Products and Polarizations of Super-Isolated Abelian Varieties

Stefano Marseglia

Utrecht University

Simon Fraser University - (Q)NTAG - 03 December 2020

Today's plan:

- Quick intro: Abelian Varieties
- Super-Isolated Abelian Varieties (SIAV)
  - Weil generators
  - *ideal* varieties : equivalence of categories
- Products of SIAV
- Principal Polarization on SIAV
- Applications (powers and Jacobians)

Also, all morphisms are defined over the field of definition!
Joint work with Travis Scholl.

Abelian Varieties

- An abelian variety A over a field k is a projective geometrically connected group variety over k.
  We have morphisms $\oplus : A \times A \to A$, $\ominus : A \to A$ and a k-rational point $e \in A(k)$ such that $(A, \oplus, \ominus, e)$ is a group object in the category of projective geom. connected varieties over k.
- In practice, we have diagrams $\rightsquigarrow$ “natural” group structure on $A(\overline{k})$.
- eg. ($\ominus$ is the “inverse” morphism)

$$
\begin{tikzcd}
A \times_k A \arrow[rr, "(\ominus,\mathrm{id})"] & & A \times_k A \arrow[d, "\oplus"] \\
A \arrow[u, "\Delta"] \arrow[r] & \mathrm{Spec}(k) \arrow[r, "e"] & A
\end{tikzcd}
\qquad
\begin{tikzcd}
A \times_k A \arrow[rr, "(\mathrm{id},\ominus)"] & & A \times_k A \arrow[d, "\oplus"] \\
A \arrow[u, "\Delta"] \arrow[r] & \mathrm{Spec}(k) \arrow[r, "e"] & A
\end{tikzcd}
$$

Example : $\dim A = 1$ elliptic curves

- AVs of dimension 1 are called Elliptic Curves.
- They admit a plane model: if $\operatorname{char} k \neq 2,3$

$$Y^2Z = X^3 + AXZ^2 + BZ^3 \quad A, B \in k \text{ and } e = [0:1:0]$$

- The groups law is explicit:
  if $P = (x_P, y_P)$ then $\ominus P = (x_P, -y_P)$ and
  if $Q = (x_Q, y_Q) \neq \ominus P$ then $P \oplus Q = (x_R, y_R)$ where

$$x_R = \lambda^2 - x_P - x_Q, \quad y_R = y_P + \lambda(x_R - x_P),$$

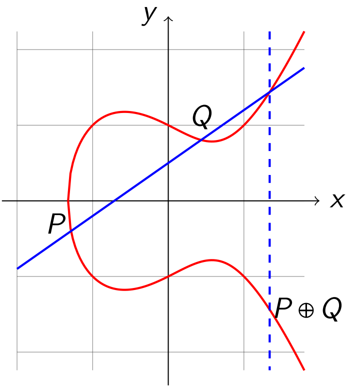
where

$$\lambda = \begin{cases} \frac{3x_P^2 + B}{2A} & \text{if } P = Q \\ \frac{y_P - y_Q}{x_P - x_Q} & \text{if } P \neq Q \end{cases}$$

Over $\mathbb{R}$:
consider the abelian variety:

$$y^2 = x^3 - x + 1$$

Addition law: $P, Q \rightsquigarrow P \oplus Q$



Motivation: why SIAV?

- Super-Isolated AVs (SIAV) where introduced by Scholl in the context of Elliptic Curves Cryptography:
- ECDLP: Consider $E/\mathbb{F}_p$. Pick $P, Q \in E(\mathbb{F}_p)$. Solve

$$kP = Q.$$

- Fastest 'general' attack is Pollard $\rho \rightsquigarrow O(\sqrt{p})$ running-time.

A possible attack:

- if there exists a 'computable' map $\varphi : E \to E'$ to a 'weak' curve E'...
- ... then one can move the ECDLP and crack it on E'.

Facts :

- 'computable' maps are common, 'weak' curves are not.

Prevention is better than cure:

- $\rightsquigarrow$ 'isolated' EC : small conductor gap = no 'computable' maps.
- $\rightsquigarrow$ 'super-isolated' EC : no maps at all! (to other EC)
- No reason to stick to dimension 1 : $\rightsquigarrow$ SIAV.

Some background : Isogeny classification

- A and B are isogenous if $\dim A = \dim B$ and $\exists$ a surjective hom. $\varphi : A \to B$.
- Being isogenous is an equivalence relation.
- $A/\mathbb{F}_q$ 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 $T_\ell(A) = \varprojlim A[\ell^n] \simeq \mathbb{Z}_\ell^{2d}$.

- $h_A(x) := \mathrm{char}(\mathrm{Frob}_A)$ is a q-Weil polynomial and isogeny invariant.
- By Honda-Tate theory, the association

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

is injective and allows us to list all isogeny classes.

SIAV : Definition

Let h be a char. polynomial $\rightsquigarrow \mathscr{C}_h$ isogeny class.

Definition

- *$\mathscr{C}_h$ is super-isolated if it contains only one isomorphism class.*
- *$A/\mathbb{F}_q$ is super-isolated if $\mathscr{C}_{h_A}$ is so.*

All information about A is encoded by the polynomial h_A.
Questions:

- How do we read from a q-Weil poly h whether $\mathscr{C}_h$ is super-isolated?
- Can we count super-isolated $\mathscr{C}_h$?
- What about polarizations?

Characterize SIAV

A special class of AVs

Definition

We say that $A/\mathbb{F}_q \in \mathscr{C}_{h_A}$ *is ideal if*

- h_A *is squarefree, i.e. splits into distinct irred. factors,* $\rightsquigarrow$ $A \sim B_1 \times \ldots \times B_s$, B_i *simple, pair-wise non-isogenous*
- h_A *has no real roots, and*
- A *is ordinary, or* $q = p = \mathrm{char}(\mathbb{F}_q)$. *ordinary :* $A[p](\overline{\mathbb{F}}_p) \simeq (\mathbb{Z}/p\mathbb{Z})^g$

Theorem (Deligne 1969, Centeleghe-Stix 2015)

Let $\mathscr{C}_h$ *be an ideal isogeny class. There is an equivalence of categories:*

$$\mathscr{C}_h \longleftrightarrow \left\{ \begin{array}{c} \textit{fractional-}\mathbb{Z}[\pi,\overline{\pi}]\textit{-ideals} \\ \textit{in the CM-étale algebra} \\ K_h = \mathbb{Q}[x]/(h) = \mathbb{Q}[\pi] \end{array} \right\}. \qquad \overline{\pi} = \frac{q}{\pi}$$

If $A \leftrightarrow J$ *then* $\mathrm{End}(A) \leftrightarrow (J:J) = \{z \in K_h : zJ \subseteq J\} \subseteq \mathscr{O}_K$.

Weil generators

Let K be an étale CM-$\mathbb{Q}$-algebra

$$K = K_1 \times \ldots \times K_r, \qquad K_i \text{ a CM-number field},$$

with ring of integers

$$\mathcal{O}_K = \mathcal{O}_{K_1} \times \ldots \times \mathcal{O}_{K_r},$$

and class group

$$\mathrm{Pic}(\mathcal{O}_K) = \mathrm{Pic}(\mathcal{O}_{K_1}) \times \ldots \times \mathrm{Pic}(\mathcal{O}_{K_r}).$$

Definition

Let $n \in \mathbb{Z}$. An n-Weil generator for K is an element $\alpha \in K$ such that

- $\alpha\overline{\alpha} = n$ *(i.e. in the image of the diagonal embedding $\mathbb{Z} \to K$),*
- $\mathcal{O}_K = \mathbb{Z}[\alpha, \overline{\alpha}]$.

ideal SIAV & Weil Generators

Theorem

Let $\mathscr{C}_h$ be an ideal isogeny class $\mathbb{F}_q$. Put $K_h = \mathbb{Q}[x]/(h) = \mathbb{Q}[\pi]$. Then:

$$\mathscr{C}_h \text{ is super-isolated} \iff \begin{cases} \pi \text{ is a } q\text{-Weil generator of } K_h, \text{ and} \\ K_h \text{ has class number } 1. \end{cases}$$

Proof: by the previous Theorem

$$\{\text{isom. classes in } \mathscr{C}_h\} \longleftrightarrow \{\text{ideal classes of } \mathbb{Z}[\pi, \overline{\pi}]\}.$$

Hence $\mathscr{C}_h$ is super-isolated iff

$$\mathbb{Z}[\pi, \overline{\pi}] = \mathscr{O}_{K_h} \text{ and } K_h \text{ has cl. number } 1.$$

QED

An example

Consider the polynomials

$$
\begin{aligned}
h_1(x) &= (x^4 - 2x^3 + 3x^2 - 4x + 4),\\
h_2(x) &= (x^6 - 4x^5 + 9x^4 - 15x^3 + 18x^2 - 16x + 8),\\
h_3(x) &= (x^6 - 3x^5 + 6x^4 - 9x^3 + 12x^2 - 12x + 8),\\
h_4(x) &= (x^8 - 5x^7 + 12x^6 - 20x^5 + 29x^4 - 40x^3 + 48x^2 - 40x + 16),\\
h_5(x) &= (x^8 - 5x^7 + 13x^6 - 25x^5 + 39x^4 - 50x^3 + 52x^2 - 40x + 16),\\
h_6(x) &= (x^8 - 4x^7 + 5x^6 + 2x^5 - 11x^4 + 4x^3 + 20x^2 - 32x + 16).
\end{aligned}
$$

Let $h = \prod_i h_i$ and put $K_h = \mathbb{Q}[x]/(h) = \mathbb{Q}[\pi]$. One computes that

$$\mathcal{O}_{K_h} = \mathbb{Z}[\pi, 2/\pi] \text{ and } \#\operatorname{Pic}(\mathcal{O}_{K_h}) = 1.$$

Hence $\mathscr{C}_h$ is an isogeny class of 20-dimensional SIAV over $\mathbb{F}_2$.

A non-example

Over $\mathbb{F}_5$ let

$$A = E_1 \times E_2,$$

where

$$E_1 : y^2 = x^3 + 4x + 2 \text{ and } E_2 : y^2 = x^3 + 3x + 2.$$

By the Theorem $\rightsquigarrow$ E_1 and E_2 are SIEC, but A is not!
Indeed:

$$\mathbb{Z}[\pi_A, \overline{\pi_A}] \subsetneq \mathscr{O}_{K_{h_A}} = \mathbb{Z}[\pi_1] \times \mathbb{Z}[\pi_2] = \mathrm{End}(A).$$

So there exists A' isogenous to A with $\mathrm{End}(A') = \mathbb{Z}[\pi_A, \overline{\pi_A}]$.
In particular A is not isomorphic to A'.

Count SIAV

How many Weil generators ? Simple case

For a number field K, for $z \in K$, we define the height of z as

$$h(z) = \max\{|\varphi(z)| : \varphi : K \to \mathbb{C}\}.$$

Theorem (Scholl 2020)

Let W be the set of Weil generator in a CM-field K of degree $2g$. Then

$$\#\{\alpha \in W : h(\alpha) \leq N\} = \begin{cases} 4N + O(1) & g = 1 \\ \rho \log N + O(1) & g = 2 \text{ and } W \neq \emptyset \\ O(1) & g \geq 3 \end{cases}$$

where ρ is a constant depending on K.

Idea of the proof: All Weil generators α of K can be written in a special form:

$$\alpha = \frac{u(\gamma - \overline{\gamma}) + \eta + a}{2},$$

for a fixed γ such that $\mathcal{O}_K = \mathcal{O}_F[\gamma]$, where F is the unique totally real subfield of K, and unique triple (u, η, a) with

- $u \in \mathcal{O}_F$.
- $\eta \in T = \{\beta : \mathcal{O}_F = \mathbb{Z}[\beta]\}$. Note T is finite (up to $\mathbb{Z}$-translation).
- $a \in \mathbb{Z}$.

Exploit this formula to enumerate the Weil generators.

How many Weil generators ? Non-simple case

Theorem

Let $K = K_1 \times \ldots \times K_n$ be a CM-algebra, with K_i number fields. If $n > 1$ then K has finitely many Weil generators.

Proof:

1. Enough to prove it for $K = K_1 \times K_2$.
2. Write Weil generators α_i of K_i as:
$$\alpha_i = \frac{u_i(\gamma_i - \overline{\gamma_i}) + \eta_i + a_i}{2}$$
3. Resultant condition: $\alpha = (\alpha_1, \alpha_2)$ is a Weil generator for K iff
$$|\mathrm{Res}(g_1, g_2)| = 1$$
where g_i is the minimal polynomial of $\alpha_i + \overline{\alpha_i}$.
4. We get 3 equations $\rightsquigarrow$ an affine variety X of $\dim X = 0$.
5. We conclude since $\{\text{Weil gens of } K\} \xrightarrow{\text{finite-to-1}} X(\mathbb{Z})$. QED

How many SIAV ?

Corollary

Let g be a positive integer. There are only finitely many ideal SIAV of dimension g which are not simple. In particular there are only finitely many finite fields $\mathbb{F}_q$ for which such a variety might exist.

Proof:

1. It is enough to count Weil generators for products of CM fields of class number 1.
2. Stark '74: For a given degree, only finitely many such fields. QED

The argument is constructive $\rightsquigarrow$ Algorithm.

A list : non-simple SIAV of small dimension over $\mathbb{F}_q$

q	1×1	1×2	$1\times 1\times 2$	$1\times 2\times 2$	2×2
2	4	24	10	12	18
3	4	24	6	12	18
4		2			
5	2	12		2	6
7		8			
8		2			
9		2			
11	2	8	2	4	4
13		6			
17	2	8	2		
19					2
32		2			
41		2			

q	1×1	1×2	$1 \times 1 \times 2$	$1 \times 2 \times 2$	2×2
47		4			
59		2			
61		2			
83	2				
101	2				
173		2			
227	2				
257	2				
283		2			
383		2			
1523	2				
1601	2				
18131		2			

Polarizations

Principal Polarizations for ordinary SIAV

- $A/\mathbb{F}_q$ be a simple ordinary SIAV of dimension g. $\rightsquigarrow$ A is ideal
- For $h = h_A$ let $K = \mathbb{Q}[x]/h = \mathbb{Q}(\pi)$.

Theorem

A does not admit a principal polarization if and only if $N_{K/\mathbb{Q}}(\pi - \overline{\pi}) = 1$ and the middle coefficient a_g of h is $-1 \bmod q$ if $q > 2$ and $-1 \bmod 4$ if $q = 2$.

Proof: In Howe '95 there is a characterization of when an ordinary isogeny class $\mathscr{C}_h$ contains a PPAV in terms of the ramification of K/F. Since A is SIAV, then $\mathscr{O}_K = \mathscr{O}_F[\pi]$, and hence $\mathrm{Diff}_{K/F} = (\pi - \overline{\pi})\mathscr{O}_F$. This allows us to conclude. QED

Uniqueness of Principal Polarizations

Theorem

Let A be a simple super-isolated ordinary abelian variety over $\mathbb{F}_q$ which admits a principal polarization. Then the polarization is unique up to polarized isomorphism.

Proof: The number of principal polarizations is given by the size of the quotient

$$\frac{U_F^+}{N_{K/F}(U_K)},$$

which is trivial since K has class number 1. QED

Corollary

Let A be an ordinary ideal SIAV, say $A = \prod_1^n A_i$ with A_i simple. Then A admits a principal polarization if and only if each A_i does. If this is the case, the principal polarization is unique up to polarized isomorphism.

Some applications

Powers of SIAVs

Theorem

Let $A/\mathbb{F}_q$ be an ideal abelian variety. If A is super-isolated, then A^n is super-isolated for every $n \geq 1$. Conversely, if there exists $n \geq 1$ such that A^n is super-isolated then A is super-isolated.

Proposition

Let A be a super-isolated abelian variety. Then A^8 is principally polarized.

Proof: use Zahrin's trick. QED

Remark

Let A be an ordinary ideal PPSIAV. Then A^n is PPSIAV for every $n > 1$, but the princ. polarization is not necessarily unique.

What about Jacobians ?

Proposition

Let C and C' be smooth, projective and geometrically integral curves of genus $g > 1$ defined over $\mathbb{F}_q$ with the same zeta function. Assume that $\mathrm{Jac}(C)$ *is ordinary, ideal, and super-isolated. Then the curves C and C' are isomorphic.*

Proof: $\mathrm{Jac}(C')$ is isogenous to $\mathrm{Jac}(C) \rightsquigarrow$ isomorphic since $\mathrm{Jac}(C)$ is SIAV.
Denote by θ and θ' the canonical princ. pols of $\mathrm{Jac}(C)$ and $\mathrm{Jac}(C')$.
We deduce that $(\mathrm{Jac}(C),\theta)$ is isomorphic to $(\mathrm{Jac}(C'),\theta')$.
By Torelli's Theorem $\rightsquigarrow C \simeq C'$.
QED

Thank you!