Deligne modules.

Theorem (M.)

If $A \leftrightarrow I$, then:

back to AV's: Dual variety/Polarization

Howe ('95) defined a notion of **dual** module and of **polarization** in the category of Deligne modules.

Theorem (M.)

If $A \leftrightarrow I$, then:

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

back to AV's: Dual variety/Polarization

Howe ('95) defined a notion of **dual** module and of **polarization** in the category of Deligne modules.

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

Howe ('95) defined a notion of **dual** module and of **polarization** in the category of Deligne modules.

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

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

back to AV's: Dual variety/Polarization

Howe ('95) defined a notion of **dual** module and of **polarization** in the category of Deligne modules.

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

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

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

Example

- Let $h(x) = x^8 - 5x^7 + 13x^6 - 25x^5 + 44x^4 - 75x^3 + 117x^2 - 135x + 81$.
- $\rightsquigarrow$ isogeny class of an simple ordinary abelian varieties over $\mathbb{F}_3$ of dimension 4.
- Let F be a root of $h(x)$ and put $R := \mathbb{Z}[F, 3/F] \subset \mathbb{Q}(F)$.
- 8 over-orders of R: two of them are not Gorenstein.
- $\#\mathrm{ICM}(R) = 18 \rightsquigarrow 18$ isom. classes of AV in the isogeny class.
- 5 are not invertible in their multiplicator ring.
- 8 classes admit principal polarizations.
- 10 isomorphism classes of princ. polarized AV.

Example

Concretely:

$$
\begin{aligned}
I_1 =& 2645633792595191\mathbb{Z} \oplus (F + 836920075614551)\mathbb{Z} \oplus (F^2 + 1474295643839839)\mathbb{Z} \oplus \\
&\oplus (F^3 + 1372829830503387)\mathbb{Z} \oplus (F^4 + 1072904687510)\mathbb{Z} \oplus \\
&\oplus \frac{1}{3}(F^5 + F^4 + F^3 + 2F^2 + 2F + 670480698614361 0)\mathbb{Z} \oplus \\
&\oplus \frac{1}{9}(F^6 + F^5 + F^4 + 8F^3 + 2F^2 + 2991665243621169)\mathbb{Z} \oplus \\
&\oplus \frac{1}{27}(F^7 + F^6 + F^5 + 17F^4 + 20F^3 + 9F^2 + 68015312518722201)\mathbb{Z}
\end{aligned}
$$

principal polarizations:

$$
\begin{aligned}
x_{1,1} = \frac{1}{27}(&-121922F^7 + 588604F^6 - 1422437F^5 + \\
&+ 1464239F^4 + 1196576F^3 - 7570722F^2 + 15316479F - 12821193) \\
x_{1,2} = \frac{1}{27}(&3015467F^7 - 17689816F^6 + 35965592F^5 - \\
&- 64660346F^4 + 121230619F^3 - 191117052F^2 + 315021546F - 300025458)
\end{aligned}
$$

$$
\mathrm{End}(I_1) = R
$$

$$
\#\mathrm{Aut}(I_1, x_{1,1}) = \#\mathrm{Aut}(I_1, x_{1,2}) = 2
$$

Example

$$
\begin{aligned}
I_7 =& 2\mathbb{Z} \oplus (F+1)\mathbb{Z} \oplus (F^2+1)\mathbb{Z} \oplus (F^3+1)\mathbb{Z} \oplus (F^4+1)\mathbb{Z} \oplus \frac{1}{3}(F^5+F^4+F^3+2F^2+2F+3)\mathbb{Z}\oplus \\
&\oplus \frac{1}{36}(F^6+F^5+10F^4+26F^3+2F^2+27F+45)\mathbb{Z}\oplus \\
&\oplus \frac{1}{216}(F^7+4F^6+49F^5+200F^4+116F^3+105F^2+198F+351)\mathbb{Z}
\end{aligned}
$$

principal polarization:

$$x_{7,1} = \frac{1}{54}(20F^7-43F^6+155F^5-308F^4+580F^3-1116F^2+2205F-1809)$$

$$
\begin{aligned}
\mathrm{End}(I_7) = & \mathbb{Z} \oplus F\mathbb{Z} \oplus F^2\mathbb{Z} \oplus F^3\mathbb{Z} \oplus F^4\mathbb{Z} \oplus \frac{1}{3}(F^5+F^4+F^3+2F^2+2F)\mathbb{Z}\oplus \\
&\oplus \frac{1}{18}(F^6+F^5+10F^4+8F^3+2F^2+9F+9)\mathbb{Z}\oplus \\
&\oplus \frac{1}{108}(F^7+4F^6+13F^5+56F^4+80F^3+33F^2+18F+27)\mathbb{Z}
\end{aligned}
$$

$$\#\mathrm{Aut}(I_7, x_{7,1}) = 2$$

I_1 is invertible in R, but I_7 is not invertible in $\mathrm{End}(I_7)$.

some results from computations

	isogeny cl.	isom.cl.	isom.cl. no p.pol.	isom.cl. w/p.pol.	isom.w/ End $= \mathscr{O}_K$	isom.cl. no p.pol. End $= \mathscr{O}_K$
$\mathbb{F}_2, g=2$	14/34	21	7	15	15	3
$\mathbb{F}_3, g=2$	36/62	76	23	59	43	6
$\mathbb{F}_5, g=2$	94/128	457	207	286	159	34
$\mathbb{F}_7, g=2$	168/207	1324	638	795	387	88
$\mathbb{F}_{11}, g=2$	352/400	4925	2675	2797	1476	459
$\mathbb{F}_2, g=3$	82/210	226	102	142	112	16
$\mathbb{F}_3, g=3$	366/670	2508	1287	1492	874	187
$\mathbb{F}_5, g=3$	439/2994	30867	24693	7013	836	206
$\mathbb{F}_7, g=3$	267/7968	26506	21557	5674	721	180
$\mathbb{F}_{11}, g=3$	188/30530	18513	14291	4830	614	150

black = all ordinary squarefree isogeny classes have been computed
red = work in progress

Final remarks

- Using Centeleghe-Stix '15 we can compute the isomorphism classes in $\mathscr{C}_h$ over $\mathbb{F}_p$ where h is **square-free** and **without real roots**.

Final remarks

- Using Centeleghe-Stix '15 we can compute the isomorphism classes in $\mathscr{C}_h$ over $\mathbb{F}_p$ where h is **square-free** and **without real roots**.
  much larger subcategory!!! ... but no polarizations in this case.

Final remarks

- Using Centeleghe-Stix '15 we can compute the isomorphism classes in $\mathscr{C}_h$ over $\mathbb{F}_p$ where h is **square-free** and **without real roots**.
  much larger subcategory!!! ... but no polarizations in this case.
- we can also deal with the case $\mathscr{C}_{h^d}$ (with h square-free) when $\mathbb{Z}[F, q/F]$ is Bass (soon on arXiv).

Final remarks

- Using Centeleghe-Stix '15 we can compute the isomorphism classes in $\mathscr{C}_h$ over $\mathbb{F}_p$ where h is **square-free** and **without real roots**.
  much larger subcategory!!! ... but no polarizations in this case.
- we can also deal with the case $\mathscr{C}_{h^d}$ (with h square-free) when $\mathbb{Z}[F, q/F]$ is Bass (soon on arXiv).
- base field extensions (ordinary case).

Final remarks

- Using Centeleghe-Stix '15 we can compute the isomorphism classes in $\mathscr{C}_h$ over $\mathbb{F}_p$ where h is **square-free** and **without real roots**.
  much larger subcategory!!! ... but no polarizations in this case.
- we can also deal with the case $\mathscr{C}_{h^d}$ (with h square-free) when $\mathbb{Z}[F, q/F]$ is Bass (soon on arXiv).
- base field extensions (ordinary case).
- period matrices (ordinary case) of the canonical lift.

Thank you!