Computing isomorphism classes of abelian varieties over finite fields

Stefano Marseglia

Stockholm University

AGC^{2}T, 21 June 2017

Introduction

- Goal: describe an algorithm to compute **isomorphism classes** of (principally polarized) abelian varieties over a finite field.

Introduction

- Goal: describe an algorithm to compute **isomorphism classes** of (principally polarized) abelian varieties over a finite field.
- We start from the **isogeny** classification (**Honda-Tate**): pick $A/\mathbb{F}_q$ and let $h_A(x)$ be the characteristic polynomial of the Frob_A acting on $T_l A$. We have

$$A \sim_{\mathbb{F}_q} B_1^{n_1} \cdots B_r^{n_r},$$

where the B_i's are simple and pairwise non-isogenous, and

$$h_A(x) = h_{B_1}(x)^{n_1} \cdots h_{B_r}(x)^{n_r},$$

where the $h_{B_i}(x)$'s are (specific) powers of irreducible q-Weil polynomials.

Deligne's equivalence

Theorem (Deligne '69)

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

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

Remark

- $T(A) := H_1(\tilde{A} \otimes_\epsilon \mathbb{C})$, *where* $\tilde{A}/W(\mathbb{F}_q)$ *is the canonical lift;*
- *If* $\dim(A) = g$ *then* $\mathrm{rk}_{\mathbb{Z}}(T(A)) = 2g$*;*
- $\mathrm{Frob}(A) \rightsquigarrow F(A)$.

Deligne's equivalence

Fix a **square-free** characteristic q-Weil polynomial $h(x)$.
Let $\mathscr{C}_h$ be the corresponding isogeny class.
Let K be the étale algebra $\mathbb{Q}[x]/(h(x))$ and put $F := x \bmod (h(x))$.

Deligne's equivalence

Fix a **square-free** characteristic q-Weil polynomial $h(x)$.
Let $\mathscr{C}_h$ be the corresponding isogeny class.
Let K be the étale algebra $\mathbb{Q}[x]/(h(x))$ and put $F := x \bmod (h(x))$.
Deligne's equivalence induces:

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

$$\updownarrow$$

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

Centeleghe/Stix's equivalence

Theorem (Centeleghe/Stix 2015)

There is an equivalence of categories:

$$\left\{\begin{matrix}\textit{Abelian varieties over } \mathbb{F}_p \textit{ such that } \sqrt{p} \\ \textbf{\textit{does not belong}} \textit{ to their Weil support}\end{matrix}\right\}$$

$$\updownarrow$$

$$\left\{\begin{array}{l}\textit{pairs } (T,F), \textit{ where } T \simeq_{\mathbb{Z}} \mathbb{Z}^{2g} \textit{ and } T \xrightarrow{F} T \textit{ s.t.} \\ \textit{- } F\otimes\mathbb{Q} \textit{ is semisimple} \\ \textit{- the roots of } \mathrm{char}_{F\otimes\mathbb{Q}}(x) \textit{ have abs. value } \sqrt{p} \\ \textit{- } \sqrt{p} \textbf{\textit{ is not a root of }} \mathrm{char}_{F\otimes\mathbb{Q}}(x) \\ \textit{- } \exists V : T \to T \textit{ such that } FV = VF = p\end{array}\right\}$$

Centeleghe/Stix's equivalence

Theorem (Centeleghe/Stix 2015)

There is an equivalence of categories:

$$\left\{\begin{matrix}\textit{Abelian varieties over } \mathbb{F}_p \textit{ such that } \sqrt{p} \\ \textbf{\textit{does not belong}} \textit{ to their Weil support}\end{matrix}\right\}$$

$$\updownarrow$$

$$\left\{\begin{array}{l}\textit{pairs } (T,F), \textit{ where } T \simeq_{\mathbb{Z}} \mathbb{Z}^{2g} \textit{ and } T \xrightarrow{F} T \textit{ s.t.} \\ \textit{- } F\otimes\mathbb{Q} \textit{ is semisimple} \\ \textit{- the roots of } \mathrm{char}_{F\otimes\mathbb{Q}}(x) \textit{ have abs. value } \sqrt{p} \\ \textit{- } \sqrt{p} \textbf{\textit{ is not a root of }} \mathrm{char}_{F\otimes\mathbb{Q}}(x) \\ \textit{- } \exists V : T \to T \textit{ such that } FV = VF = p\end{array}\right\}$$

For a p-Weil **square-free** characteristic polynomial h with $h(\sqrt{p}) \neq 0$:

$$\{\text{Abelian varieties in } \mathscr{C}_h\}_{/\simeq} \longleftrightarrow \mathrm{ICM}(\mathbb{Z}[F, p/F])$$

ICM : Ideal Class Monoid

Let R be an order in a étale $\mathbb{Q}$-algebra K and $\mathscr{O}_K$ the ring of integers of 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

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

ICM : Ideal Class Monoid

Let R be an order in a étale $\mathbb{Q}$-algebra K and $\mathcal{O}_K$ the ring of integers of 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

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

- $\mathrm{ICM}(R)$ is a finite monoid: use the Minkowski bound: SLOW!
- $$\mathrm{ICM}(R) \supseteq \bigsqcup_{R \subseteq S \subseteq \mathcal{O}_K} \mathrm{Pic}(S).$$

Weak equivalence

Theorem (Dade, Taussky, Zassenhaus '62)

Two fractional R-ideals I and J are ***weakly equivalent*** *($I \sim_{wk} J$) if one of the following equivalent conditions hold:*

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

(2) $1 \in (I : J)(J : I)$;

(3) $(I : I) = (J : J)$ *and* $\exists$ *an invertible* $(I : I)$*-ideal* L *s.t.* $I = LJ$.

Weak equivalence

Theorem (Dade, Taussky, Zassenhaus '62)

*Two fractional R-ideals I and J are **weakly equivalent** ($I \sim_{wk} J$) if one of the following equivalent conditions hold:*

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

(2) $1 \in (I:J)(J:I)$;

(3) $(I:I) = (J:J)$ *and* $\exists$ *an invertible* $(I:I)$*-ideal* L *s.t.* $I = LJ$.

Notation: for any order R:

- $\mathscr{W}(R) := {\{\text{fractional } R\text{-ideals}\}}/{\sim_{\mathrm{wk}}}$;
- $\overline{\mathscr{W}}(R) := {\{\text{fractional } R\text{-ideals } I \text{ with } (I:I) = R\}}/{\sim_{\mathrm{wk}}}$;
- $\overline{\mathrm{ICM}}(R) := {\{\text{fractional } R\text{-ideals } I \text{ with } (I:I) = R\}}/{\simeq_R}$

Compute $\mathscr{W}(R)$ and $\mathrm{ICM}(R)$

Let $\mathfrak{f}_R = (R : \mathcal{O}_K)$ be the conductor of R and I a fractional R-ideal. Without changing the weak eq. class, we can assume that

$$I\mathcal{O}_K = \mathcal{O}_K.$$

Hence $\mathfrak{f}_R \subseteq I \subseteq \mathcal{O}_K$, and therefore:

Compute $\mathscr{W}(R)$ and $\mathrm{ICM}(R)$

Let $\mathfrak{f}_R = (R : \mathscr{O}_K)$ be the conductor of R and I a fractional R-ideal. Without changing the weak eq. class, we can assume that

$$I\mathscr{O}_K = \mathscr{O}_K.$$

Hence $\mathfrak{f}_R \subseteq I \subseteq \mathscr{O}_K$, and therefore:

$$\mathscr{W}(R) \overset{\sim_{\text{wk}}}{\twoheadleftarrow} \{ \text{ fractional } R\text{-ideals } I \, : \, I\mathscr{O}_K = \mathscr{O}_K \}$$

$$\begin{array}{c} \cap\!\! | \\ \left\{ \text{sub-}R\text{-modules of } {}^{\mathscr{O}_K}\!\big/_{\mathfrak{f}_R} \right\} \end{array}$$

Compute $\mathscr{W}(R)$ and $\mathrm{ICM}(R)$

Let $\mathfrak{f}_R = (R : \mathscr{O}_K)$ be the conductor of R and I a fractional R-ideal. Without changing the weak eq. class, we can assume that

$$I\mathscr{O}_K = \mathscr{O}_K.$$

Hence $\mathfrak{f}_R \subseteq I \subseteq \mathscr{O}_K$, and therefore:

$$\mathscr{W}(R) \overset{\sim_{\mathrm{wk}}}{\twoheadleftarrow} \left\{ \text{fractional } R\text{-ideals } I \,:\, I\mathscr{O}_K = \mathscr{O}_K \right\}$$

$$\rotatebox{90}{$\supseteq$}$$

$$\left\{ \text{sub-}R\text{-modules of } {}^{\mathscr{O}_K}\!/\!_{\mathfrak{f}_R} \right\}$$

Theorem

The action of $\mathrm{Pic}(R)$ *on* $\overline{\mathscr{W}}(R)$ *is free and transitive and the orbit is precisely* $\overline{\mathrm{ICM}}(R)$*. In particular, we can compute:*

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

Dual variety/Polarization

- Howe defined a notion of **dual** module and of **polarization** in the category of Deligne modules (**ordinary** case).

Dual variety/Polarization

- Howe defined a notion of **dual** module and of **polarization** in the category of Deligne modules (**ordinary** case).
- In the isogeny class $\mathscr{C}_h$ with h square-free and ordinary

$$A \leftrightarrow I \Longrightarrow A^{\vee} \leftrightarrow \overline{I}^{t}$$

Dual variety/Polarization

- Howe defined a notion of **dual** module and of **polarization** in the category of Deligne modules (**ordinary** case).
- In the isogeny class $\mathscr{C}_h$ with h square-free and ordinary

$$A \leftrightarrow I \Longrightarrow A^\vee \leftrightarrow \overline{I}^t$$

- a polarization 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.

Dual variety/Polarization

- Howe defined a notion of **dual** module and of **polarization** in the category of Deligne modules (**ordinary** case).
- In the isogeny class $\mathscr{C}_h$ with h square-free and ordinary

$$A \leftrightarrow I \Longrightarrow A^\vee \leftrightarrow \overline{I}^t$$

- a polarization 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.
- if $A \leftrightarrow I$ admits a principal polarization and $S := (I : I)$ then

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

and $\mathrm{Aut}(A, \lambda) = \{\text{torsion units of } S\}$

Example : Elliptic curves

For elliptic curves the number of isomorphism classes can be expressed as a closed formula (Deuring, Waterhouse).
Let $h(x) = x^2 + \beta x + q$, with $q = p^r$ and β an integer coprime with p such that $\beta^2 < 4q$.
Put $F := x \bmod (h(x))$ in $K := \mathbb{Q}[x]/(h)$.
Then $\mathbb{Z}[F] = \mathbb{Z}[F, q/F]$ and

$$\mathrm{ICM}(\mathbb{Z}[F]) = \bigsqcup_{n|f} \mathrm{Pic}(\mathbb{Z} + n\mathcal{O}_K)$$

where $f := \#(\mathcal{O}_K : \mathbb{Z}[F])$, which implies that

$$\#\left\{\begin{matrix}\text{iso. classes of ell. curves} \\ \text{with } q-1+\beta \ \mathbb{F}_q\text{-points}\end{matrix}\right\} = \frac{\#\mathrm{Pic}(\mathcal{O}_K)}{\#\mathcal{O}_K^\times} \sum_{n|f} n \prod_{p|n} \left(1 - \frac{\Delta_K}{p} \frac{1}{p}\right)$$

Example : higher dimension

- 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 α be a root of $h(x)$ and put $R := \mathbb{Z}[\alpha, 3/\alpha] \subset \mathbb{Q}(\alpha)$;
- 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:

$$
\begin{aligned}
I_1 =& 2645633792595191\mathbb{Z} \oplus (\alpha + 836920075614551)\mathbb{Z} \oplus (\alpha^2 + 1474295643839839)\mathbb{Z}\oplus \\
&\oplus (\alpha^3 + 1372829830503387)\mathbb{Z} \oplus (\alpha^4 + 1072904687510)\mathbb{Z}\oplus \\
&\oplus \frac{1}{3}(\alpha^5 + \alpha^4 + \alpha^3 + 2\alpha^2 + 2\alpha + 670480698614361 0)\mathbb{Z}\oplus \\
&\oplus \frac{1}{9}(\alpha^6 + \alpha^5 + \alpha^4 + 8\alpha^3 + 2\alpha^2 + 2991665243621169)\mathbb{Z}\oplus \\
&\oplus \frac{1}{27}(\alpha^7 + \alpha^6 + \alpha^5 + 17\alpha^4 + 20\alpha^3 + 9\alpha^2 + 680153125187222 01)\mathbb{Z}
\end{aligned}
$$

principal polarizations:

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

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

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

Example

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

principal polarization:

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

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

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

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