Computation of isogenies in higher genus

Marius Vuille

September 2021

Abstract

In this course we will discuss about the computation of isogenies between polarized abelian varieties, and highlight the basics behind one of the approaches, using the theory of theta functions and projective embeddings.

1 Introduction

There are two things one can understand when people talk about "isogeny computation", and both equally deserve to be called so. Let's for simplicity assume we are in genus 1, and let us fix an algebraically closed field k.

1. Given two elliptic curves E and E' that are isogenous, one could be interested in
   - finding the/a kernel of the/an isogeny.
   - finding the equations of a/the isogeny $f\colon E \to E'$.
   - evaluating an isogeny f on points (i.e. given $P \in E(k)$, compute $f(P) \in E'(k)$).

2. Given an elliptic curve E and a finite subgroup $G \subset E(k)$, one could be interested in
   - finding the target elliptic curve $E' = E/G$.
   - finding equations for $f\colon E \to E'$.
   - evaluating f on points.

In this course we will focus on the second question only. While for elliptic curves you may take any finite subgroup of your choice, there are rather restrictive conditions on the kernel for the existence of an isogeny in higher dimensions (which we will discuss in Section 3.1).
As we already know, for elliptic curves we can find algebraic equations that define the variety, and we can find equations for isogenies (Vélu's formula), i.e. given $P = (x_P, y_P) \in E(k)$ find "quotients of polynomials" so that $f(x_P, y_P) = (f_1(x_P, y_P), f_2(x_P, y_P)) \in E'(k)$. In higher dimensions things get more complicated. The goal of this course is to see why things are getting more complicated, which additional information one has to take into account when studying higher dimensions, and highlight some of the ideas on how to compute isogenies in this case.

2 Polarizations

Elliptic curves are nice since we know/can determine their algebraic equations. But we tend to ignore an additional natural object elliptic curves (and Jacobian varieties in general) are endowed with, which are *polarizations*. There is a rather technical definition (algebraic equivalence class of an ample line bundle), an easier way to see it is: "a certain kind of isogeny $A \to A^\vee$" (here, A is an abelian variety and $A^\vee$ its dual abelian variety). We will see in Section 2.2 how polarizations look like over $\mathbb{C}$.

2.1 Why do polarizations matter?

Let us state two reasons why it is necessary to look at polarizations when one studies higher-dimensional abelian varieties.

i) For a Jocabian variety of a curve a (principal) polarization uniquely determines the underlying curve (up to isomorphism). E.g. we know from dimension 1 that if E is an elliptic curve, then any finite subgroup G induces an isogeny $E \to E/G =: E'$, and E' is a unique (up to isomorphism) well defined elliptic curve. However, for a higher-dimensional Jacobian variety $\mathrm{Jac}(C)$, assuming that for some finite subgroup G we know that the quotient is the Jacobian variety of some smooth curve, i.e. there exists C' such that $\mathrm{Jac}(C)/G \cong \mathrm{Jac}(C')$, the curve C' need **not** be unique! There might exist C'' not isomorphic to C' such that $\mathrm{Jac}(C'') \cong \mathrm{Jac}(C')$ (as abelian varieties). As we know from Torelli's theorem, if one considers pairs of a Jacobian variety together with a *principal polarization*, then an isomorphism class of principally polarized Jacobians uniquely determines an isomorphism class of curves. Hence, if one wants to compute isogenies from kernel (i.e. given $\mathrm{Jac}(C)$ and G, compute the curve C' such that $\mathrm{Jac}(C)/G \cong \mathrm{Jac}(C')$) one **needs** to consider principal polarizations too!

ii) The Jacobian variety $\mathrm{Jac}(C)$ is an abelian variety, and the group structure is easy to understand (it is probably also easy to construct group morphisms $\mathrm{Jac}(C) \to \mathrm{Jac}(C')$). But it is highly non-trivial to see/describe the algebraic structure (recall that for elliptic curves we have/can find an equation $E : y^2 = x^3 + ax + b$). A way to study the algebraic structure of higher-dimensional abelian varieties is via the theory of projective embeddings by means of theta functions (for which you need polarizations).

2.2 Polarizations over $\mathbb{C}$

Recall that any connected compact complex Lie group is a complex torus $A = \mathbb{C}^g/\Lambda$.

Definition 1. A *polarization* H on A is a positive definite hermitian form $H\colon \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{C}$, which, if written $H = \mathrm{Re}H + i\,\mathrm{Im}H$, must satisfy $\mathrm{Im}H|_{\Lambda\times\Lambda} \to \mathbb{Z}$.

By the elementary divisor theorem there exists a $\mathbb{Z}$-basis $\lambda_1, \ldots, \lambda_g, \mu_1, \ldots, \mu_g$ of Λ such that

$$\mathrm{Im}H = \begin{pmatrix} 0 & \delta \\ -\delta & 0 \end{pmatrix},$$

$\delta = \mathrm{diag}(d_1, .., d_g)$ with $d_1 \mid \cdots \mid d_g$. The form $\mathrm{Im}H$ is non-degenerate, which is equivalent to $d_i \neq 0$ for all i. The vector $(d_1, \ldots, d_g)$ is called the *type* of the polarization, $d_1 \cdots d_g$ is the *degree* of the polarization, and degree-1 polarizations are called *principal polarization*.

Example 1. Let $E = \mathbb{C}/\tau\mathbb{Z} \oplus \mathbb{Z}$ be an elliptic curve, where $\tau = \tau_1 + i\tau_2$ with $\tau_2 > 0$. Consider the hermitian form

$$H(u, v) = \frac{u \cdot \bar{v}}{\tau_2}.$$

It is easily seen to be positive, and on the (natural) basis $\{\tau, 1\}$ of $\tau\mathbb{Z} \oplus \mathbb{Z}$ we have:

$$\begin{aligned} &\mathrm{Im}H(\tau, \tau) = \mathrm{Im}H(1, 1) = 0 \\ &\mathrm{Im}H(\tau, 1) = 1 = -\mathrm{Im}H(1, \tau). \end{aligned}$$

We deduce that elliptic curves are principally polarized!

This construction generalizes to tori $\mathbb{C}^g/\Omega\mathbb{Z}^g \oplus \mathbb{Z}^g$, where $\Omega \in \mathcal{H}_g$ - the Siegel upper half-space. ($\mathcal{H}_g$ is a moduli space for principally polarized abelian varieties (p.p.a.v.) of dimension g.)

2.3 Theta functions over $\mathbb{C}$

Recall the definition of the Jacobi theta function

$$\theta \colon \mathbb{C} \times \mathcal{H} \to \mathbb{C}, \;\; \theta(z, \tau) = \sum_{\nu \in \mathbb{Z}} \exp(\pi i \nu^2 \tau + 2\pi i \nu z).$$

Given $a, b \in \mathbb{R}$, we can define the theta function with characteristics as

$$\theta \begin{bmatrix} a \\ b \end{bmatrix} (z, \tau) = \sum_{\nu \in \mathbb{Z}} \exp(\pi i (\nu + a)^2 \tau + 2\pi i (\nu + a)(z + b)).$$

(With generalization to higher dimensions, replacing $\tau \in \mathcal{H}$ with $\Omega \in \mathcal{H}_g$.)
Consider τ fixed, and let us have a look at the torus $E_\tau = \mathbb{C}/\tau\mathbb{Z} \oplus \mathbb{Z}$ and the theta function $\theta \begin{bmatrix} a \\ b \end{bmatrix} (z, \tau)$. It satisfies some "quasi-periodicity" with respect to the lattice $\tau\mathbb{Z} \oplus \mathbb{Z}$:

$$\theta \begin{bmatrix} a \\ b \end{bmatrix} (z + n\tau + m) = \exp(-\pi i n^2 \tau - 2\pi i n z + 2\pi i (am - bn))\, \theta \begin{bmatrix} a \\ b \end{bmatrix} (z).$$

If we tweak the function a bit (to turn it into a theta function for a degree-4 polarization, see Example 2) and define

$$\widetilde{\theta} \begin{bmatrix} a \\ b \end{bmatrix} (z) := \theta \begin{bmatrix} a \\ b \end{bmatrix} (4z, 4\tau)$$

and restrict to $a \in \{d/4 : d = 0, .., 3\}$ and $b = 0$, we obtain four functions that satisfy

$$\widetilde{\theta} \begin{bmatrix} d/4 \\ 0 \end{bmatrix} (z + n\tau + m) = \exp(-4\pi i n^2 \tau - 8\pi i n z)\, \widetilde{\theta} \begin{bmatrix} d/4 \\ 0 \end{bmatrix} (z).$$

Note that the quasi-periodicity no longer depends on the characteristic $d/4$.
The four functions $\widetilde{\theta} \begin{bmatrix} 0/4 \\ 0 \end{bmatrix}, \ldots, \widetilde{\theta} \begin{bmatrix} 3/4 \\ 0 \end{bmatrix}$ are not periodic with respect to $\tau\mathbb{Z} \oplus \mathbb{Z}$, and therefore do not induce functions on the torus $\mathbb{C}/\tau\mathbb{Z} \oplus \mathbb{Z}$. However:

- Quotients of theta functions are $\mathbb{C}$-valued functions on $\mathbb{C}/\tau\mathbb{Z} \oplus \mathbb{Z}$ (called abelian functions).
- The map

$$\varphi \colon \mathbb{C}/\tau\mathbb{Z} \oplus \mathbb{Z} \to \mathbb{P}^3, \; z \mapsto (\widetilde{\theta} \begin{bmatrix} 0/4 \\ 0 \end{bmatrix} (z) : \cdots : \widetilde{\theta} \begin{bmatrix} 3/4 \\ 0 \end{bmatrix} (z))$$

  is a well defined function (provided not all $\widetilde{\theta} \begin{bmatrix} d/4 \\ 0 \end{bmatrix}$ vanish simultaneously).

Theorem 1 (Lefschetz)**.** For $n \geq 3$, if we have n $\mathbb{C}$-linearly independent such functions, then $\varphi\colon \mathbb{C}/\tau\mathbb{Z} \oplus \mathbb{Z} \to \mathbb{P}^{n-1}$ is an analytic embedding.

See e.g. [BL04, Thm. 4.5.1] for the above theorem.

Theorem 2 (Chow)**.** A closed analytic subvariety of $\mathbb{P}^{n-1}$ is an algebraic variety.

As a consequence of the above theorems: given a polarized abelian variety $(\mathbb{C}^g/\Lambda, H)$ with "sufficiently many theta functions", one can embed

$$\mathbb{C}^g/\Lambda \hookrightarrow \mathbb{P}^{n-1},$$

where $n = \dim_{\mathbb{C}}\{\text{theta functions}\}$.

Example 2. The functions $\widetilde{\theta}\left[\begin{smallmatrix}0/4\\0\end{smallmatrix}\right], \ldots, \widetilde{\theta}\left[\begin{smallmatrix}3/4\\0\end{smallmatrix}\right]$ can be seen as theta functions with respect to the polarization $H(u,v) = 4\frac{u\cdot\bar{v}}{\tau_2}$ (which is of type (4)), and they induce an embedding of the elliptic curve $\mathbb{C}/\tau\mathbb{Z} \oplus \mathbb{Z}$ into $\mathbb{P}^3$.

More generally, given a Jacobian variety $\mathrm{Jac}(C)$ with a polarization of sufficiently high degree (e.g. a power of principal polarization), we have an embedding

$$\mathrm{Jac}(C) \hookrightarrow \mathbb{P}^{n-1}.$$

As a consequence: algebraic relations among theta functions can be seen as equations defining $\mathrm{Jac}(C)$. They are referred to as *Riemann's theta relations*. In a series of three papers [Mum66], [Mum67a], [Mum67b], called *On the equations defining abelian varieties*, David Mumford showed that the same is true over any algebraically closed field.

2.4 Theta functions over arbitrary fields

Given an algebraically closed field k, we cannot consider theta functions as actual k-valued functions on the abelian variety, but should see them as global sections of some line bundles. Let A be an abelian variety over k and $\mathcal{L}$ an ample line bundle on A. If $\theta : A \to \mathcal{L}$ is a global section of $\mathcal{L}$ and if $x \in A(k)$, then for any open neighborhood $\mathcal{U}$ of x there exists a k-valued function $\theta_{\mathcal{U}}\colon \mathcal{U} \to k$. On overlaps we have $\theta_{\mathcal{U}}|_{\mathcal{U}\cap\mathcal{V}} = \lambda_{\mathcal{U},\mathcal{V}}\cdot\theta_{\mathcal{V}}|_{\mathcal{U}\cap\mathcal{V}}$ and the "factor of automorphy" $\lambda_{\mathcal{U},\mathcal{V}}\colon \mathcal{U}\cap\mathcal{V} \to k^\times$ does not depend on θ. Given $\theta_1, \ldots, \theta_n\colon A \to \mathcal{L}$, we can thus define a map

$$\varphi\colon A \to \mathbb{P}^{n-1},\ z \mapsto (\theta_{1,\mathcal{U}}(z) : \cdots : \theta_{n,\mathcal{U}}(z)) = (\theta_{1,\mathcal{V}}(z) : \cdots : \theta_{n,\mathcal{V}}(z))$$

(provided not all θ_i vanish simultaneously).

Theorem 3 (Lefschetz)**.** If we have sufficiently many k-linearly independent theta functions, then φ is an algebraic embedding.

3 Computing isogenies from kernel

Given (A, H) a principally polarized abelian variety (here, H stands for the algebraic equivalence class of a line bundle) and a finite subgroup $G \subset A(k)$, we are interested in "computing" the target abelian variety $B := A/G$ and in evaluating the isogeny $f\colon A \to B$ on points (given P, compute $f(P)$). As we have seen, for elliptic curves you can take any finite subgroup G and E/G will always be principally polarizable. In higher dimension you need to carefully pick your subgroup if you want A/G to admit a principal polarization! Let us first list some results that we have at our disposal that will help us to compute A/G:

i) Thomae's formula [Tho70]: if C is a hyperelliptic curve of genus g, we can compute 4^g theta coordinates (evaluated at 0) out of the Weierstrass points of C (up to some projective factor).

ii) Reciprocal of i) [vW98]: knowing 4^g theta coordinates (up to some projective factor) of a hyperelliptic Jacobian evaluated at 0, we can compute the Weierstrass points of the **unique** (up to isomorphism) hyperelliptic curve.

iii) Vanishing criteria [Mum84, Cor. 6.7] and [Mum84, Thm. 9.1]: theta functions (of a certain type) evaluated at 0 tell us whether the underlying principally polarized abelian variety is the Jacobian of a hyperelliptic curve or not (if not, it might not even be a Jacobian).

iv) In dimension 2: all principally polarized abelian varieties are hyperelliptic Jacobians.

v) In dimension 3: all principally polarized abelian varieties are Jacobians, but can be either hyperelliptic (minority) or quartic (majority). By iii) we have a criteria to decide on the nature of the Jacobian, ii) to recover the model of a curve in the hyperelliptic case, and in the quartic case we have a formula as well to compute a plane model (by computing bitangents of the underlying curve, seeWeber's formula [Web76]).

When it comes to the evaluation of the isogeny on points, what we want is: given the theta coordinates $(\theta_1^A(P) : \cdots : \theta_n^A(P)) \in \mathbb{P}^{n-1}$ of a point P, compute the theta coordinates $(\theta_1^{A/G}(f(P)) : \cdots : \theta_n^{A/G}(f(P))) \in \mathbb{P}^{n-1}$ of $f(P)$. In dimension 2 over finite fields, there exists the Magma package *AVIsogenies* (Bisson, Cosset, Robert) for the conversion Mumford $\leftrightarrow$ theta.

3.1 Polarizability of the quotient

Given a principally polarized abelian variety (A, H), one may ask for which finite subgroup $G \subset A(k)$ the quotient A/G does admit a principal polarization (compatible with H via the isogeny $A \to A/G$)? In order to find the answer we need to look at the endomorphism algebra! Recall that the principal polarization induces an anti-involution on $\mathrm{End}(A)$,

$$(\cdot)^\dagger \colon \mathrm{End}(A) \to \mathrm{End}(A),$$

called the *Rosati involution*. An endomorphism $\beta \colon A \to A$ is called a *real endomorphism* if it is fixed by the Rosati involution, i.e. $\beta^\dagger = \beta$. Real endomorphisms form an additive subgroup denoted by $\mathrm{End}^+(A)$. The real endomorphisms whose characteristic polynomial's roots are all positive are called *totally positive real endomorphisms*, and are denoted by $\mathrm{End}^{++}(A)$. It is a well known fact that polarizations on A are in bijection with totally positive real endomorphisms, see e.g. [BL04, Thm. 5.2.4].

Example 3. For an elliptic curve $E/\mathbb{F}_q$, the real endomorphisms are just $\mathbb{Z}$ and hence the polarizations are $\mathbb{Z}_{>0}$.

Note that for a totally positive real endomorphism, $\ker \beta$ is a symplectic space of order $(\deg \beta)^2$, where the symplectic pairing arises as a composition of the Weil pairing with β.
We can now state the criteria for the quotient to be principally polarizable.

Lemma 1. Given a principally polarized abelian variety (A, H) and a finite subgroup $G \subset A(k)$, then A/G admits a principal polarization compatible with H under $A \to A/G$ if and only if there exists $\beta \in \mathrm{End}^{++}(A)$ such that $G \subset \ker \beta$ is maximal isotropic.

Note that by the above lemma, G is necessarily of order $\deg \beta$.

Example 4. For elliptic curves, any cyclic subgroup $G \subset E(k)$ (of order ℓ coprime to the characteristic of k) is maximal isotropic inside $\ker[\ell] = E[\ell]$. Hence, every isogeny from kernel $E \to E/G$ preserves principal polarizability.

3.2 Types of isogenies

Let us fix a dimension $g > 1$, and let ℓ be a prime number (different from $char(k)$). There are different types of isogenies that have been studied:

- $(\ell, \dots, \ell)$-isogenies, those are the isogenies with kernel isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^g$. Since the ℓ-torsion subgroup is exactly $A[\ell] = \ker[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^{2g}$, these isogenies are tightly linked to the real endomorphism $[\ell] \in \mathrm{End}^{++}(A)$ by Lemma 1. In some sense they are very "natural" in that their existence is always guaranteed (and the number of $(\ell, \dots, \ell)$-kernels inside A can be computed and equals $\prod_{i=1}^{g}(\ell^i + 1)$) **but** it remains incredibly hard to compute them! (And would be out of scope for this course.) For an algorithm exploiting projective embeddings and theta functions, see e.g. [CR11], [LR12] or [Rob10]. An implementation for dimension 2 hyperelliptic Jacobians over finite fields is available in the magma package AVIsogenies. There are other, notable approaches too, based on the use of abelian functions (in dimensions 2 and 3), see e.g. [CE15] or [Mil17].

- cyclic isogenies, those are the ones with kernel isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$. The existence of such isogenies is much more restricted, since the existence of totally positive degree-ℓ endomorphfisms is not always guaranteed. One has to look at the real endomorphism algebra $K^+ = \mathrm{End}^+(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ inside $K = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ and the splitting behaviour of the ideal (ℓ) in K^+. Attempts for computing such isogenies (for A ordinary and simple) can be found in [DJRV17] and [Vui20].

  The ideas behind the computation of cyclic isogenies are similar to the ideas for the computation of $(\ell, \dots, \ell)$-isogenies, but there is a major additional difficulty due to polarization (which is linked to the endomorphism β as opposed to the "natural" endomorphism $[\ell]$).

References

[BL04] C. Birkenhake and H. Lange, *Complex abelian varieties*, second ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 302, Springer Verlag, Berlin, 2004.

[CE15] Jean-Marc Couveignes and Tony Ezome, *Computing functions on Jacobians and their quotients*, LMS J. Comput. Math. **18** (2015), no. 1, 555–577. MR 3389883

[CR11] R. Cosset and D. Robert, *Computing (ℓ, ℓ)-isogenies in polynomial time on jacobians of genus 2 curves*, http://eprint. iacr.org/2011/143, 2011.

[DJRV17] Alina Dudeanu, Dimitar Jetchev, Damien Robert, and Marius Vuille, *Cyclic isogenies for abelian varieties with real multiplication*, arXiv:1710.05147, 2017.

[LR12] D. Lubicz and D. Robert, *Computing isogenies between abelian varieties*, Compos. Math. **148** (2012), no. 5, 1483–1515.

[Mil17] Enea Milio, *Computing isogenies between jacobian of curves of genus 2 and 3*, arXiv:1709.06063, 2017.

[Mum66] D. Mumford, *On the equations defining abelian varieties. I*, Invent. Math. **1** (1966), 287–354.

[Mum67a] ———, *On the equations defining abelian varieties. II*, Invent. Math. **3** (1967), 75–135.

[Mum67b] ———, *On the equations defining abelian varieties. III*, Invent. Math. **3** (1967), 215–244.

[Mum84] David Mumford, *Tata lectures on theta. II*, Modern Birkhäuser Classics, Birkhäuser Boston, Inc., Boston, MA, 1984, Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura, Reprint of the 1984 original.

[Rob10] D. Robert, *Fonctions thêta et applications à la cryptologie*, Ph.D. thesis, Nancy, 2010.

[Tho70] J. Thomae, *Beitrag zur Bestimmung von θ(0,...,0) durch die Klassenmoduln algebraischer Funktionen*, Journal fur die Reine und Angewandte Mathematik (1870), 70:201–222.

[Vui20] Marius Lorenz Vuille, *Computing cyclic isogenies between principally polarized abelian varieties over finite fields*, Ph.D. thesis, EPFL, Lausanne, 2020, p. 138.

[vW98] Paul van Wamelen, *Equations for the Jacobian of a hyperelliptic curve*, Trans. Amer. Math. Soc. **350** (1998), 3083–3106.

[Web76] H. M. Weber, *Theorie der Abelschen Functionen vom Geschlecht 3*, Berlin: Druck und Verlag von Georg Reimer (1876).