Isogenies in higher dimension

Caipi Symposium

Sabrina Kunzweiler

April 29th, 2024

Inria, IMB, Bordeaux, France

Elliptic Curves

polarization:
$\phi_{\mathcal{L}} : A \to \hat{A}$
special isogeny

$V \subset \mathbb{P}^n$
zero-locus of a family
of homogeneous polynomials

$\downarrow$ $\downarrow$

Principally	polarized	abelian	variety	of dimension 1

$\uparrow$ $\uparrow$ $\uparrow$

$\phi_{\mathcal{L}} : A \xrightarrow{\sim} \hat{A}$

algebraic group

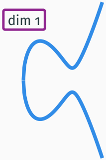
dimension:
maximal d with
$V_0 \subset \cdots \subset V_d \subseteq V$

- All 1-dimensional principally polarized abelian varieties (p.p.a.v.) are elliptic curves.

This talk: Dimension $d > 1$.

The higher dimensional picture

dimension 1
(abelian curves)

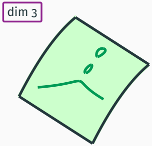


elliptic curve

Moduli space of d-dimensional abelian varieties: dimension $\frac{d(d+1)}{2}$.

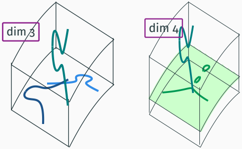
dimension 2
(abelian surfaces)

product of elliptic curves

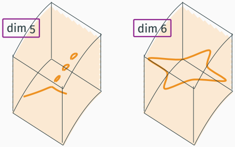


Jacobian of a genus-2 curve

dimension 3
(abelian threefolds)



products



Jacobians of genus-3 curves

Abelian Surfaces

Genus-2 curves

Elliptic Curve E

$$E : y^2 = f(x), \text{ with } \deg(f) = 3.$$

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

$$E(\bar{k}) = \{(u, v) \in \bar{k}^2 \mid v^2 = f(u)\} \cup \{\infty\}.$$

Genus-2 curve C

$$\mathcal{C} : y^2 = f(x), \text{ with } \deg(f) \in \{5, 6\}.$$

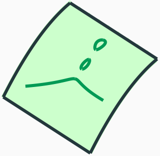
$$y^2 = x(x^2 - 1)(x^2 - 4)$$

$$C(\bar{k}) = \{(u, v) \in \bar{k}^2 \mid v^2 = f(u)\} \cup \begin{cases} \{\infty\} & \text{if } \deg(f) = 5 \\ \{\infty_+, \infty_-\} & \text{if } \deg(f) = 6 \end{cases}$$

⚠ Points on C do not form a group.

Jacobians of genus-2 curves

Formally: $Jac(C)$ is the abelian variety so that for any field $k \subset K \subset \bar{k}$,



$$Jac(C)(K) = \mathrm{Pic}^0_C(K),$$

where Pic_C is the Picard group of C.

Essentially: Elements in $Jac(\mathcal{C})(k)$ correspond to pairs of points $\{P, Q\} \in \mathcal{C}(\bar{k})^2$ invariant under $Gal(\bar{k}/k)$.

Representing $[P + Q - D_\infty] \in Jac(\mathcal{C})$, where $D_\infty = \begin{cases} 2 \cdot \infty \\ \infty_+ + \infty_- \end{cases}$

Mumford presentation of an element $\{P, Q\} \in Jac(C)$ with $P = (x_1, y_1), Q = (x_2, y_2)$ (affine):
$(a, b) = (x^2 + a_1 x + a_0, b_1 x + b_0) \in k[x]$ so that $a(x_i) = 0, b(x_i) = y_i$.

Group law: blackboard

Torsion elements over a finite field ($\mathrm{char}(k) = p$)

Elliptic Curve $E : y^2 = f(x)$

- $E[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$ for $m \in \mathbb{N}$ with $p \nmid m$.
- The **Weil pairing**

$$e_m : E[m] \times E[m] \to \mu_m$$

is a bilinear, alternating pairing.

Example: $E[2] \setminus \{0\}$

- Weierstrass points $P_i = (\alpha_i, 0)$

$$e_2\left(P_i, P_j\right) = \begin{cases} -1 & \text{if } i \neq j, \\ 1 & \text{otherwise.} \end{cases}$$

Genus-2 curve $C : y^2 = f(x)$

- $Jac(C)[m] \cong (\mathbb{Z}/m\mathbb{Z})^4$ for $m \in \mathbb{N}$ with $p \nmid m$.
- The **Weil pairing**

$$e_m : Jac(C)[m] \times Jac(C)[m] \to \mu_m$$

is a bilinear, alternating pairing.

Example: $Jac(C)[2] \setminus \{0\}$

- pairs of Weierstrass points $R_{ij} = ((\alpha_i, 0), (\alpha_j, 0))$

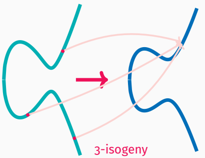
$$e_2\left(R_{ij}, R_{kl}\right) = \begin{cases} -1 & \text{if } \mid \{i,j\} \cap \{k,l\} \mid = 1, \\ 1 & \text{otherwise.} \end{cases}$$

Isogenies of Abelian Surfaces

Comparison to the 1-dimensional setting

dimension 1

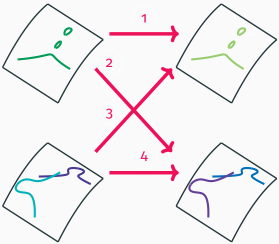
N-isogeny $\phi : E \to E'$ surjective morphism with $\ker(\phi) \simeq \mathbb{Z}/N\mathbb{Z}$.



all isogenies are generic

dimension 2

(N, N)-isogeny surjective morphism $\phi : A \to A'$ has *isotropic*[1] $\ker(\phi) \simeq (\mathbb{Z}/N\mathbb{Z})^2$



4 isogeny types:

1. generic
2. splitting
3. gluing
4. product

[1] Weil pairing is trivial.

Isotropic subgroups

Elliptic curves Any basis $\mathcal{B} = (P_1, P_2)$ of $E[N]$ is symplectic, i.e. $\log_{\mu_N}(e_N(P_i, P_j)) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ for some μ_N.

- $G = \langle P_1 + aP_2 \rangle$ is an N-subgroup for any $a \in \mathbb{Z}/N\mathbb{Z}$
  $\Rightarrow N$ groups out of $O(N)$ in total.

Abelian surface A basis $\mathcal{B} = (D_1, D_2, D_3, D_4)$ for $A[N] \simeq (\mathbb{Z}/N\mathbb{Z})^4$ is symplectic if

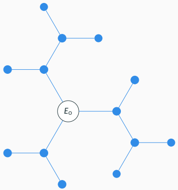
$$\log_{\mu_N}\left(e_N(D_i, D_j)\right) = \begin{pmatrix} 0 & I_2 \\ -I_2 & 0 \end{pmatrix}.$$

- $G = \langle D_1 + aD_3 + bD_4, D_2 + bD_3 + cD_4 \rangle$ is an isotropic (N, N)-group for any $a, b, c \in \mathbb{Z}/N\mathbb{Z}$.
  $\Rightarrow N^3$ groups out of $O(N^3)$ in total.

Isogeny graphs: ℓ prime

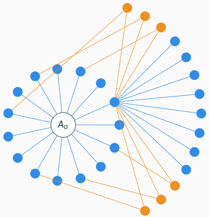
Elliptic curves

- $N = \ell$ prime: $\ell + 1$ isotropic ℓ-groups.
- Non-backtracking composition of two ℓ-isogenies: ℓ^2-isogeny



Abelian surfaces

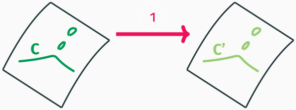
- $N = \ell$ prime: $\ell^3 + \ell^2 + \ell + 1$ isotropic (ℓ, ℓ)-groups in total.
- Non-backtracking composition of two (ℓ, ℓ)-isogenies: (ℓ^2, ℓ^2)-isogeny , (ℓ^2, ℓ, ℓ)-isogeny



isogeny graph $\ell = 2$

Computing $(2,2)$-isogenies

Richelot isogenies



Generic case $\phi : Jac(C) \to Jac(C')$

Write $C : y^2 = g_1(x)g_2(x)g_3(x)$ with g_i quadratic. Then

$$G = \langle (g_1(x), 0), (g_2(x), 0) \rangle \subset Jac(C)[2]$$

is an isotropic $(2, 2)$-group.

Let $\delta = \det\left((g_{ij})_{ij}\right)$ with $(g_{ij})_j$ coefficients of g_i.

If $\delta \neq 0$, then $Jac(C)/G = Jac(C')$, where

$$C' : y^2 = h_1(x)h_2(x)h_3(x) \quad \text{with } h_i = \delta^{-1}(g'_{i+1}g_{i+2} - g_{i+1}g'_{i+2}).$$

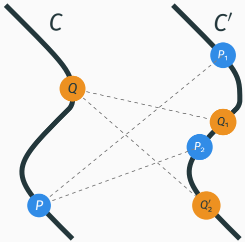
The isogeny $\phi : Jac(C) \to Jac(C')$ is called **Richelot isogeny**.

Richelot correspondence

Richelot isogenies are evaluated using the **Richelot correspondence** $R \subset C \times C'$:

$$R : 0 = g_1(u)h_1(u') + g_2(u)h_2(u')$$
$$vv' = g_1(u)h_1(u')(u - u')$$

for points $(P, P') = ((u, v), (u', v')) \in C \times C'$.



This induces a map $\phi : Jac(C) \to Jac(C')$, where

$$[P + Q - D_\infty] \mapsto [P_1 + P_2 + Q_1 + Q_2 - 2 \cdot D_\infty] = [P' + Q' - D_\infty]$$

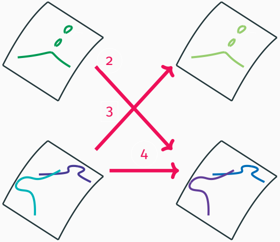
Methods for the evaluation of Richelot isogenies

1. Naive method (previous slide):
   - Representation $(P, Q) \in Jac(C)$
   - Requires factorizations and field extensions

2. Gröbner basis approach (implementation of the SIDH attack by Castryck-Decru):
   - Mumford representation $(a(x), b(x)) \in Jac(C)$
   - Idea: Image of (a, b) is essentially GB of $I = (a, b) + I(C) + I(C') + I(R)$.

3. Explicit formulas (K.)
   - Mumford representation $(a(x), b(x)) \in Jac(C)$
   - Idea: Model similar to Montgomery model for elliptic curves $y^2 = x(x^2 + Ax + 1)(x^2 + Bx + C)$, and find explicit formulas for the map.

Non-generic cases



2. Splitting $\phi : Jac(C) \to E \times E'$
3. Gluing $\phi : E \times E' \to Jac(C)$
4. Product $\phi : E \times E' \to E'' \times E'''$

In cases 2 and 3, there exist degree-2 covers $C \to E$ and $C \to E'$.
$\Rightarrow$ one can deduce explicit formulas

Example

$$\begin{tikzcd}[column sep=tiny] & C : y^2 = (x^2-1)(x^2-2)(x^2-3) \arrow[dl, "x^2 \mapsto x"'] \arrow[dr, "x^2 \mapsto 1/x"] & \\ E : y^2 = (x-1)(x-2)(x-3) & & E' : y^2 = 6(x-1)(x-1/2)(x-1/3) \end{tikzcd}$$

Isogenies in higher dimensions

Kummer surface

Dimension 2 Before, we used the identification $Jac(C)(K) \simeq \mathrm{Pic}^0_C(K)$. We can also view $Jac(C)$ as a variety!

- Cassels-Flynn: $Jac(C) = V(F_1, \ldots, F_{72}) \subset \mathbb{P}^{15}$.
- Kummer surface: $K = Jac(C)/\langle \pm 1 \rangle = V(F) \subset \mathbb{P}^3$ quartic surface.
  - K has 16 singularities.
  - Remnants of the group structure: Multiplications, isogenies.

Models for the Kummer surface

- The "standard model" with $C : y^2 = f(x)$

$$K : (x_1^2 - 4x_0x_2)x_3^2 - 2F_1(x_0, x_1, x_2)x_3 + F_0(x_0, x_1, x_2) = 0,$$

  where F_0, F_1 are explicitly known polynomials.
- The theta model

$$\begin{aligned} K : & x_0^4 + x_1^4 + x_2^4 + x_3^4 - 2Ex_0x_1x_2x_3 - F(x_0^2x_3^2 + x_1^2x_2^2) \\ & - G(x_0^2x_2^2 + x_1^2x_3^2) - H(x_0^2x_1^2 + x_2^2x_3^2) = 0, \end{aligned}$$

  where E, F, G, H are constants.

Kummer varieties

Dimension d

- An abelian variety A of dimension $d > 3$ can not always be represented as the Jacobian of a curve.
- For the Kummer variety $K = A/\langle \pm 1 \rangle$, the level-2 theta functions define a map
$$\iota : K \to \mathbb{P}^{2^d - 1}.$$
This is an embedding if A is irreducible.

Uniform Representation for all p.p.a.v.

Isogenies in theta coordinates

Algorithm for $(\ell, \ldots, \ell)$-isogenies of d-dimensional p.p.a.v.
(char(k) $\nmid \ell$, $\ell \neq 2$)

- Cosset-Lubicz-Robert (2014): $\tilde{O}(\ell^d)$ if $\ell \equiv 1 \pmod 4$, $\tilde{O}(\ell^{2d})$ if $\ell \equiv 3 \pmod 4$.
- Lubicz-Robert (2022): $O((n\ell)^d \log(\ell))$ for level n even.

Special case: $(2^n, \ldots, 2^n)$-isogenies

- notes on a generic algorithm for arbitrary dimension d: Robert (2023)
- $d = 1$: Robert-Sarkis (2024)
- $d = 2$: Dartois-Maino-Pope-Robert (2024)
- $d = 4$: Dartois (in preparation)

Thanks for your attention!