The module action on abelian varieties

2024/10/15 — Canari Seminar — Bordeaux

Damien Robert

Équipe Canari, Inria Bordeaux Sud-Ouest

université de BORDEAUX

Inria

Table of Contents

Ideals and isogenies: the oriented case

- $E_0/k, k = \mathbb{F}_q$, elliptic curve with a primitive orientation by a quadratic imaginary order $R = \mathbb{Z}[\sqrt{-\Delta}] \hookrightarrow \mathrm{End}_k(E_0)$
- Oriented isogeny: $\phi : E_1 \to E_2$ that commutes with the orientations
- Oriented kernel: K stable by R

  Unique R-orientation compatible on E/K with the quotient isogeny $E \to E/K$, and the isogeny is horizontal or ascending

Example: Frobenius orientation

- E_0/k with non trivial π_k-action: ordinary curves, supersingular curves over $\mathbb{F}_p$
- π_k-oriented isogenies = rational isogenies.

Kernels, isogenies, and ideals

- $I \mapsto \phi_I : E_0 \to E_I$ oriented isogeny with kernel $E_0[I] = \{P \in E_0(\bar{k}), \alpha(P) = 0, \forall \alpha \in I\}$
- $K \mapsto \mathfrak{I}(K) := \{\alpha \in R \mid \alpha(K) = 0\}$
- $I \to E_0[I] \Leftrightarrow K \mapsto \mathfrak{I}(K)$: bijections[1] between R-stable kernels and integral ideals I of R
- Ideals $\Leftrightarrow$ oriented isogenies
- $I \sim J \Leftrightarrow E_I \simeq E_J$

[1] At least in the separable case: $E_0[\pi_p]$ is not represented by an ideal if p inert in R

Class group actions

- $E_I := E_0/E_0[I]$ primitively oriented by $O(I) := \{\alpha \in R \otimes_{\mathbb{Z}} \mathbb{Q} \mid \alpha I \subset I\}$
- I is invertible $\Leftrightarrow O(I) = R \Leftrightarrow$ the isogeny is horizontal
- $\mathrm{Pic}(R) := \{[I], I \text{ invertible ideal}\}$

- Invertible ideals I of $R \Leftrightarrow$ oriented horizontal isogenies $\phi_I : E \to E_I$ [Colò-Kohel 2020, Onuki 2020]
- $\widetilde{\phi_I} = \phi_{\overline{I}} : E_I \to E$
- Special case: p inert in R (can only happen for an orientation on a supersingular curve $E/\mathbb{F}_{p^2}$)
- $\pi_p : E \to E^\sigma$ is not represented by an ideal
- An oriented isogeny $\phi : E \to E'$ comes from an ideal iff the representations $\rho_R(E)$ and $\rho_R(E')$ are equivalent, $\rho_R(E)$ representation of R on the k-vector space $T_0(E)$

Group action:

- $\mathrm{Pic}(R) \circlearrowright \{E \text{ primitively } R\text{-oriented}\}$
- $[I] \cdot E \mapsto E_I$
- Free and transitive action (if p ramified or split; two orbits if p inert in R)

- $E[\mathfrak{m}](\overline{k}) \simeq R/\mathfrak{m}R$ as R-modules [Lenstra 1996] $(p \wedge \mathfrak{m} = 1)$
- Generalised class group action (ray class groups modulo $\mathfrak{m}$) to incorporate $\mathfrak{m}$-level structure [ACELV 2024]

Applications of class group actions

- Let $\{E_1, \dots, E_N\}$ be the orbit of E_0 under $\mathrm{Pic}(R)$. Then $H(X) = \prod (X - j(E_i))$ is the reduction modulo p of the Hilbert class polynomial H_R.
- Reduction modulo p of CM class polynomials can also be understood in term of actions by the Shimura class group
- The CRS/ CSIDH key exchange:

$$\begin{array}{ccc} E_0 & \longrightarrow & E_{I_1} = I_1 \cdot E_0 \\ \downarrow & & \downarrow \\ E_{I_2} = I_2 \cdot E_0 & \longrightarrow & E_{I_1 \otimes_R I_2} \simeq I_1 I_2 \cdot E_0 \end{array}$$

As a commutative group action, susceptible to Kuperberg's subexponential quantum algorithm

Ideals and isogenies: the supersingular case

- Deuring correspondance
- Maximal orders $\mathcal{O}$ in $B_{p,\infty}$ = supersingular curves $E/\mathbb{F}_{p^2}$ (up to quadratic twists and Galois conjugates)
- $I \mapsto E_0[I], K \mapsto \mathfrak{I}(K)$: bijection between kernels and left O_0-ideals $\quad (O_0 = \mathrm{End}(E_0))$
- Ideals $\Leftrightarrow$ Isogenies
- $\mathrm{End}(E_I) = O_R(I)$ the right order of I; $\quad \deg \phi_I = N(I) := \mathrm{nrd}(I)$

Ideal to isogeny: $I \Leftrightarrow E_0 \to E_I := E_0/E[I]$

- Not a group action!
- SIDH relied on pushforwards, these depend on the paths, so need extra informations:

$$\begin{array}{ccc} E_0 & \longrightarrow & E_1 \\ \downarrow & & \downarrow \\ E_2 & \longrightarrow & E_{12} \end{array}$$

Table of Contents

The power object in an abelian category

- $A \in \mathcal{A}$ an abelian category, $R \subset \mathrm{End}_{\mathcal{A}}(A)$
- If $X \in \mathcal{A}$, $\mathrm{Hom}_{\mathcal{A}}(X, A)$ has a natural R-module structure
- If M f.p. R-module, the power object $\mathcal{HOM}_R(M, A)$ exists in $\mathcal{A}$:

$$\mathrm{Hom}_{\mathcal{A}}(X, \mathcal{HOM}_R(M, A)) = \mathrm{Hom}_R(M, \mathrm{Hom}_{\mathcal{A}}(X, A)) \quad \forall X \in \mathcal{A}$$

- If R is commutative, we have an abelian category $\mathcal{A}_R$ of R-oriented objects, and $\mathcal{HOM}_R(M, A)$ is naturally R-oriented, and is the power object both in $\mathcal{A}$ and $\mathcal{A}_R$.
- Symmetric monoidal contravariant action:

$$M \cdot A := \mathcal{HOM}_R(M, A)$$

- $M_1 \cdot M_2 \cdot A = (M_1 \otimes_R M_2) \cdot A$
- Functorial action: morphisms and objects act on morphisms and objects

- The copower object $M \otimes_R A$ also exists in $\mathcal{A}$:

$$\mathrm{Hom}_{\mathcal{A}}(M \otimes_R A, X) = \mathrm{Hom}_R(M, \mathrm{Hom}_{\mathcal{A}}(A, X)) \quad \forall X \in \mathcal{A}$$

- If R commutative, this is also the copower object in $\mathcal{A}_R$ and we have a covariant action $M \mapsto M \otimes_R A$

- All monoidal actions are of this type (using an enrichement in a presheaf category)

Explicit constructions of the power object

- $\mathcal{HOM}_R(R^n, A) = A^n$

$$R^m \to^F R^n \to M \to 0$$
$$0 \to \mathcal{HOM}_R(M, A) \to A^n \to^{F^T} A^m$$

- If M projective module, $R^n = M \oplus M' \Rightarrow$

$$A^n = \mathcal{HOM}_R(M, A) \oplus \mathcal{HOM}_R(M', A)$$

- Splitting of idempotents

Theorem (The action by projective modules)

If $\mathrm{End}_R(A) = R$*, then* $\mathrm{Hom}_R(M_2, M_1) = \mathrm{Hom}_{\mathcal{A}_R}(M_1 \cdot A, M_2 \cdot A)$ *for* M_1, M_2 *f.p. projective* R*-modules.*
The action $M \mapsto M \cdot A$ *gives an antiequivalence of category between f.p. projective* R*-modules and the Cauchy completion (for categories enriched in* R*-modules) of* A *in* $\mathcal{A}_R$*.*

Exactness properties

- Left exact on the left and right exact on the right:

$$0 \to M_2 \hookrightarrow M_1 \twoheadrightarrow M_1/M_2 \to 0,$$
$$0 \to (M_1/M_2) \cdot A \to M_1 \cdot A \to M_2 \cdot A$$

$$0 \to A_1 \hookrightarrow A_2 \twoheadrightarrow A_3 \to 0,$$
$$0 \to M \cdot A_1 \to M \cdot A_2 \to M \cdot A_3$$

- The right exact functor $\mathcal{HOM}_R(\cdot, A)$ gives rise to derived functors $\mathcal{E}xt_R^i(\cdot, A)$
- Taking a free resolution of M, applying $\mathcal{HOM}_R(\cdot, A)$ and taking the cohomology gives the $\mathcal{E}xt_R^i$

$$0 \to M_2 \hookrightarrow M_1 \twoheadrightarrow M_1/M_2 \to 0,$$
$$0 \to (M_1/M_2) \cdot A \to M_1 \cdot A \to M_2 \cdot A \to \mathcal{E}xt_R^1(M_1/M_2, A) \to \mathcal{E}xt_R^1(M_1, A) \to \cdots$$

The power object on abelian varieties

- $\mathcal{A}$ abelian category of proper group schemes over the base field k
- If A/k is an abelian variety with $R \subset \mathrm{End}(A)$, $M \cdot A$ is a proper group scheme in general
- If R domain,
$$\dim M \cdot A = \mathrm{rank}_R M \times \dim A$$
- If M projective, $M \cdot A$ is an abelian variety
- More generally, we say that M is compatible with A if M is torsion free and $M \cdot A$ is an abelian variety
If R is a domain and $0 \to M \to R^n \to P \to 0$, $M \cdot A$ is an abelian variety iff $\mathrm{Ext}^1_R(P, A) = 0$.

Example

- Torsion: $R/I \cdot A = A[I]$
- Rational points: $(M \cdot A)(k') \simeq \mathrm{Hom}_R(M, A(k'))$, k' a k-algebra

We can define the $\mathcal{E}xt^i_R$ more formally by embedding group schemes over k in the category of fppf sheafs over k.

From now on, we implicitly assume that M is compatible with A

Isogenies

Definition (Module isogeny)

A module isogeny is a monomorphism $M_2 \hookrightarrow M_1$ of torsion free modules with finite cokernel M_1/M_2
$\Leftrightarrow$ monomorphism $M_2 \hookrightarrow M_1$ of torsion free modules of the same rank
$\Leftrightarrow$ finite cokernel map $M_2 \to M_1$ of torsion free modules of the same rank

Proposition (Module isogeny to abelian variety isogeny)

If R domain and each M_i is compatible with A, then $M_1 \cdot A \twoheadrightarrow M_2 \cdot A$ is an isogeny with kernel $(M_1/M_2) \cdot A$:

$$0 \to (M_1/M_2) \cdot A \to M_1 \cdot A \to M_2 \cdot A \to 0$$

i.e., $\mathcal{E}xt^1_R(M_1/M_2, A) = 0$

Isogeny = epimorphism (with finite kernel) $\Leftrightarrow$ monomorphism (=inclusion) of modules (with finite cokernel)

Duality

- $(A, \lambda_A)/k$ ppav, $\bar{\cdot}$ the Rosatti involution on $\mathrm{End}_k(A)$
- $(R, \bar{\cdot}) \subset \mathrm{End}(A)$ domain
- Then R is a "CM order"
- Either R is totally real and $\overline{x} = x$
- Or R is a quadratic imaginary extension of a totally real order, and $\overline{x}$ is the complex conjugation

- $(M \cdot A)^\vee \simeq M^* \cdot A^\vee$, where $M^* = \mathrm{Hom}_R(M, R)$ and $A^\vee$ the dual abelian variety
- $(M \cdot A)^\vee \simeq M^\vee \cdot A$, where $M^\vee = \mathrm{Hom}_{\overline{R}}(M, R)$

- $\psi : M_2 \to M_1$, $\psi \cdot A : M_1 \cdot A \to M_2 \cdot A$
- $\psi^\vee : M_1^\vee \to M_2^\vee$, $\gamma \mapsto (v \mapsto \gamma \circ \psi(v))$
- $\psi^\vee \cdot A : M_2^\vee \cdot A^\vee \to M_1^\vee \cdot A^\vee$.
- This is the dual of ψ.

Hermitian modules and polarisations

- A polarisation Φ on $B = M \cdot A$ corresponds to:
  1. A morphism $B \to B^\vee$
  2. Which is autodual $\Phi = \Phi^\vee : B \simeq B^{\vee\vee} \to B^\vee$
  3. And induced by an ample line bundle

- A polarisation Ψ on M corresponds to:
  1. A morphism $M^\vee \to M$
  2. Which is autodual under the double duality: $M \simeq M^{\vee\vee}, m \mapsto (\phi \mapsto \overline{\phi(m)})$
  3. And is "positive"
- This is an integral positive definite Hermitian form H on $M^\vee$

  We will assume R Gorenstein for simplicity to have good biduality theorems. This is the case if the real suborder of R is maximal, e.g. R quadratic imaginary.

- Hermitian module action: the action by a polarised module (M, H_M) on a polarised abelian variety (A, λ_A) gives a polarised abelian variety $(M \cdot A, H_M \cdot \lambda_A)$
- If λ_A is principal and H_M unimodular, $H_M \cdot \lambda_A$ is principal.

Example

- The Shimura class group is the class group of unimodular rank 1 Hermitian R-modules
- Given a CM ppav (A, λ_A), acting by the Shimura class group gives other CM ppavs

Hermitian forms

Definition (Hermitian forms)

- R-sesquilinear: $H : M \times M \to R, H(\alpha x, y) = \alpha H(x,y), H(x, \overline{\alpha} y) = H(x,y)\overline{\alpha}$
- Hermitian: $H(y,x) = \overline{H(x,y)}$
- Positive definite: $H(x,x) \in \mathbb{Z}^{>0}, \quad \forall x \neq 0 \in M$
- Unimodular: $H : M \simeq M^\vee, m \mapsto H(m, \cdot)$
  $\Leftrightarrow M^\sharp := \{v \in M \otimes \mathbb{Q}, H(m,v) \in R \quad \forall m \in R\} = M$

Corollary (Principal polarisations, (A, λ_A) ppav)

- *Unimodular Hermitian R-form* H *on* $M \Rightarrow$ *Principal polarisation* $\lambda : M \cdot A \to (M \cdot A)^\vee$
- *N-similitude* $\Phi : (M_2, H_2) \to (M_1, H_1)$

$$\Phi^* H_1 = N H_2$$

$\Rightarrow$ *N-isogeny* $\phi : (A_1, \lambda_{A_1}) \to (A_2, \lambda_{A_2}) \quad$ *($A_i = M_i \cdot A$)*

Proposition (Contragredient = Adjoint)

If $\phi = \psi \cdot A : (A_1, \lambda_1) \to (A_2, \lambda_2)$ for $\psi : (M_2, H_2) \to (M_1, H_1)$, then $\widetilde{\phi} = \widetilde{\psi} \cdot A$, where $\widetilde{\psi} : M_1 \to M_2$ is the adjoint: $H_1(\psi(x), y) = H_2(x, \psi^*(y))$

Table of Contents

A general equivalence of category

Oriented case: E_0/k primitively oriented by R quadratic imaginary

Theorem (Module antiequivalence of category)

The action $M \mapsto M \cdot E_0$ gives an antiequivalence of category between the category of R-oriented abelian varieties [a] A k-isogenous to E_0^g and R-oriented k-morphisms; and the category of f.p. torsion free R-modules M of rank g and R-module morphisms.

Inverse map: $A \mapsto \mathrm{Hom}_R(A, E_0)$: module of (oriented) morphisms from A to E_0

[a] with the technical condition $\rho_R(A) \simeq \oplus_{i=1}^{g} \rho_R(E_0)$

[Waterhouse 1969], [Kani 2011], [Jordan, Keeton, Poonen, Rains, Shepherd-Barron, Tate 2018], [Kirschmer, Narbonne, Ritzenthaler, R. 2021], [Page-R. 2023]

Alternative approaches to equivalences of category of abelian varieties (e.g. via lifting to characteristic zero): [Deligne, Howe, Centeleghe-Stix, Marseglia]…

Example

- Frobenius orientation: all rational isogenies at level "above" E_0 in the volcano
- Supersingular case: the action by f.p. left $\mathfrak{O}_0$-modules also gives an antiequivalence of categories to maximal supersingular abelian varieties, $\mathfrak{O}_0 = \mathrm{End}(E_0)$.

Warmup: ideals

- $I \hookrightarrow R$ induces $\phi_I : E_0 = R \cdot E_0 \to E_I = I \cdot E_0$
- Canonical unimodular Hermitian form on I:

$$H_I(x,y) = \frac{x\overline{y}}{N(I)}$$

- The inclusion $(I, H_I) \subset (R, H_R)$ is a $N(I)$-similitude
- Handles ascending isogenies: I not invertible (the R-orientation needs not be primitive on E_I)

$\phi : E_{I_1} \to E_{I_2}, \quad I_1, I_2$ invertible

- Ideal point of view: $\phi \Leftrightarrow$ some integral ideal J equivalent to $I = I_2 I_1^{-1}$
- $I^{-1} = \overline{I}/N(I)$ so if $x \in I, J := I\overline{x}/N(I) \sim I; \quad N(J) = N(x)/N(I)$

- Module point of view: $\phi \Leftrightarrow \psi : (I_2, H_R/N(I_2)) \to (I_1, H_R/N(I_1))$
- If $z \in I^{-1}$: $\psi_z : r \mapsto zr$ is a $N := N(z)N(I_2)/N(I_1)$-similitude
- $z = \overline{x}/N(I), N = N(x)/N(I)$
- If I integral: canonical isogeny via $z = 1 \in R \subset I^{-1}$

- Module point of view + specific isogeny $E_0 \to E$ = ideal point of view

Forgetting the orientation on supersingular elliptic curves

- $E_0/\mathbb{F}_{p^2}$ supersingular, $R \subset \mathfrak{O}_0 := \mathrm{End}(E_0)$ primitive orientation
- Two type of actions: by left f.p. R-modules M_R and by left f.p. $\mathfrak{O}_0$-modules $M_{\mathfrak{O}}$
- If $A = M_R \cdot_R E_0$, $A = (\mathfrak{O}_0 \otimes_R M_R) \cdot_{\mathfrak{O}_0} E_0$
- Forgetting the orientation
- Conversely: $M_R = \mathrm{Hom}_R(A, E_0)$, $M_{\mathfrak{O}} = \mathrm{Hom}(A, E_0)$

Example (Rational isogenies from irrational endomorphisms)

In CSIDH, if we know $\mathfrak{O} = \mathrm{End}(E)$, we can recover $I = \mathrm{Hom}(E, E_0)$ by linear algebra, hence the module $\mathfrak{a} = \mathrm{Hom}_{\mathbb{F}_p}(E, E_0)$ as the morphisms in I commuting with π.
This simplifies an argument due to [Castryck, Panny, Vercauteren 2019].

Similitudes to isogenies

Module morphism to morphism of abelian varieties:

$$\begin{array}{ccccccc} R^{m_1} & \longrightarrow & R^{n_1} & \twoheadrightarrow & M_1 & \longrightarrow & 0 \\ \uparrow & & \uparrow & & \uparrow & & \\ R^{m_2} & \longrightarrow & R^{n_2} & \twoheadrightarrow & M_2 & \longrightarrow & 0 \end{array} \quad \Leftrightarrow \quad \begin{array}{ccccccc} 0 & \longrightarrow & M_1 \cdot A & \hookrightarrow & A^{n_1} & \longrightarrow & A^{m_1} \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & M_2 \cdot A & \hookrightarrow & A^{n_2} & \longrightarrow & A^{m_2} \end{array}$$

R^n is a projective module, so we can lift module maps. The commutative diagram allows to find the kernel of $M_1 \cdot A \to M_2 \cdot A$.

- N-similitudes $\Leftrightarrow$ N-isogenies
- $(M_2, H/N) \subset (M_1, H) \Rightarrow \phi : A_1 = M_1 \cdot A \twoheadrightarrow A_2 = M_2 \cdot A$
- $M_1 = \mathrm{Hom}(R, M_1)$, so $m_1 \in M_1$ induces $m_1 \cdot A : A_1 \to A$
  We say that M_1 is a module orientation on $A_1 = M_1 \cdot A$
- $\mathrm{Ker}\, \phi = A_1[M_2] \subset A_1[N]$

$$A_1[M_2] := \{P \in A_1(\bar{k}), (m \cdot A)(P) = 0, \forall m \in M_2\}$$

- Equivalence practical if N smooth, the N-torsion on A_1 is accessible, and the orientation of M_1 on A_1 is effective

Computing the module action

- We want to compute $A = (M, H) \cdot E_0$
- Find a smooth similitude $(M, H) \rightarrow (R^g, H_R^g)$
- The R^g-module orientation on E_0^g is effective (as long as the R-orientation on E_0 is)
- So we can convert the similitude to an isogeny $E_0^g \rightarrow A$

- Clapoti(s): it suffice to build two N_1, N_2-similitudes with $N_1 \wedge N_2 = 1$ (or small)

☡ There are unimodular Hermitian R-modules (M, H_M) such that no N-similitude $R^g \hookrightarrow M$ exist for any N, c.f. the arithmetic obstructions in [Kirschmer, Narbonne, Ritzenthaler, R. 2021]

- Solution: look at $R^{g+1} \hookrightarrow M \times R$

☡ Conductor gap: a N-isogeny $E_0^g \rightarrow E \times A$ (with the product polarisations) inducing a non trivial isogeny $E_0 \rightarrow E$ satisfy

$$f_{E/E_0} \mid N$$

Module kernels and kernel modules

- $A_1 = M_1 \cdot A$, M_1-oriented abelian variety
- $M_2 \subset M_1 \mapsto A[M_2] = \{P \in A_1(\bar{k}), (m \cdot A_1)(P) = 0, \forall m \in M_2\}$
- $K \subset A_2 \mapsto M(K) = \{m \in M_1, m(K) = 0\}$
- These are Galoisian adjunctions
- This restrict to a bijection between module kernels and kernel modules
- In our case ($A \sim E_0^g$), every module is a kernel module; and a kernel is a module kernel iff A_1/K is in the orbit of A by the module action.

Isogeny to similitude:

- $\phi : A_1 \to A_2$ a N-isogeny of kernel K induced by $\psi : M_2 \to M_1$
- $A_1 = M_1 \cdot A$ with effective orientation
- $M_2 := \{m \in M_1, m \cdot (K) = 0\}, H_2 = H_1/N$
  Needs efficient DLPs in $A_1[N]$ to compute M_2
- The orientation of M_2 on A_1 descends to an effective orientation on A_2
  (via isogeny division, at least in nice cases)

Direct sums and pushforwards

$(A_1, \lambda_1) = (M_1, H_1) \cdot A_0$ and $(A_2, \lambda_2) = (M_2, H_2) \cdot A_0$

Product polarisations: $(A_1 \times A_2, \lambda_1 \times \lambda_2) = (M_1 \oplus M_2, H_1 \oplus H_2) \cdot A_0$

Pushforwards:

- If $\phi_1 : A_0 \to A_1$ and $\phi_2 : A_0 \to A_2$ correspond to $\psi_1 : M_1 \to M$ and $\psi_2 : M \to M_2$, their pushforward A_{12} corresponds to the fiber product $M_1 \times_M M_2$
- If $\phi_1 : A_0 \twoheadrightarrow A_1, \phi_2 : A_0 \twoheadrightarrow A_2$ are isogenies, $\psi_1 : M_1 \hookrightarrow M, \psi_2 : M_2 \hookrightarrow M$ are monomorphisms, and the fiber product $M_1 \times_M M_2$ is just the intersection $M_1 \cap M_2 \subset M$

$$\begin{array}{ccc} A_0 & \twoheadrightarrow & A_1 \\ \downarrow\!\!\downarrow & & \downarrow\!\!\downarrow \\ A_2 & \twoheadrightarrow & A_{12} \end{array} \quad \Leftrightarrow \quad \begin{array}{ccc} M & \hookleftarrow & M_1 \\ \uparrow & & \uparrow \\ M_2 & \hookleftarrow & M_1 \cap M_2 \end{array}$$

Table of Contents

Finding curves with many points

- $C/\mathbb{F}_q$ is a defect o curve if $\#C(\mathbb{F}_q) = 1 + q + g\lfloor 2\sqrt{q} \rfloor$
- Then $\mathrm{Jac}(C) \sim E_0^g$, E_0 of trace $-\lfloor 2\sqrt{q} \rfloor$.
- $\mathrm{Jac}(C) = M \cdot E_0$ (if E_0 at the bottom of the volcano)

Algorithm [Kirschmer, Narbonne, Ritzenthaler, R. 2021]:

- List all unimodular Hermitian modules (M, H) over $R = \mathrm{End}_{\mathbb{F}_q}(E_0)$
  1. Enumerate all O_R-genus, and construct an O_R-lattice L for each genus
  2. Explore adjacent lattices to L until we have found all O_R-isometry classes in the genus
  3. Build the R-isometry classes of unimodular lattices from the O_R-unimodular lattices
- Compute all ppavs $(A, \lambda_A) = (M, H_M) \cdot E_0$
- Find which are Jacobians of defect 0 curves

Beware of twists! In the non hyperelliptic case, a maximal Jacobian may only correspond to a minimal curve

- We use algebraic modular forms to check in which case we are

The isogeny graph of oriented isogenies in higher dimension

Assume R quadratic imaginary, $A \sim E_0^g$, so $A = M \cdot E_0$

- M torsion free of rank g: $M \simeq R^{g-1} \oplus I$ Assume R maximal for simplicity
- $A \simeq E_0^{g-1} \times E_I$ as unpolarised varieties
- $\# \mathrm{Cl}(R)$ isomorphism classes of non-polarised R-oriented abelian varieties R-isogenous to E_0^g

- Polarisations add supersingular like graph complexity if $g > 1$ $(\mathrm{End}_R(E_0^g) = M_g(R))$
- Universal group action: $I \cdot (M, H_M) = (IM, H_M/N(I)) \subset (M, H_M)$ (I invertible)
- $I \cdot A = A_I := A/A[I]$
- Intuition: multiplication by $[n] \Rightarrow$ multiplication by $[I]$
- Multiple orbits; linked together by oriented isogenies (which are not multiplication by $[I]$)

Example: rational supersingular abelian surfaces

- $E_0/\mathbb{F}_p$ supersingular, $R = \mathrm{End}_{\mathbb{F}_p}(E) = \mathbb{Z}[\sqrt{-p}]$ (or its maximal order)
- $g = 2$: graph of supersingular abelian surfaces isogeneous to E_0^2 over $\mathbb{F}_p$ and $\mathbb{F}_p$-rational isogenies
- Universal group action from $\mathrm{Cl}(R)$
- Conjecture: $\approx p^{3/2}$ nodes (≈ #supersingular curves × # $\mathrm{Cl}(R)$)
- If $\ell = \mathfrak{l}\bar{\mathfrak{l}}$ splits in R, $A[\ell] = A[\mathfrak{l}] \oplus A[\bar{\mathfrak{l}}] \Rightarrow$ action by $\mathfrak{l}$ and $\bar{\mathfrak{l}}$
  and $\ell + 1$ (?) other oriented ℓ-isogenies.

Weil's restriction of supersingular elliptic curves

$E_0/\mathbb{F}_p$ supersingular, $R = \mathrm{End}_{\mathbb{F}_p}(E) = \mathbb{Z}[\sqrt{-p}]$

- If $E/\mathbb{F}_{p^2}$, its Weil restriction $W_{\mathbb{F}_{p^2}/\mathbb{F}_p} E$ is a p.p. abelian surface over $\mathbb{F}_p$ (which is neither a Jacobian nor a product of curves over $\mathbb{F}_p$).
- The Weil restriction of an N-isogeny $\phi/\mathbb{F}_{p^2} : E_1 \to E_2$, is an $\mathbb{F}_p$-rational isogeny between rational the abelian surfaces $A_1 \to A_2$, $A_i = W_{\mathbb{F}_{p^2}/\mathbb{F}_p} E_i$

⇒ If E is maximal, $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$ is isogeneous to E_0^2

- $\mathrm{Hom}_{\mathbb{F}_p}(W_{\mathbb{F}_{p^2}/\mathbb{F}_p} E_1, W_{\mathbb{F}_{p^2}/\mathbb{F}_p} E_2) = \mathrm{Hom}_{\mathbb{F}_{p^2}}(W_{\mathbb{F}_{p^2}/\mathbb{F}_p} E_1 \otimes_{\mathbb{F}_p} \mathbb{F}_{p^2}, E_2) = \mathrm{Hom}_{\mathbb{F}_{p^2}}(E_1 \oplus E_1^\sigma, E_2) = \mathrm{Hom}_{\mathbb{F}_{p^2}}(E_1, E_2) \oplus \mathrm{Hom}_{\mathbb{F}_{p^2}}(E_1, E_2)^\sigma$

- The dimension 2 supersingular graph over $\mathbb{F}_p$ contains, via the Weil restriction, the supersingular graph of elliptic curves over $\mathbb{F}_{p^2}$ (with E collapsed with E^σ)

⇒ Convenient way to obtain $\mathbb{F}_p$-rational isogenies in dimension 2

⇒ Module-Inversion in dimension 2 at least as hard as the supersingular isogeny path problem.

- Weil restriction from the module point of view: If $\phi/\mathbb{F}_{p^2} : E_1 \to E_2$ is represented by $\psi/O_0 : I_2 \to I_1$, we can find directly the module representation $\Psi/R : M_2 \to M_1$ of $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}\phi$

Table of Contents

Symmetric monoidal actions

Definition (The module monoidal contravariant action)

- If M is a projective module, the action by M is $M \cdot A = \mathcal{HOM}_R(M, A)$.
- If $\phi : A_1 \to A_2$ is a N-isogeny, $M \cdot \phi : M \otimes_R A_1 \to M \otimes_R A_2$ is a N-isogeny.
- If $\psi : M_2 \hookrightarrow M_1$ is a N-similitude, $\psi \cdot A : M_1 \cdot A \to M_2 \cdot A$ is a N-isogeny.

Example (The action by ideals)

$I \otimes_R M \simeq IM$ when I is inversible (or simply $f_I \wedge f_M = 1$), so $I \cdot A$ recovers the usual CSIDH action

Definition (Tensor product)

If $A_1 = M_1 \cdot A_0, A_2 = M_2 \cdot A_0, A_1 \otimes_{A_0} A_2 := (M_1 \otimes_R M_2) \cdot A_0$

The module action for isogeny based cryptography

Proposition (Higher dimensional CSIDH via the monoidal action)

$$\begin{array}{ccc} A_0 & \rightsquigarrow & A_1 = M_1 \cdot A_0 \\ \wr\downarrow & & \wr\downarrow \\ A_2 = M_2 \cdot A_0 & \rightsquigarrow & A_{12} = (M_1 \otimes_R M_2) \cdot A_0 \end{array}$$

If $\dim A_0 = g_0$, $\operatorname{rank} M_1 = g_1$, $\operatorname{rank} M_2 = g_2$, *then* $\dim A_{12} = g_0 g_1 g_2$.

Example (Monoidal action by rank 2 modules: $A_0 = E_0, g_1 = g_2 = 2$)

M_i projective module of rank $2 \Leftrightarrow E_0^2 \twoheadrightarrow A_i$ a path:

$$\begin{array}{ccc} E_0^2 & \longrightarrow & A_1 \\ \downarrow & & \wr\downarrow \\ A_2 & \rightsquigarrow & A_1 \otimes_{E_0} A_2 \end{array}$$

Common secret: the dimension 4 abelian variety $A_1 \otimes_{E_0} A_2$

The module action for isogeny based cryptography

Proposition (Higher dimensional CSIDH via the monoidal action)

$$\begin{array}{ccc} A_0 & \rightsquigarrow & A_1 = M_1 \cdot A_0 \\ \wr\downarrow & & \wr\downarrow \\ A_2 = M_2 \cdot A_0 & \rightsquigarrow & A_{12} = (M_1 \otimes_R M_2) \cdot A_0 \end{array}$$

If $\dim A_0 = g_0$, $\operatorname{rank} M_1 = g_1$, $\operatorname{rank} M_2 = g_2$, *then* $\dim A_{12} = g_0 g_1 g_2$.

- ☹ Acting by rank g projective modules increase the dimension if $g > 1$
- ☺ Protects (hopefully!) from Kuperberg

- Security: Action-DDH ≤ Action-CDH ≤ Action-Inversion
- Action-Inversion ≈ HomModule-Inversion
  Indeed, if $M = \operatorname{Hom}_R(A, E_0)$, then $A = M \cdot E_0$
  Recall that, thanks to Weil's restriction, Module-Inversion on supersingular abelian surfaces over $\mathbb{F}_p$ is at least as hard as solving the supersingular isogeny path problem over $\mathbb{F}_{p^2}$
- Action-CDH: Hope for exponential quantum security when $g > 1$

Computing the symmetric monoidal action

M_1 projective of rank g, $A_1 = M_1 \cdot E_0$
We want to compute $M_1 \cdot A_2$ for an R-oriented A_2 (with effective R-orientation)
General idea: look at how we construct $A_1 = M_1 \cdot E_0$ from E_0, and apply the same recipe replacing E_0 by A_2.

The smooth case:

- Suppose we can construct a smooth similitude $R^g \subset M_1$ (by duality, this is equivalent to constructing a smooth isogeny $E_0^g \to A_1$), this gives us a smooth similitude $A_2^g \to M_1 \cdot A_2$
- Via the orientation, we can transpose the kernel of $E_0^g \to A_1$ to the kernel of $A_2^g \to M_1 \cdot A_2$. The codomain gives us $M_1 \cdot A_2$
- Similar to the usual way the CSIDH action is computed

The general case:

- If instead A_1 is computed via Clapoti(s), splitting an appropriate endomorphism on $E_0^{g_1}$
- Then we can compute $M_1 \cdot A_2$ by splitting an appropriate endomorphism on $A_2^{g_1}$

☹ Needs to work in dimension $2g_1g_2$

Computing the symmetric monoidal action: the smooth case

$$R^g \longleftarrow M_1 \qquad \Leftrightarrow \qquad E_0^g \longrightarrow\!\!\!\!\to A_1$$

$$M_2^g \longleftarrow M_1 \otimes_R M_2 \qquad\qquad A_2^g \longrightarrow\!\!\!\!\to A_1 \otimes_{E_0} A_2 = M_1 \cdot A_2$$

Proposition (Computing projective module actions: the smooth case)

If $E_0^g \twoheadrightarrow A_1 \Leftrightarrow M_1 \hookrightarrow R^g$, we can compute $A_1 \otimes_{E_0} A_2$ as the quotient of $A_2^g = E_0^g \otimes_{E_0} A_2$ given by the kernel $K \subset A_2^g$ induced by $M_1 \otimes M_2 \hookrightarrow R^g \otimes M_2$: if M_1 is generated by $(m_1, \dots, m_n)$, and $m_i = (\alpha_{i1}, \dots, \alpha_{ig}) \in R^g$, then $K = A_2^g[m_1 \otimes M_2, \dots, m_n \otimes M_2]$ and

$$A_2^g[m_i \otimes M_2] = \operatorname{Ker} A_2^g \xrightarrow{(\alpha_{ij})} A_2$$

Corollary (Computing the action in practice)

- *If A_1 is the quotient of E_0^g by $E_0^g[m_1, \dots, m_n]$, where* $E_0^g[m_i] = \operatorname{Ker}(E_0^g \to E_0, (P_1, \dots, P_g) \mapsto \sum \alpha_{ij} P_j)$
- *Then $A_1 \otimes_{E_0} A_2$ is the quotient of A_2^g by $A_2^g[m_1 \otimes M_2, \dots, m_n \otimes M_2]$, where* $A_2^g[m_i \otimes M_2] = \operatorname{Ker}(A_2^g \to A_2, (P_1, \dots, P_g) \mapsto \sum \alpha_{ij} P_j)$
- *And if $E_0^g \to A_1$ is a N-isogeny, $A_2^g \to A_1 \otimes_{E_0} A_2$ is a N-isogeny*

Computing the symmetric monoidal action: the smooth case

Commutative diagram:

$$\begin{array}{ccc} R^{g_1} \otimes_R R^{g_2} & \longleftarrow & M_1 \otimes_R R^{g_2} \\ \uparrow & & \uparrow \\ R^{g_1} \otimes_R M_2 & \longleftarrow & M_1 \otimes_R M_2 \end{array} \quad \Leftrightarrow \quad \begin{array}{ccc} E_0^{g_1} \otimes_{E_0} E_0^{g_2} \simeq E_0^{g_1 g_2} & \longrightarrow & A_1 \otimes_{E_0} E_0^{g_2} \simeq A_1^{g_2} \\ \downarrow & & \downarrow \\ E_0^{g_1} \otimes_{E_0} A_2 \simeq A_2^{g_1} & \longrightarrow & A_1 \otimes_{E_0} A_2 \end{array}$$

Pairing analogy: $\otimes_{E_0}$ = categorified bilinear map

Assume we don't know how to compute $e(P_1, P_2)$ for general P_1, P_2, but we know $e(P_0, P_2)$. Then if $P_1 = mP_0$, we can compute $e(P_1, P_2) = e(P_0, P_2)^m$

Here we use that $E_0^g \otimes_{E_0} A_2 \simeq A_2^g$ and our known path $E_0^g \twoheadrightarrow A_1$.

Monoidal actions for isogenies

- $M_1' \hookrightarrow M_1 \hookrightarrow R^g \Leftrightarrow A_2^g \twoheadrightarrow M_1 \cdot A_2 \twoheadrightarrow M_1' \cdot A_2 \Rightarrow$ recover it via the isogeny factorisation: $A_2^g[M_1 \otimes_R M_2] \subset A_g^2[M_1' \otimes_R M_2]$
- If $A_2 \to A_2'$, then we recover $M_1 \otimes_R A_2 \to M_1 \otimes_R A_2'$ via isogeny division:

$$\begin{array}{ccc} A_2^g & \longrightarrow & M_1 \cdot A_2 \\ \downarrow & & \downarrow \\ {A_2'}^g & \longrightarrow & M_1 \cdot A_2' \end{array}$$

Computing the symmetric monoidal action: the general case

$$E_0^g \longrightarrow A_1 \longrightarrow E_0^g$$

$$A_2^g \longrightarrow A_1 \otimes_{E_0} A_2 \longrightarrow A_2^g$$

Proposition (Computing projective module actions: the general case)

Assume A_1 is constructed from E_1 via Clapoti(s), i.e. constructing a N_1 and N_2-similitude $R^g \hookrightarrow M_1$, and then splitting the induced N_1N_2-endomorphism $\gamma : E_0^g \to E_0^g$. So γ is given by an explicit matrix in $M_g(R)$.
Then $\gamma \otimes_{E_0} \mathrm{Id}_{A_2}$ is the same matrix acting as an endomorphism $A_2^g \to A_2^g$ via the R-orientation, and splitting this N_1N_2-endomorphism gives $A_1 \otimes_{E_0} A_2$.

⊗-MIKE

$$\begin{array}{ccc} E_0 & \longrightarrow & E_1 \\ \downarrow & & \rightsquigarrow \\ E_2 & \rightsquigarrow & W_{\mathbb{F}_p^2/\mathbb{F}_p} E_1 \otimes_{E_0} W_{\mathbb{F}_p^2/\mathbb{F}_p} E_2 \end{array}$$

- Start with our good old friend $E_0/\mathbb{F}_p$ supersingular (with p e.g. the SQISign2d prime)
- Alice and Bob compute (smooth or not) isogenies over $\mathbb{F}_{p^2}$: $E_0 \to E_1, E_0 \to E_2$
- They send $j(E_1), j(E_2)$: no torsion information!
- Validation: check that E_i is supersingular
- The common key is the dimension 4 ppav $A_{12} := W_{\mathbb{F}_p^2/\mathbb{F}_p} E_1 \otimes_{E_0} W_{\mathbb{F}_p^2/\mathbb{F}_p} E_2$

  Alice can compute it by converting her isogeny $E_0 \to E_1$ to the module map representing $E_0^2 = W_{\mathbb{F}_p^2/\mathbb{F}_p} E_0 \to W_{\mathbb{F}_p^2/\mathbb{F}_p} E_1$ and then applying the module action to $W_{\mathbb{F}_p^2/\mathbb{F}_p} E_2$.

  The smooth case requires a dimension 4 isogeny, and the non smooth case requires splitting a dimension 4 endomorphism, so a dimension 8 isogeny…

- Size: $p = 2\lambda, j(E_i) = 2\log_2(p) = 4\lambda$: 64B. Very compact!
- NIKE. PKE a la ElGamal/SiGamal

- Need good dimension 4 modular invariants to represent A_{12} (e.g. suitable symmetric polynomials in the theta constants?)
- Security? Action-CDH on supersingular abelian surfaces coming from the Weil restriction of elliptic curves

⊗-MIKE

$$\begin{array}{ccc} E_0 & \longrightarrow & E_1 \\ \downarrow & & \wr \\ E_2 & \rightsquigarrow & W_{\mathbb{F}_p^2/\mathbb{F}_p} E_1 \otimes_{E_0} W_{\mathbb{F}_p^2/\mathbb{F}_p} E_2 \end{array}$$

Example of parameters:

- $p = u2^e - 1$. Ex: $p = 5 \cdot 2^{248} - 1$.
- Alice and Bob each compute a 2^e-isogeny from E_0 over $\mathbb{F}_{p^2}$
- Then the common key requires computing a 2^e-isogeny in dimension 4 over $\mathbb{F}_p$

- Unfortunately, for the dimension 4 isogeny, the theta null point will only be defined over $\mathbb{F}_{p^2}$, so our known isogeny formulas will require to work over $\mathbb{F}_{p^2}$ for the dimension 4 isogeny too
- Solution: use Scholten's construction $W'_{\mathbb{F}_2/\mathbb{F}_p}$ instead of the Weil restriction
- Start with E_0 at the bottom of the 2-volcano, $\mathrm{End}(E_0) = R = \mathbb{Z}[\sqrt{-p}]$
- The climbing 2-isogeny is given by $E_0 \to \mathfrak{f} E_0$, $\mathfrak{f}$ the conductor ideal in $O_R = \mathbb{Z}[(1+\sqrt{-p})/2]$
- $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p} E = \mathfrak{f} W_{\mathbb{F}_{p^2}/\mathbb{F}_p} E \Rightarrow$ explicit construction in term of modules
- Special case: If $E_0 : y^2 = x^3 + x$, $E_0' : y^2 = x^3 - x$ is its quartic twist, and $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p} E_0' = {E_0'}^2$

⊗-MIKE

$$\begin{array}{ccc} E_0 & \longrightarrow & E_1 \\ \downarrow & & \wr\!\downarrow \\ E_2 & \rightsquigarrow & W_{\mathbb{F}_p^2/\mathbb{F}_p} E_1 \otimes_{E_0} W_{\mathbb{F}_p^2/\mathbb{F}_p} E_2 \end{array}$$

Example of parameters:

- $p = u2^e - 1$. Ex: $p = 5 \cdot 2^{248} - 1$.
- Alice and Bob each compute a 2^e-isogeny from E_0 over $\mathbb{F}_{p^2}$
- Then the common key requires computing a 2^e-isogeny in dimension 4 over $\mathbb{F}_p$

- I am beginning to have serious doubts about the security of action-CDH when both isogenies have the same degree 2^e
- Solution: take coprime degrees
- ☹ Unfortunately this slows down the scheme
- Either we use 2^e and 3^f-isogenies like in SIDH, but this requires to double the size of p to obtain the required torsion, so this double the key size. And a 3-isogeny in dimension 4 is going to be $\approx 5\times$ slower than a 2-isogeny
- Or we build our isogenies via Clapotis, splitting an appropriate dimension 1 supersingular endomorphism. The good new is that our curves E_i will be statically uniform. The bad new is that computing the key exchange will require splitting a dimension 4 endomorphism, hence involves a dimension 8 isogeny, for a $\approx 32\times$ slow down.