Computing isomorphism classes of abelian varieties over finite fields.

Stefano Marseglia

Utrecht University

Simons Collaboration - May meeting

Abelian varieties

- An **abelian variety** over a field k is a connected projective group scheme over k.
- Our goal: compute k-isomorphism classes of AVs for $k = \mathbb{F}_q$.
- eg. AVs of dim 1 are elliptic curves:

$$ZY^2 = X^3 + AXZ^2 + BZ^3, \quad 4A^3 + 27B^2 \neq 0$$

- In higher dim: equations are too big.
- First step is to simplify the problem: work up to **isogeny** (=surjective homomorphism with finite kernel).

Isogeny classification over $\mathbb{F}_q$

- $A/\mathbb{F}_q$ comes with a **Frobenius** endomorphism, that induces an action

$$\mathrm{Frob}_A : T_\ell A \to T_\ell A \text{ for any } \ell \neq p,$$

where $T_\ell(A) = \varprojlim A[\ell^n] \simeq \mathbb{Z}_\ell^{2g}$.
- $h_A(x) := \mathrm{char}(\mathrm{Frob}_A)$ is a q-Weil polynomial and **isogeny invariant**.
- By **Honda-Tate** theory,

$$A \sim_{\mathbb{F}_q} B \Longleftrightarrow h_A(x) = h_B(x),$$

and using the association

$$\text{isogeny classes of } A \longmapsto h_A(x)$$

allows us to enumerate all AVs up to isogeny
(see Dupuy-Kedlaya-Roe-Vincent and LMFDB).
- Also, $h_A(x)$ is squarefree $\iff$ $\mathrm{End}_{\mathbb{F}_q}(A)$ is commutative.

Squarefree case: Deligne ('69) and Centeleghe-Stix ('15)

- Fix a **squarefree** char. poly. h which is **ordinary** or with $q = p$ **prime**.
- $\rightsquigarrow$ an isogeny class $\mathscr{C}_h/\mathbb{F}_q$.
- Put $K := \mathbb{Q}[x]/(h) = \mathbb{Q}[F]$, an étale algebra = product of number fields.
- Put $V = q/F$.
- Deligne and C-S's results give:

Theorem

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

$$\updownarrow$$

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

ideal class monoid

- Problem: $\mathbb{Z}[F,V]$ might not be maximal $\rightsquigarrow$ non-invertible ideals.

ICM : Ideal Class Monoid

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

- Recall: for **fractional** R**-ideals** I and J

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

- We have

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

with equality $\updownarrow$ iff $R = \mathcal{O}_K$

- ...and actually

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

simplify the problem

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

- **weak equivalence**:

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

$$\Updownarrow$$

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

- We denote the set of weak eq. classes by $\mathscr{W}(R)$.
- If I and J are weakly equivalent (or isomorphic) then ...
  ... they have the same **multiplicator ring**: $(I:I) = (J:J)$.

Compute $\mathrm{ICM}(R)$

Partition w.r.t. the multiplicator ring:

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

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

the "pedix" $-_S$ means "only classes with multiplicator ring S"

Theorem (M.)

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

$$\mathscr{W}_S(R) = \mathrm{ICM}_S(R) / \mathrm{Pic}(S).$$

To sum up:

To compute $\mathrm{ICM}(R)$, we need to:

1. compute the overorders $R \subseteq S \subseteq \mathscr{O}_K$ ...
   ... solved by Hofmann-Sircana '19.

2. for each such S, compute $\mathrm{Pic}(S)$ ...
   ... use:

$$1 \to S^\times \to \mathscr{O}_K^\times \to \frac{(\mathscr{O}_K/\mathfrak{f})^\times}{(S/\mathfrak{f})^\times} \to Pic(S) \to Pic(\mathscr{O}_K) \to 1$$

   where $\mathfrak{f} = (S : \mathscr{O}_K)$ is the conductor. See Klüners-Pauli '05.

3. for each S, compute $W_S(R)$, as I now will explain.

Weak equivalence classes

- Fix an overorder S of R.
- We compute $W_S(R)$ recursively.
- If $S = \mathcal{O}_K$ then $W_S(R)$ consists only of the class of $1 \cdot \mathcal{O}_K$.
- If $S \subsetneq \mathcal{O}_K$ then pick a non-invertible prime $\mathfrak{p}$ of S.
- Put $T = (\mathfrak{p} : \mathfrak{p}) \supsetneq S$ and let $J_1, \dots, J_n$ be the representatives of $W_T(R)$.
- Proposition: each class in $W_S(R)$ admits a representative I such that $IT = J_i$ for a unique i, which implies

$$\mathfrak{p}I = \mathfrak{p}J_i \subset I \subset J_i.$$

- Enough to list all the sub-$S/\mathfrak{p}$-vector spaces of $J_i/\mathfrak{p}J_i$.

back to AVs:

- To sum up:
- Given a **squarefree** q-Weil polynomial h which is ordinary or over the prime field...
- ... $\rightsquigarrow$ algorithm to compute the isomorphism classes of AVs in $\mathscr{C}_h$.
- See

  `https://github.com/stmar89/AlgEt`

  for a Magma package to compute the ideal class monoid of an order in an étale algebra. (Should appear in the next Magma release)

About the computation

- **input**: all ordinary, or over a prime field, squarefree isogeny classes of dimension g over $\mathbb{F}_q$ for:

$$\begin{array}{ll} g = 1 & q = 2, \ldots, 128 \\ g = 2 & q = 2, \ldots, 128 \\ g = 3 & q = 2, 3, 4, 5, 7, 8, 9, 16, 25 \\ g = 4 & q = 2, 3, 4 \\ g = 5 & q = 2 \end{array}$$

  for a total of 615.269 isogeny classes.
- **output**: got 1.659.022.602 isomorphism classes.

Some stats

	g=1	g=2	g=3	g=4	g=5
q=2	1	2	4	12	54
q=3	1	3	9	57	–
q=4	2	5	27	285	–
q=5	1	5	36	–	–
q=7	2	8	97	–	–
q=8	2	17	259	–	–
q=9	2	14	242	–	–
q=11	2	15	–	–	–
q=13	2	20	–	–	–
q=16	4	53	2352	–	–
q=17	2	29	–	–	–
q=19	2	35	–	–	–
q=23	2	47	–	–	–
q=25	3	63	5024	–	–

Table: (rounded) average number of isomorphism classes per isogeny class.

Some stats

	g=1	g=2	g=3	g=4	g=5
q=2	1	1	1	1	4
q=3	1	1	2	8	–
q=4	1	2	4	48	–
q=5	1	2	4	–	–
q=7	2	4	24	–	–
q=8	3	6	36	–	–
q=9	2	8	48	–	–
q=11	1	4	–	–	–
q=13	2	8	–	–	–
q=16	4	16	480	–	–
q=17	1	8	–	–	–
q=19	2	16	–	–	–
q=23	1	12	–	–	–
q=25	2	24	1440	–	–

Table: most frequent size

Some stats

	g=1	g=2	g=3	g=4	g=5
q=2	1	5	40	668	7849
q=3	2	10	162	9188	–
q=4	2	20	1404	346064	–
q=5	2	29	2196	–	–
q=7	2	66	15824	–	–
q=8	3	180	44226	–	–
q=9	3	136	39960	–	–
q=11	4	142	–	–	–
q=13	4	220	–	–	–
q=16	5	832	2271240	–	–
q=17	4	672	–	–	–
q=19	4	568	–	–	–
q=23	6	1184	–	–	–
q=25	6	935	8674136	–	–

Table: max. number of isomorphism classes per isogeny class.

Thank you!