Quadratic and bilinear forms on abelian varieties

2026/11/18 — **Isogenies of Abelian Varieties, Applications to Post-Quantum Cryptography** — EPFL

Damien Robert



Inria

Table of Contents

1. Introduction
2. What are bilinear and quadratic forms, actually?
3. Bilinear and quadratic forms on abelian varieties
4. Arithmetic structures on geometric objects from bilinear and quadratic forms
5. Algorithmic applications

Table of Contents

1. Introduction
2. What are bilinear and quadratic forms, actually?
3. Bilinear and quadratic forms on abelian varieties
4. Arithmetic structures on geometric objects from bilinear and quadratic forms
5. Algorithmic applications

Codes and lattices

- Strong analogy between code based cryptography and lattice based cryptography
- Analogy used to great effect to transfer results from one to the other

- Isogeny based cryptography seems radically different
- But is it, really?

Module LIP

- A lattice is a free abelian group M of finite rank, endowed with a positive definite homogeneous quadratic form $q : M \to \mathbb{R}$.

- Let K be a number field, O_K its maximal order, and $K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R}$.
- An O_K-lattice is a finitely generated projective O_K-module M of rank r, endowed with a positive definite homogeneous quadratic form $q : M \to \mathbb{R}$, compatible with the scalar action:

$$b(\gamma x, y) = b(x, \overline{\gamma} y) \qquad (\gamma \in K_{\mathbb{R}},\ x, y \in M_{\mathbb{R}}).$$

  Here $M_{\mathbb{R}} = M \otimes_{\mathbb{Z}} \mathbb{R} \simeq K_{\mathbb{R}}^r$, b is the polarization of $q_{\mathbb{R}}$, and conjugation acts componentwise on $K_{\mathbb{R}}$.
- An isometry of O_K-lattices $\phi : (M_1, q_1) \to (M_2, q_2)$ is an O_K-linear isomorphism such that

$$\phi^* q_2 = q_1.$$

- Module LIP (lattice isomorphism problem): given two isometric O_K-lattices (M_1, q_1) and (M_2, q_2), find an explicit O_K-linear isometry between them.

Module LIP and Hermitian forms

- When K is totally real or a CM field*, and q is rational (i.e. $q(M) \subset \mathbb{Q}$), there is a unique Hermitian form $H : M \times M \to K$ such that

$$b(x,y) = \mathrm{Tr}_{K/\mathbb{Q}} H(x,y)$$

- Up to rescaling, H takes values in O_K, and $Q(x) = H(x,x)$ is positive definite with values in O_F, F the totally real subfield of K, so that

$$q(x) = \tfrac{1}{2} \mathrm{Tr}_{K/\mathbb{Q}} Q(x).$$

- An O_K-linear isomorphism $\psi : M_1 \to M_2$ preserves q iff it preserves H, equivalently Q. The same holds for n-similitudes.
- Thus module LIP asks for an isometry of Hermitian modules.

*or even a totally definite quaternion algebra

The isogeny problem

- The isogeny problem asks, given two isogenous elliptic curves $E_1, E_2/\mathbb{F}_q$, or more generally two isogenous ppavs $(A_1, \lambda_1), (A_2, \lambda_2)/\mathbb{F}_q$, to find a polarised isogeny between them, i.e. an isogeny $\phi : A_1 \to A_2$ such that $\phi^* \lambda_2 = n\lambda_1$ for $n \in \mathbb{Z}$.
- Sometimes we add some constraints on n (e.g. $n = 2^e$), or on ϕ (e.g. with respect to level structures)

- Let R be an order in a totally real or CM field K.
- An orientation of (A, λ_A) is an inclusion $i : R \to \mathrm{End}(A)$ compatible with the polarisation: $i(r)^\dagger = i(\bar{r})$.
- The oriented isogeny problem asks to find an oriented polarised isogeny between $(A_1, \lambda_1), (A_2, \lambda_2)$:

$$\phi(i_1(r) \cdot x) = i_2(r) \cdot \phi(x)$$

A unifying framework

- Both instances are a special case of the quadratic module similitude problem.
- A quadratic module (M, q) is an R-module M endowed with a positive definite quadratic form $q : M \to Z$ (for some suitable arithmetic object Z)
- The quadratic module similitude problem asks to find a similitude $\phi : (M_1, q_1) \to (M_2, q_2)$:

$$\phi^* q_2 = n q_1 \quad n \in \mathbb{Z}^*$$

- **Goal of this talk**: explain how to see a ppav as a quadratic module
- Warning : this module will have torsion, and is not of finite rank. Most importantly it lives in a different "mathematical universe".
- Constructing this "mathematical universe" is a bit technical so I will skip a lot of details
- I'll include more details in footnotes, so **do not read the footnotes**‡

*Or even a totally positive real element of R

‡You lost already!

Damien trying to sell his talk to the organizers

So the plan is to present a somewhat different view point on polarisations and line bundles on abelian varieties than the usual one.

In particular, in the first part, I plan to explain how we can view a line bundle on A as a (derived) quadratic form $q : A \to B\mathbb{G}_m$ (so with values in torsors), and a polarisation as a (derived) symmetric bilinear form $b : A \times A \to B\mathbb{G}_m$.

In the second part, I'll give some algorithmic applications of this view point.

(Before you get scared: I'll try my best to give an **accessible** talk…)

Table of Contents

1 Introduction

2 What are bilinear and quadratic forms, actually?

3 Bilinear and quadratic forms on abelian varieties

4 Arithmetic structures on geometric objects from bilinear and quadratic forms

5 Algorithmic applications

Projective embeddings and line bundles

- To work with an abelian variety $A/\mathbb{F}_q$, we need coordinates
- These correspond to an embedding $i : A \to \mathbb{P}^N_{\mathbb{F}_q}$
- Often we are happy to relax the embedding to a map $i : A \to \mathbb{P}^N_{\mathbb{F}_q}$ defined everywhere
- We have a pullback square:

$$\begin{array}{ccc} X_{\mathcal{L}} & \longrightarrow & \mathbb{A}^{N+1} \setminus \{0\} \\ \downarrow & & \downarrow \\ A & \xrightarrow{i} & \mathbb{P}^N = \left(\mathbb{A}^{N+1} \setminus \{0\}\right)/\mathbb{G}_m \end{array}$$

- $\mathbb{A}^{N+1} \setminus \{0\} \to \mathbb{P}^N$ is a (punctured) line bundle*
- So its pullback $X_{\mathcal{L}} \to A$ is too, and $A = X_{\mathcal{L}}/\mathbb{G}_m$
- Adding the zero section gives a line bundle whose sheaf of sections is an invertible sheaf $\mathcal{L}^\vee$.
- Pulling back the $N+1$ standard coordinate sections $X_i \in \Gamma(\mathbb{P}^N, \mathcal{O}_{\mathbb{P}^N}(1))$ gives coordinates:

$$X_i \in \Gamma(A, \mathcal{L}) \simeq \left\{ f \in \Gamma(X_{\mathcal{L}}, \mathcal{O}_{X_{\mathcal{L}}}) \,\middle|\, f(\lambda x) = \lambda f(x) \quad \forall \lambda \in \mathbb{G}_m \right\}$$

- These sections have no common zero
- $\mathbb{P}^N$ is the moduli space of line bundles with $N+1$ sections without base points:

$$\{\text{Maps } A \to \mathbb{P}^N\} \simeq \left\{ \mathcal{O}_A^{N+1} \twoheadrightarrow \mathcal{L}, \quad \mathcal{L} \text{ invertible} \right\}$$

*Equivalently: a $\mathbb{G}_m$-torsor

Partial coordinates

- It is convenient to be able to work with $N+1$ partial coordinates X_i
- These can have base points: points $P \in A(\bar{k})$ such that $X_i(P) = 0$ for every i
- So we want to consider $\mathbb{G}_m$-equivariant maps $X_{\mathcal{L}} \to \mathbb{A}^{N+1}$ that may not land in $\mathbb{A}^{N+1} \setminus \{0\}$
- This gives a pullback square

$$\begin{array}{ccc} X_{\mathcal{L}} & \longrightarrow & \mathbb{A}^{N+1} \\ \downarrow & & \downarrow \\ A & \longrightarrow & [\mathbb{A}^{N+1}/\mathbb{G}_m] \end{array}$$

- We have

$$\{\text{Maps } A \to [\mathbb{A}^{N+1}/\mathbb{G}_m]\} \simeq \left\{O_A^{N+1} \to \mathcal{L}, \quad \mathcal{L} \text{ invertible}\right\}$$

- Because $\mathbb{G}_m$ fixes $0 \in \mathbb{A}^{N+1}$, we need a special quotient $[\mathbb{A}^{N+1}/\mathbb{G}_m]^*$

*Called a stacky quotient because it retains stabilizers

No coordinates

- $X_{\mathcal{L}}$ is a space of coordinate lifts for A; we want to describe it without choosing particular coordinate sections
- Consider the diagram above taking zero coordinate sections ($N + 1 = 0$):

$$\begin{array}{ccc} X_{\mathcal{L}} & \longrightarrow & \operatorname{Spec} k \\ \downarrow & & \downarrow \\ A & \longrightarrow & B\mathbb{G}_m = [\operatorname{Spec} k / \mathbb{G}_m] \end{array}$$

- This is again a pullback square*
- $B\mathbb{G}_m$ is the classifying stack of line bundles:

$$\{\text{Maps } A \to B\mathbb{G}_m\} \simeq \{\mathcal{L} \text{ invertible}\}$$

- This is a weird space: it has dimension $N = 0 - 1 = -1$

*of stacks, so a 2-pullback square

The action groupoid

- When a group G acts on a set X, the naive quotient $X/G = \{\text{orbits}\}$ forgets X[*]
- Instead we can build the action groupoid: $[X/G]$.
- This is a category, where objects are given by the $x \in X$, and arrows of the form

$$g : x \to g.x$$

- A G-equivariant map induces a functor $[X/G] \to [Y/G]$
- In particular we have a canonical map $[X/G] \to BG = [*/G]$
- BG has one object $*$, but this element has nontrivial automorphisms: $\mathrm{Aut}(*) = G$
- This map remembers X, as the pullback:

$$\begin{array}{ccc} X & \longrightarrow & * \\ \downarrow & & \downarrow \\ [X/G] & \longrightarrow & BG \end{array}$$

[*] However if we know that the action was free, then we have a non canonical isomorphism $X \simeq \coprod_{x \in X/G} G$

Stacky quotients

- For G/k a group scheme acting on X, $[X/G]$ is the sheafified* version of the action groupoid
- Alternatively it is the action groupoid constructed internally in the fppf topos

- Let $BG = [\mathrm{Spec}\, k/G]$. Then an object in $BG(T)$ is a G-torsor on T: it is trivial only fppf-locally
- BG is the classifying stack of G-torsors
- $\pi_0(BG(k)) = H^1_{fppf}(k, G) = H^1(k, G)$**
- At the trivial torsor $*$, $\pi_1(BG(k), *) = G(k)$

*Or stackification

**Where the last equality assumes that G is smooth so $H^1_{fppf}(k, G) = H^1_{etale}(k, G)$

Everyone ♡ ∞-categories

- To construct our good quotients we had to leave the world of sets (or sheaves of sets, i.e. of topos) to instead consider groupoids (and sheaves of groupoids, i.e. stacks)
- Quotients are a special case of geometric realisations*, it will be convenient to have "good" geometric realisations
- For that we need to work with ∞-groupoids (and sheaves of ∞-groupoids, i.e. an ∞-topos).

- It turns out that ∞-categories work almost the same as ordinary categories (and in many cases work out better), modulo a few adjustments:
  - Replace everywhere the base category Set by the base ∞-category Ani of ∞-groupoids (aka Animae, aka homotopy types of spaces)
  - Replace everywhere equalities $=$ by equivalences $\simeq$ (aka homotopies), including equivalences between equivalences and so on. Notably an equivalence $\gamma : x \simeq y$ has to be witnessed explicitly (e.g. by a path between x and y).
  - To look cool, randomly add the word "homotopy" or the letter h in the formulas

*i.e. colimits of simplicial objects

Everyone ♡ ∞-categories

Example. Instead of saying:

The set of morphisms $\mathrm{Hom}(G_1, G_2)$ between two groups G_1, G_2 is the set of maps $\phi : G_1 \to G_2$ that satisfy the extra property $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$

Say:

The anima of morphisms $\mathrm{Map}(G_1, G_2)$ between two animated groups G_1, G_2 is the anima of maps $\phi : G_1 \to G_2$ along with the extra structure given by equivalences $\gamma_{g_1,g_2} : \phi(g_1 g_2) \simeq \phi(g_1)\phi(g_2)$ and appropriate higher coherence conditions on these γ_{g_1,g_2} (and recursively).

From Animae back to Sets

- If X is an Anima, $\pi_0(X)$ is the set of elements of X up to isomorphisms.
- If $x \in X$, then $\mathrm{Aut}_x(X)$* is an Anima, and we let $\pi_1(X, x) = \pi_0(\mathrm{Aut}_x(X))$, and so on.

*This is the loop space $\Omega_x X$

Topoi as mathematical universes

- A topos is its own "Mathematical universe": it has its own internal logic
- The internal logic "this object is foo" encodes into "this object is locally foo" in the external logic
- Warning ☙: the law of excluded middle does not hold in general ⇒ we use intuitionistic logic

- ∞-topoi also have their own internal logic, given by HoTT (Homotopy Type Theory)

Bilinear and quadratic forms in an ∞-topos: the internal point of view

- In the standard topos Set, a bilinear form $b : X \times Y \to Z$ between abelian groups is a map that satisfies the equations:

$$b(x_1 + x_2, y) = b(x_1, y) + b(x_2, y)$$
$$b(x, y_1 + y_2) = b(x, y_1) + b(x, y_2)$$

- A quadratic map (i.e. a map of degree ≤ 2) $q : X \to Z$ is a map that satisfies

$$q(x + y + z) - q(y + z) - q(x + z) - q(x + y) + q(x) + q(y) + q(z) - q(0) = 0$$

- Equivalently,

$$b_q(x, y) = q(x + y) - q(x) - q(y) + q(0)$$

  is symmetric bilinear
- q is homogeneous of degree 2 iff $q(0) = 0$ and $q(-x) = q(x)$.
- The exact same definitions work internally in a topos
- And also in an ∞-topos, provided we replace the equalities by equivalences, e.g. a quadratic map satisfies

$$q(x + y + z) - q(y + z) - q(x + z) - q(x + y) + q(x) + q(y) + q(z) - q(0) \simeq 0$$

  via equivalences that have to satisfy some higher coherences*

*These higher coherences do a lot of the heavy lifting… In practice, we will be mostly working with 1-truncated objects, so the equivalences on our equivalences will be equalities.

Bilinear and quadratic forms in a topos: the external point of view

- A bilinear map $b : X \times Y \to Z$ is the same as a $\mathbb{Z}$-linear map $X \otimes_{\mathbb{Z}} Y \to Z$
- A symmetric bilinear map $b : X \times X \to Z$ is the same as a $\mathbb{Z}$-linear map $\mathrm{Sym}^2 X \to Z$
- A quadratic map $q : X \to Z$ is the same as a $\mathbb{Z}$-linear map $P_2 X \to Z$ where $X \to P_2 X$ is the universal degree ≤ 2 map

- We just need to extend (e.g.) the functor Sym^2 to any ∞-topos, to define a symmetric bilinear map $b : X \times X \to Z$ as an element of $\mathrm{Hom}_{\mathbb{Z}}(\mathrm{Sym}^2 X, Z)$
- For a sheaf of $\mathbb{Z}$-modules X in a topos $\mathrm{Sh}(\mathcal{X}, \mathrm{Set})$, we simply sheafify the functor

$$U \mapsto \mathrm{Sym}^2 X(U).$$

- For a sheaf of animated $\mathbb{Z}$-modules X in an ∞-topos $\mathrm{Sh}(\mathcal{X}, \mathrm{Ani})$, we also sheafify the functor $U \mapsto \mathrm{Sym}^2 X(U)$. But first, we need to make sense of how to build Sym^2 on animated $\mathbb{Z}$-modules

Animation of a functor

- The category of R-modules is strongly finitely presentable: it is freely generated by finite free modules under sifted colimits (i.e. filtered colimits and "quotients"*)
- Equivalently, a module M is the same as a contravariant functor from finite free modules to Set that sends a coproduct $R^n \oplus R^m$ to a product.
- A functor F from finite free modules to a cocomplete category $\mathcal{D}$ uniquely extends to a sifted-colimit preserving functor from R-modules to $\mathcal{D}$.
- This extension commutes with colimits iff $F(0) = 0_D, F(R^n \oplus R^m) = F(R^n) \coprod F(R^m)$
- Example: $\mathrm{Sym}^2(R^n) = R^{n(n+1)/2}$ has basis $e_i \cdot e_j$ $(i \leq j)$.

*More precisely reflexive coequalizers

Animation of a functor

- The category of animated R-modules is freely generated by finite free modules under ∞-sifted colimits (i.e. filtered colimits and geometric realizations).
- Equivalently, an animated module M is the same as a contravariant functor from finite free modules to Ani that sends a coproduct $R^n \oplus R^m$ to a product.
- A functor F from finite free modules to a cocomplete ∞-category $\mathcal{D}$ uniquely extends to an ∞-sifted-colimit preserving functor from animated R-modules to $\mathcal{D}$.

- We have an inclusion $\mathrm{Mod}_R \subset \mathsf{Ani}(\mathrm{Mod}_R)$ of classical R-modules into animated R-modules.
- Thus a functor F from finite free R-modules to R-modules uniquely extends to a functor F from R-modules to R-modules and to a functor $\mathsf{Ani}(F)$ from animated R-modules to animated R-modules.
- For an animated module:

$$\pi_0 \mathsf{Ani}(F)(M) = F(\pi_0(M)).$$

Animation vs Derivation

- Animation can be seen as an extension of derived functors to the non additive case
- By Dold-Kan, we have an isomorphism $\mathsf{Ani}(\mathsf{Mod}_R) \simeq D_{\geq 0}(R)$ between animated R-modules and the connective derived category (in homological grading)
- If F preserves sifted colimits **and** is additive, it is right exact, and its animation is its left derived functor:

$$\mathsf{Ani}(F) \simeq LF : D_{\geq 0}(R) \to D_{\geq 0}(R).$$

- In a topos $\mathsf{Sh}(\mathcal{X}, \mathsf{Set})$, $D_{\geq 0}(\mathsf{Sh}(\mathcal{X}, \mathsf{Mod}_R)) \simeq \mathsf{Sh}_{hyp}(\mathcal{X}, D_{\geq 0}(R))$.
- For F additive right exact as above, if $\mathcal{F}$ is its sheafification, then $L\mathcal{F}$ is the hypersheafification of $\mathsf{Ani}(F)$.

- If $F : \mathsf{Mod}_R \to \mathsf{Mod}_R$ preserves sifted colimits but is not additive, we still have that the hypersheafification of $\mathsf{Ani}(F)$ coincides with Dold-Puppe construction of $L\mathcal{F}$ via simplicial flat resolutions.

Derived bilinear and quadratic forms

In $D_{\geq 0}(\mathsf{Sh}(\mathcal{X}, Ab))$:

- A derived bilinear form $A \times B \to B\mathbb{G}_m$ is an element of $R\,\mathsf{Hom}_{\geq 0}(A \otimes^L B, \mathbb{G}_m[1])$
- A derived symmetric bilinear form $A \times A \to B\mathbb{G}_m$ is an element of $R\,\mathsf{Hom}_{\geq 0}(L\,\mathsf{Sym}^2 A, \mathbb{G}_m[1])$
- A derived quadratic form $A \to B\mathbb{G}_m$ is an element of $R\,\mathsf{Hom}_{\geq 0}(LP_2 A, \mathbb{G}_m[1])$

- $L\,\mathsf{Sym}^2, LP_2 : D_{\geq 0}(\mathsf{Sh}(\mathcal{X}, Ab)) \to D_{\geq 0}(\mathsf{Sh}(\mathcal{X}, Ab))$ can be computed via simplicial flat resolutions or via hypersheafification of the animation of the functors $\mathsf{Sym}^2, P_2 : Ab \to Ab$.

Table of Contents

1 Introduction

2 What are bilinear and quadratic forms, actually?

3 Bilinear and quadratic forms on abelian varieties

4 Arithmetic structures on geometric objects from bilinear and quadratic forms

5 Algorithmic applications

Line bundles on abelian varieties

On an abelian variety A/k, the following are equivalent:

- A Weil divisor D (up to linear equivalence)
- A Cartier divisor (modulo principal divisors)
- A line bundle $\mathcal{L} \to A$ (up to isomorphism)
- The invertible sheaf L of sections $A \to \mathcal{L}$ (conversely $\mathcal{L}$ is the total space of L)
- A $\mathbb{G}_m$-torsor $X_{\mathcal{L}} = \mathcal{I}som(\mathcal{L}, A \times \mathbb{A}^1) = \mathcal{I}som(L, \mathcal{O}_A) \simeq \mathcal{L}^{\vee \times}$ (up to isomorphism)
- A map $A \to B\mathbb{G}_m$ (up to equivalence)

In what follows, we will work in the internal logic of the fppf ∞-topos.*

*Given by the fppf sheaves of Animae. Note that schemes over k embed into the fppf topos, hence also into the fppf ∞-topos. In practice, we will mostly work in the prestable ∞-category of sheafs of animated abelian groups or sheafs of animated R-modules.

Quadratic forms on abelian varieties

Theorem (Grothendieck, Breen)

Let A/k be an abelian variety, $\mathcal{L}$ a line bundle on A, and $q_{\mathcal{L}} : A \to B\mathbb{G}_m$ the associated map. Then $q_{\mathcal{L}}$ is automatically quadratic[a].

[a] More precisely has a unique quadratic structure

Sketch.

Let $p_1, p_2, p_3 : A^3 \to A$ be the three projections, $p_{ij} = p_i + p_j, p_{123} = p_1 + p_2 + p_3, p_0 = 0_A$. Then the theorem of the cube gives a trivialisation of

$$p_{123}^*\mathcal{L} \otimes p_{12}^*\mathcal{L}^{-1} \otimes p_{23}^*\mathcal{L}^{-1} \otimes p_{13}^*\mathcal{L}^{-1} \otimes p_1^*\mathcal{L} \otimes p_2^*\mathcal{L} \otimes p_3^*\mathcal{L} \otimes p_0^*\mathcal{L}^{-1},$$

hence

$$q(x+y+z) - q(y+z) - q(x+z) - q(x+y) + q(x) + q(y) + q(z) - q(0) \simeq 0$$

Now a map $A^r \to \mathbb{G}_m$ has to be constant because A is proper and $\mathbb{G}_m$ affine. So the higher coherence conditions are automatically satisfied. □

- We say that $q_{\mathcal{L}}$ is a positive definite quadratic form if $\mathcal{L}$ is ample.
- Ample line bundles form a cone in $NS(A)_{\mathbb{R}}$, so this notion behaves as expected.

Symmetric bilinear forms on abelian varieties

- Let q be a quadratic form $q : A \to B\mathbb{G}_m$ corresponding to a line bundle $\mathcal{L}$
- For convenience we will always assume that we have fixed an equivalence $q(0) \simeq 0$, this is equivalent to choosing a rigidification of $\mathcal{L}$ at 0.
- Let $b_q(x,y) \simeq q(x+y) - q(x) - q(y)$, this is a symmetric bilinear form

$$b_q : A \times A \to B\mathbb{G}_m$$

- Warning ❦: b_q does not determine q[*]
- From b_q, we can only reconstruct $q_2(x) = b_q(x,x)$ which corresponds to $\mathcal{L} \otimes [-1]^*\mathcal{L}$.

[*] Because changing q by a linear factor does not change b_q

Linear forms on abelian varieties

- Since q is normalized, it is of degree ≤ 1 iff it is linear, equivalently, $b_q \simeq 0$*

$$q(x+y) \simeq q(x) + q(y)$$

- In other words:

$$q \in \mathcal{H}om_{\mathbb{Z}}(A, B\mathbb{G}_m) \simeq A^\vee \simeq \mathrm{Pic}^0 A$$

- Indeed, by the theorem of the square, if $\mathcal{L} \in \mathrm{Pic}^0(A)$, we have

$$\mathcal{L}_{x+y} \otimes \mathcal{L}_0 \simeq \mathcal{L}_x \mathcal{L}_y$$

- So, $A^\vee$ gives precisely the characters $\chi : A \to B\mathbb{G}_m$

- For a general quadratic $q : A \to B\mathbb{G}_m$, $b_q(x, \cdot)$ is a character.
- If q is positive definite quadratic, the map:

$$A \to A^\vee, x \mapsto b_q(x, \cdot)$$

corresponds to the polarisation :

$$\Phi_{\mathcal{L}} : A \to A^\vee, P \mapsto t_P^* \mathcal{L} \otimes \mathcal{L}^{-1}.$$

- Conversely, if $\lambda : A \to A^\vee$ is a polarisation, the associated symmetric bilinear form is:

$$b_\lambda(x, y) = \lambda(y)(x).$$

*Here the coherence conditions matter: we want $b_q \simeq 0$ as a symmetric bilinear form. But for an abelian variety this is automatic.

Recovering a (symmetric) quadratic form from a symmetric bilinear form

- If $\mathcal{L}$ is ample, the data of b_q is equivalent to the data of the polarisation $\lambda = \Phi_{\mathcal{L}} : A \to A^\vee$ associated to $\mathcal{L}$
- Conversely, a polarisation λ is only induced by a (symmetric) ample line bundle étale locally on the base
- Indeed, we have a gerbe (banded by μ_2) of square roots of the line bundle $\mathcal{M}/A$ associated to $b(x,x)$, given by the (homotopy) pullback

$$\begin{array}{ccc} \sqrt{\mathcal{M}/A} & \longrightarrow & B\mathbb{G}_m \\ \downarrow & & \downarrow [2] \\ A & \xrightarrow{b(x,x)} & B\mathbb{G}_m \end{array}$$

  so we get an obstruction in $H^2_{fppf}(A, \mu_2)$.

- More generally, we have a fiber/cofiber sequence*

$$A^\vee \to \mathrm{Pic}_{rig}\, A \to NS(A) \to BA^\vee$$

- The fiber over $\lambda \in NS(A)$ is an $A^\vee$-torsor: its class in $H^1(k, A^\vee) = \pi_0(BA^\vee(k))$ is the obstruction to representing λ by a line bundle over k.

*Here $\mathrm{Pic}_{rig} = \mathrm{Map}_*(A, B\mathbb{G}_m)$ is the sheaf of normalised quadratic forms / rigidified line bundles on A; $A^\vee \simeq \mathrm{Pic}^0 A$, and $NS(A) = [\mathrm{Pic}_{rig}/A^\vee]$ is the sheaf of symmetric bilinear forms on A

The Poincaré line bundle

- The Poincaré line bundle $\mathcal{P}_A$ over $A \times A^\vee$ is given by the universal evaluation

$$b_{\mathcal{P}_A} : A \times A^\vee \to B\mathbb{G}_m, (x, \chi) \mapsto \chi(x)$$

- This is both a quadratic and a bilinear form on $A \times A^\vee$
- It is nondegenerate, by biduality.
- if $\lambda : A \to A^\vee$ is a polarisation,

$$b_\lambda \simeq (\mathrm{Id}_A \times \lambda)^* b_{\mathcal{P}_A} : A \times A \to B\mathbb{G}_m$$

  is the pullback of the Poincaré bilinear form.

The dual isogeny

- If $\phi : A_1 \to A_2$ is a morphism, then the dual is

$$\phi^\vee : A_2^\vee \to A_1^\vee, \chi_{A_2} \mapsto \phi^* \chi_{A_2} = P \mapsto \chi_{A_2}(\phi(P))$$

- This is also the adjoint for the Poincaré pairing: for $P \in A_1$ and $Q \in A_2^\vee$

$$b_{\mathcal{P}_{A_1}}(P, \phi^\vee Q) \simeq b_{\mathcal{P}_{A_2}}(\phi(P), Q)$$

Bilinear forms on abelian varieties

- We have a bijection between morphisms $A_1 \to A_2^\vee$ and bilinear forms $A_1 \times A_2 \to B\mathbb{G}_m$
- To $\phi : A_1 \to A_2^\vee$, using biduality, we associate:

$$b_\phi \simeq (\mathrm{Id}_{A_1} \times \phi^\vee)^* b_{\mathcal{P}_{A_1}}$$

$$b_\phi(x,y) \simeq \phi(x)(y) \simeq \phi^\vee(y)(x)$$

Homogeneous degree 2 forms

- Recall: $q : A \to B\mathbb{G}_m$ is linear iff $q(-x) \simeq -q(x)$ iff $\mathcal{L} \in \mathrm{Pic}^0(A)$.
- This corresponds to anti-symmetric line bundles $\mathcal{L}$.

- q is homogeneous of degree 2 iff $q(nx) \simeq n^2 q(x)$
- This is equivalent to $q(0) \simeq 0$ and $q(-x) \simeq q(x)$*
- This corresponds to a symmetric line bundle.
- The choice of an explicit equivalence $q(-x) \simeq q(x)$ corresponds to a choice of isomorphism $[-1]^*\mathcal{L} \simeq \mathcal{L}$
- We will always take the normalized one, i.e. that is the identity at $\mathcal{L}(0)$.

*Again, this is an extra structure, called a Σ-structure by Breen.

Pairings

- Let λ be a polarisation, and $b : A \times A \to B\mathbb{G}_m$ the associated symmetric bilinear form.
- Then b restricts to
$$b : A[n] \times A \to B\mu_n$$
because $nb(x,y) \simeq b(nx,y) \simeq b(0,y) \simeq 0$
- In particular, on k-points, taking the π_0, we get a (classical) bilinear map
$$A[n](k) \times A(k) \to H^1(k,\mu_n) \simeq k^*/k^{*,n}$$
- This is the (classical) non reduced Tate pairing $t_{n\lambda}$!

- On $A[n] \times A[n]$, we also have $nb(x,y) \simeq b(x,ny) \simeq b(x,0) \simeq 0$, so we get two different equivalences $nb(x,y) \simeq 0$.
- Comparing the two, we get a bilinear alternating* map $e_{n\lambda} : A[n] \times A[n] \to \mu_n$
- This is the (classical) Weil pairing

- Non degeneracy follows from non degeneracy of the Poincare pairing:
  - $e_{n\lambda}$ is non degenerate when $\mathrm{Ker}(\lambda) \cap A[n] = 0$
  - $t_{n\lambda} : A[n](k) \times A(k)/nA(k) \to H^1(k,\mu_n)$ is non degenerate on the right if the n-torsion is rational

*Bilinearity comes from the fact that $e_{n\lambda}$ is an automorphism of the trivial bilinear form. Furthermore, because nb is symmetric, $e_{n\lambda}$ is alternating.

Pairings and delooping

- Delooping e_n (on the second variable) gives:

$$Be_n : A[n] \times BA[n] \to B\mu_n$$

- We also have the cofiber:

$$A \xrightarrow{[n]} A \longrightarrow BA[n]$$

- We get back the Tate pairing via:

$$A[n] \times A \longrightarrow A[n] \times BA[n] \xrightarrow{Be_n} B\mu_n$$

- Since $b_{\mathcal{P}} : A \times A^\vee \to B\mathbb{G}_m$ is bilinear, we can also take its delooping in the first variable:

$$Bb : BA \times A^\vee \to B^2\mathbb{G}_m$$

- For k a nonarchimedean local field, passing to k-points and taking the π_0, we recover Tate's local pairing:

$$H^1(k, A) \times A^\vee(k) \to H^2(k, \mathbb{G}_m) \simeq \mathbb{Q}/\mathbb{Z}$$

Weil-Cartier and Tate-Cartier pairings

- Let $\phi : A_1 \to A_2^\vee$ be an isogeny of exponent n.
- The bilinear form $b_\phi : A_1 \times A_2 \to B\mathbb{G}_m$ also has two trivialisations over $A_1[\phi] \times A_2[\phi^\vee]$ via:

$$0 \simeq b(\phi(P), Q) \simeq b(P, \phi^\vee Q) \simeq 0$$

- We obtain the Weil-Cartier pairing:

$$e_\phi : A_1[\phi] \times A_2[\phi^\vee] \to \mu_n$$

as an automorphism of the trivial bilinear form over $A_1[\phi] \times A_2[\phi^\vee]$

- By delooping and using the cofiber $A_2 \xrightarrow{[\phi^\vee]} A_1^\vee \to BA_2[\phi^\vee]$, we obtain the Tate-Cartier pairing:

$$t_\phi : A_1[\phi] \times A_1^\vee \to A_1[\phi] \times BA_2[\phi^\vee] \xrightarrow{Be_\phi} B\mu_n$$

- We can also recover it via

$$t_\phi : A_1[\phi] \times A_1^\vee \to A_1[n] \times A_1^\vee \xrightarrow{b_{\mathcal{P}_{A_1}}} B\mu_n$$

- Thus the Tate-Cartier pairing gives information on the fibers of $\phi^\vee \Rightarrow$ radical isogenies
- Compatibility with isogenies directly follows from how b_ϕ is constructed.

A quadratic refinement of pairings

- For a symmetric quadratic $q : A \to B\mathbb{G}_m$, $2nq \simeq 0$ on $A[n]$, via:

$$2nq(x) \simeq nb_q(x,x) \simeq b_q(nx,x) \simeq 0$$

- Also $n^2 q \simeq 0$ on $A[n]$, via:

$$n^2 q(x) \simeq q(nx) \simeq q(0) \simeq 0$$

- It follows that $nq \simeq 0$ if n is odd.

- We obtain:

$$q : A[n] \to B\mu_{n\cdot\gcd(2,n)}$$

- In particular, passing to k-points and taking the π_0, we obtain a classical quadratic form

$$A[n](k) \to k^*/k^{*,n\cdot\gcd(n,2)}$$

- These give functorial square-root refinements of the (non reduced) self Tate pairing

$$A[n](k) \to k^*/k^{*,n}, P \mapsto t_n(P,P)$$

Polarised isogenies

- Recall that a polarised n-isogeny $\phi : (A_1, \lambda_1) \to (A_2, \lambda_2)$ between ppavs is an isogeny such that
$$\widetilde{\phi} \circ \phi = [n]$$
where $\widetilde{\phi} = \lambda_1^{-1} \circ \phi^\vee \circ \lambda_2$
- Equivalently, $\phi^* b_{\lambda_2} \simeq n b_{\lambda_1}$
- Thus a polarised n-isogeny is exactly an n-similitude

Orientations and polarisations

- An R-orientation on A is a morphism $i : R \to \mathrm{End}(A)$, i.e. an R-module structure on A.
- An R-oriented isogeny $\phi : A \to B$ is a morphism of R-modules.

- We have a dual orientation on $A^\vee$ via $i^\vee(r) = i(\bar{r})^\vee$
- If λ_A is a principal polarisation, it is R-oriented iff $i(r)^\dagger = i(\bar{r})$, equivalently for $b = b_{\lambda_A}$:

$$b(rx, y) \simeq b(x, \bar{r}y) \quad \forall r \in R$$

- So $b : A \times A \to B\mathbb{G}_m$ factors as: *

$$A \otimes_{\mathbb{Z}} A \to A \otimes_R \overline{A} \to B\mathbb{G}_m$$

where $\overline{A}$ is A given by the conjugate orientation $\bar{i}(r) = i(\bar{r})$

*Under Dold-Kan this is $A \otimes^L_R \overline{A} \to \mathbb{G}_m[1]$

Orientations, polarisations, and the module action

- If M is an (animated) R-module, a sesquilinear form $H : M \times M \to R$ is a bilinear map

$$H : M \otimes_R \overline{M} \to R$$

- We then obtain an R-oriented bilinear form on $M \otimes_R A$ via contraction*:

$$\begin{aligned} H \otimes_R b : (M \otimes_R A) \otimes_{\mathbb{Z}} (M \otimes_R A) &\to (M \otimes_R A) \otimes_R (\overline{M} \otimes_R \overline{A}) \\ &\to (M \otimes_R \overline{M}) \otimes_R (A \otimes_R \overline{A}) \to R \otimes_R (A \otimes_R \overline{A}) \\ &\to (A \otimes_R \overline{A}) \to B\mathbb{G}_m \end{aligned}$$

- So $(H \otimes_R b)(m_1 \otimes_R x_1, m_2 \otimes_R x_2) = b(H(m_1, m_2)x_1, x_2)$ is an R-oriented bilinear form
- It is symmetric when H is Hermitian.

- For M finite projective and H positive definite Hermitian, this construction preserves polarisations; if H is unimodular, it preserves principal polarisations.
- This explains how polarisation works in the covariant module action; a similar argument works for the contravariant action.

*Recall that I work in the ∞-topos, so all tensor products are derived

Theta characteristics

- If q is symmetric, i.e. $i_x : q(-x) \simeq q(x)$, $2b_q$ is alternate on $A[2] \times A[2]$ via:

$$2b_q(x,x) \simeq 4q(x) \simeq q(2x) \simeq q(0) \simeq 0$$

- Furthermore if $x \in A[2]$, $i_x : q(x) \simeq q(x)$ gives an element $e_q(x) \in \mathbb{G}_m$, hence we have

$$e_{q,*} : A[2] \to \mu_2$$

  a classical quadratic form whose associated symmetric bilinear form is $e_{2q} : A[2] \times A[2] \to \mu_2$:

$$e_{q,*}(x+y) = e_{q,*}(x)e_{q,*}(y)e_{2q}(x,y)$$

- This is precisely the theta characteristic associated to $\mathcal{L}$

Table of Contents

1 Introduction

2 What are bilinear and quadratic forms, actually?

3 Bilinear and quadratic forms on abelian varieties

4 Arithmetic structures on geometric objects from bilinear and quadratic forms

5 Algorithmic applications

The arithmetic structure associated to a linear form

- Let U be a commutative group scheme, $\mathcal{L}/U$ a line bundle, $X_{\mathcal{L}}$ the associated torsor, and $q : U \to B\mathbb{G}_m$ the corresponding map. Assume that q is quadratic.
- Assume furthermore that $\gamma : b_q \simeq 0$ as a bilinear form.
- Then $X_{\mathcal{L}}$ is a group, an extension of U by $\mathbb{G}_m$
- Indeed, the choice of an equivalence $b_q \simeq 0$ gives $q(x+y) \simeq q(x) + q(y)$ which gives a multiplication law:
$$\mathcal{L}_x \otimes \mathcal{L}_y \to \mathcal{L}_{x+y}.$$
- Warning ❦: It is not commutative in general, commutativity defect is given by the commutator pairing
$$e_{\mathcal{L}} : U \times U \to \mathbb{G}_m$$

- $\gamma : b_q \simeq 0$ as a symmetric bilinear form iff the group structure is commutative
- Then q is a linear form[*]:
$$q \in \mathcal{H}om_{\mathbb{Z}}(U, B\mathbb{G}_m)$$
- Taking π_0[**], we obtain an element in $\mathcal{E}xt^1(U, \mathbb{G}_m)$, as expected.

[*] In the previous situation it was just an E_1-form

[**] Using that under the Dold-Kan isomorphism, $B\mathbb{G}_m$ corresponds to $\mathbb{G}_m[1]$

The theta group

- Let $\mathcal{L}_0$ be an ample principal line bundle on A, with associated map $q_0 : A \to B\mathbb{G}_m$ and bilinear map b_0
- Then $\mathcal{L} = \mathcal{L}_0^{\otimes n}$ is associated with $q = nq_0$ and $b = nb_0$, and as we saw, b is trivial over $A[n] \times A$ *
- It follows that $G(\mathcal{L}) = X_{\mathcal{L}} \mid A[n]$ is a group: the theta group.
- Since b is trivial over $A[n] \times A$, we even get an action of the theta group $G(\mathcal{L})$ on $X_{\mathcal{L}}$.

- N.B.: the theta group $G(\mathcal{L})$ is commutative if $\mathcal{L} \in \mathrm{Pic}^0 A$. If $\mathcal{L}$ is ample of level > 1, $G(\mathcal{L})$ is never commutative

*With a unique trivialisation given by the rigidity of A and our implicit choice of rigidification $q(0) \simeq 0$

Theta structures and theta functions

- Let $\mathcal{L} = \mathcal{L}_0^{\otimes n}$ of level n as above, with $\mathcal{L}_0$ symmetric and rigidified, and n even, so $q = nq_0$
- Recall that q_0 gives $A[n] \to B\mu_{2n}$, so we get $q : A[n] \to B\mu_2$
- A symmetric theta structure is:
  - A choice of symplectic basis (e_i, f_i) for $(A[n], e_{\mathcal{L}})$
  - A choice of trivialisation $\tilde{x} : q(x) \simeq *$ of μ_2-torsors for each x in this symplectic basis
- Equivalently, this is the same as a choice of (symmetric) quadratic trivialisation $q \mid \langle x \rangle \simeq *$ for each x in this symplectic basis
- Or to an isomorphism between $G(\mathcal{L})$ and the Heisenberg group, compatible with the canonical involutions.
- Warning ❦: this does not give a global trivialisation of $q : A[n] \to B\mu_2$ as a quadratic form.*

*On the other hand if n is odd, we have $q_0 : A[n] \to B\mu_n$ so q admits a canonical quadratic trivialisation over $A[n]$. A symmetric theta structure in odd level is determined uniquely by the symplectic basis.

Theta structures and theta functions

- Given a symmetric theta structure, the associated theta coordinates are given by the unique (up to equivalence) map $A \to [\mathbb{A}^{n^g}/\mathbb{G}_m]$ above q such that the action on $\mathbb{A}^{n^g}$ of the $\tilde{x}$ above is given by the Heisenberg matrices:

$$\begin{array}{ccc} G(\mathcal{L}) \curvearrowright X_{\mathcal{L}} & \longrightarrow & G(\mathcal{L}) \curvearrowright \mathbb{A}^{n^g} \\ \downarrow & & \downarrow \\ A[n] \curvearrowright A = (G(\mathcal{L}) \curvearrowright X_{\mathcal{L}})/\mathbb{G}_m & \longrightarrow & A[n] \curvearrowright [\mathbb{A}^{n^g}/\mathbb{G}_m] \end{array}$$

- Recall Sabrina's talk this Monday for the Heisenberg matrices!

Isogenies and descent

- Let $\mathcal{L}$ be an ample line bundle on A_1 with associated quadratic form q, and $\phi : A_1 \to A_2 = A_1/K$ an isogeny with kernel K.
- Then a descent of $\mathcal{L}$ to a line bundle $\mathcal{M}$ on B is given by:
  - A trivialisation $b_q \simeq 0$ over $K \times A_1$
  - A trivialisation $q \simeq 0$ over K
  - Such that they both induce the same trivialisation $b_q \simeq 0$ over $K \times K$
- Geometrically, this corresponds to a group lift $\widetilde{K}$ of K in the theta group $G(\mathcal{L})$
- This gives an explicit equivalence $q_{A_1} \simeq q_{A_2} \circ \phi$, canonically determined by choices of rigidification of q_{A_1}, q_{A_2} at 0.

- A section $U \in \Gamma(A_1, \mathcal{L})$ descends to $V \in \Gamma(A_2, \mathcal{M})$, iff U seen as a map $A_1 \to [\mathbb{A}^1/\mathbb{G}_m]$ above q_{A_1} factors through A_2:

$$\begin{array}{ccc} A_1 & \xrightarrow{U} & [\mathbb{A}^1/\mathbb{G}_m] \\ \downarrow{\scriptstyle \phi} & \overset{V}{\nearrow} & \downarrow \\ A_2 = [A_1/K] & \xrightarrow{q_{A_2}} & B\mathbb{G}_m \end{array}$$

- Geometrically, this means that U is invariant under the action of $\widetilde{K}$

Cubical isogenies

- We have $X_{\mathcal{M}} = [X_{\mathcal{L}}/\widetilde{K}]$
- The isogeny ϕ lifts uniquely to a cubical isogeny $\widetilde{\phi} : X_{\mathcal{L}} \to X_{\mathcal{M}}$
- To a cubical point $\widetilde{P} : q_A(P) \simeq 0$ on A, we associate the cubical point $\widetilde{\phi(P)} : q_B(\phi(P)) \simeq 0$ via the equivalence $q_B \circ \phi \simeq q_A$

Biextensions: the arithmetic structure associated to a bilinear form

- Let $b : A_1 \times A_2 \to B\mathbb{G}_m$ be a bilinear form and $X_b \to A_1 \times A_2$ the associated torsor.
- Then for each $P \in A_1$, $b(P, \cdot)$ is linear so we get a group structure on the slice $X_{P \times A_2}$:

$$g_{P,Q_1} \star_2 g_{P,Q_2}$$

- Likewise, for each $Q \in A_2$, $b(\cdot, Q)$ is linear, and we get a group structure on the slice $X_{A_1 \times Q}$:

$$g_{P_1,Q} \star_1 g_{P_2,Q}$$

- Moreover these two group structures are compatible with each other.

$$(g_{P_1,Q_1} \star_2 g_{P_1,Q_2}) \star_1 (g_{P_2,Q_1} \star_2 g_{P_2,Q_2}) = (g_{P_1,Q_1} \star_1 g_{P_2,Q_1}) \star_2 (g_{P_1,Q_2} \star_1 g_{P_2,Q_2})$$

- If $b : A \times A \to B\mathbb{G}_m$ is symmetric, we also have a canonical involution $i(g_{P,Q}) = g_{Q,P}$ compatible with the biextension laws.

Example: The Poincaré biextension on an elliptic curve

$\mathcal{Y}$ the biextension associated to (0_E) above $E \times E$:

- An element $g_{P,Q}$ of $\mathcal{Y}$ above $(P, Q) \in E \times E$ is a function with divisor

$$(P + Q) + (0_E) - (P) - (Q)$$

- Biextension law:

$$\begin{aligned} g_{P_1,Q} \star_1 g_{P_2,Q} = g_{P_1+P_2,Q} &:= g_{P_1,Q}(\cdot) g_{P_2,Q}(\cdot - P_1) \\ &= g_{P_1,Q}(\cdot) g_{P_2,Q}(\cdot) \frac{g_{P_1,P_2}(\cdot - Q)}{g_{P_1,P_2}(\cdot)} \end{aligned}$$

Pairings via biextensions

- If $P = 0_E$ or $Q = 0_E$, $(P+Q) + (0_E) - (P) - (Q) = 0$, so a biextension element $g_{0_E,Q}$ or $g_{P,0_E}$ is a constant function on E.
- If $P \in E[n](\mathbb{F}_q)$ and $Q \in E(\mathbb{F}_q)$, the function $g_{nP,Q} = g_{P,Q}^{\star_1,n}$ is a constant $t \in \mathbb{F}_q^*$.
- Changing $g_{P,Q}$ by $\lambda g_{P,Q}$ changes t by $t\lambda^n$, so t is well defined in $\mathbb{F}_q^*/\mathbb{F}_q^{*,n}$.
- This is the Tate pairing!
  Proof: Recall that the Tate pairing $t_n(P,Q) \in B\mu_n(k)$, is given by the restriction $b : E[n] \times E \to B\mu_n$. Given $g_{P,Q} : b(P,Q) \simeq_{\mathbb{G}_m(k)} *$, the biextension arithmetic allows to compute $t : nb(P,Q) \simeq b(nP,Q) \simeq *$ and the μ_n-torsor is given by $\{x^n = t\}$

- Likewise, the Weil pairing is given by

$$e_n(P,Q) = \frac{g_{P,Q}^{\star_1,n}}{g_{P,Q}^{\star_2,n}}$$

for $P, Q \in E[n]$.

Cubical points

- If $\mathcal{L}$ is base point free (e.g. very ample), and $X_0, \dots X_N \in \Gamma(A, \mathcal{L})$ is a basis of sections, recall the commutative diagram

$$\begin{array}{ccc} X_{\mathcal{L}} & \longrightarrow & \mathbb{A}^{N+1} \setminus \{(0,\dots,0)\} \\ \downarrow & & \downarrow \\ A & \longrightarrow & \mathbb{P}^N \end{array}$$

- Given $P \in A$, a cubical point $\widetilde{P}$ is an element $\widetilde{P} \in X_{\mathcal{L}}$ above P via the projection $X_{\mathcal{L}} \to A$
- All other cubical points above P are of the form $\lambda\widetilde{P}$ for $\lambda \in \mathbb{G}_m$ ($X_{\mathcal{L}}$ is a $\mathbb{G}_m$-torsor)
- The coordinates X_i extend to cubical points via $X_i(\widetilde{P}) = \widetilde{P}(X_i(P))$
- The image in $\mathbb{P}^N$ of $P \in A$ is given by projective coordinates:

$$(X_0(P) : X_1(P) : \cdots : X_N(P)) \in \mathbb{P}^N$$

- A choice of cubical point $\widetilde{P}$ above P is a choice of lift of projective coordinates to affine coordinates:

$$(X_0(\widetilde{P}), X_1(\widetilde{P}), \dots, X_N(\widetilde{P})) \in \mathbb{A}^{N+1} \setminus \{(0,\dots,0)\}$$

- If $q_{\mathcal{L}} : A \to B\mathbb{G}_m$ is the associated quadratic form, the choice of $\widetilde{P}$ is a choice of equivalence: $\widetilde{P} : q(P) \simeq *$

Examples: cubical points on an elliptic curve

- $D = (0_E)$: level-1 coordinate Z_1
- $D = 2(0_E)$: level-2 coordinates $X_2, Z_2 = Z_1^2$
- $D = 3(0_E)$: level-3 coordinates $X_3 = X_2 Z_1, Y_3, Z_3 = Z_1^3$
- Weierstrass coordinates: $x = X_3/Z_3 = X_2/Z_2, y = Y_3/Z_3$.
  $P \in E$ is determined by $(x(P), y(P))$.

- A level 3 cubical point $\widetilde{P}$ is a choice of $(X_3(\widetilde{P}), Y_3(\widetilde{P}), Z_3(\widetilde{P}))$ above $(X_3(P) : Y_3(P) : Z_3(P))$.
  N.B: $D = 3(0_E)$ is very ample. Example: fix $\widetilde{O} = (0, 1, 0)$.

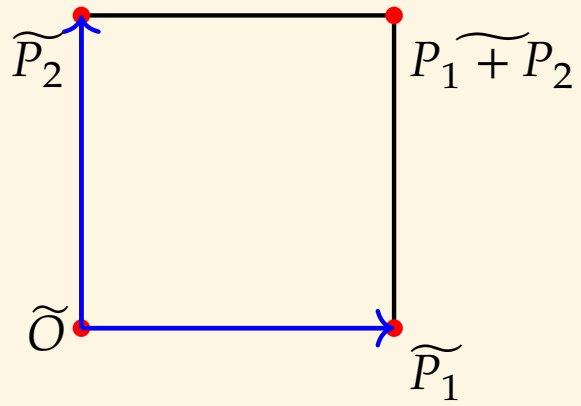
- A level 2 cubical point $\widetilde{P}$ is a choice of $(X_2(\widetilde{P}), Z_2(\widetilde{P}))$ above $(X_2(P) : Z_2(P))$.
  N.B: $D = 2(0_E)$ is base point free. Example: fix $\widetilde{O} = (1, 0)$.

- A level 1 cubical point $\widetilde{P}$ is a choice of $Z_1(\widetilde{P})$.
  N.B: 0_E is a base point of $D = (0_E)$, so we define $\tilde{0}_E$ by (for instance) $\frac{Z_1}{x/y}(\tilde{0}_E) = 1$.

Cubical arithmetic: the degenerate case

- Let $\mathcal{L}$ be a line bundle on A, $q : A \to B\mathbb{G}_m$ the associated quadratic form.
- Assume that q is linear, i.e. $b_q \simeq 0$ (i.e. $\mathcal{L}$ is algebraically equivalent to 0; if D is a divisor on E, this is equivalent to $\deg D = 0$)
- We saw $X_{\mathcal{L}}$ is a commutative group, an extension of A by $\mathbb{G}_m$

- Reformulation: we have a square structure on $X_{\mathcal{L}}$



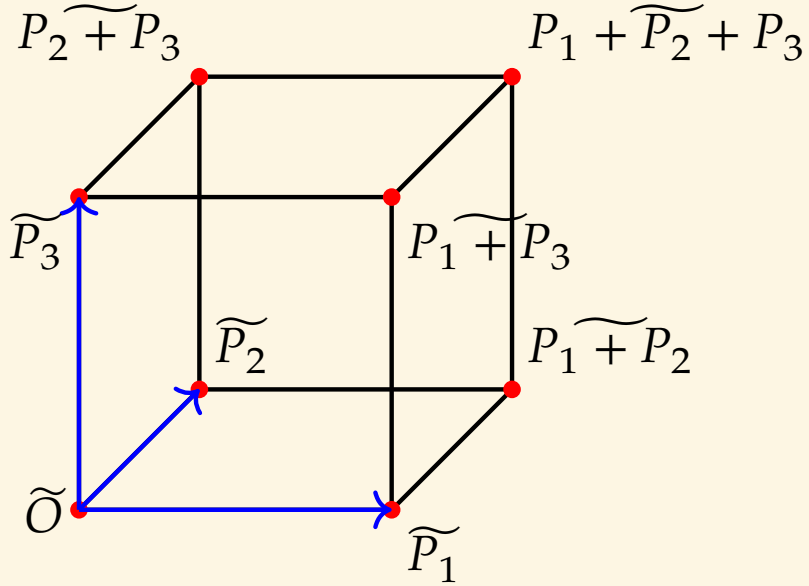
- $\widetilde{P_1 + P_2}$ is uniquely determined by $\widetilde{P_1}, \widetilde{P_2}$ (and $\widetilde{O}$)
- The square structure also determines $-\widetilde{P}$

Corollary

Given $\widetilde{P}_i$ the cubical point $\sum n_i \widetilde{P}_i$ is uniquely determined for all $n_i \in \mathbb{Z}$

Cubical arithmetic: the general case

- We want to work with $\mathcal{L}$ ample and symmetric
- We don't have a group / a square structure anymore
- But we do have a symmetric cubical structure!



- $P_1 + \widetilde{P_2} + P_3$ is uniquely determined by $\widetilde{P_1}, \widetilde{P_2}, \widetilde{P_3}, \widetilde{P_1 + P_2}, \widetilde{P_1 + P_3}, \widetilde{P_2 + P_3}$ (and $\widetilde{O}$)

Corollary

Given $\widetilde{P_i}$ and $\widetilde{P_i + P_j}$ for $i < j$, the cubical point $\sum n_i \widetilde{P_i}$ is uniquely determined for all $n_i \in \mathbb{Z}$.

Without symmetry, the cubical structure does not determine $-\widetilde{P}$ anymore nor $2\widetilde{P}$ from $\widetilde{P}$. However, given $\widetilde{P_i}$ and $\widetilde{P_i + P_j}$ for $i \leq j$, the cubical point $\sum n_i \widetilde{P_i}$ is still uniquely determined for all $n_i \in \mathbb{N}$.

Formulas 1

- Cubical arithmetic arises from a canonical isomorphism:

$$\mathcal{L}_{P_1+P_2+P_3} \otimes \mathcal{L}_{P_1} \otimes \mathcal{L}_{P_2} \otimes \mathcal{L}_{P_3} \simeq \mathcal{L}_0 \otimes \mathcal{L}_{P_2+P_3} \otimes \mathcal{L}_{P_1+P_3} \otimes \mathcal{L}_{P_1+P_2}$$

- Given $Z \in \Gamma(A, \mathcal{L})$ with associated divisor D, the isomorphism comes from a function cub_D:

$$\frac{Z(P_1 + \widetilde{P_2} + P_3) \cdot Z(\widetilde{P_1}) \cdot Z(\widetilde{P_2}) \cdot Z(\widetilde{P_3})}{Z(\widetilde{O}) \cdot Z(P_2 \widetilde{+} P_3) \cdot Z(P_1 \widetilde{+} P_3) \cdot Z(P_1 \widetilde{+} P_2)} = \mathrm{cub}_D(P_1, P_2, P_3)$$

Proposition

- *Neutrality:* $\mathrm{cub}_D(0_A, 0_A, 0_A) = 1$.
- *Commutativity:* $\mathrm{cub}_D(\sigma(P_1, P_2, P_3)) = \mathrm{cub}_D(P_1, P_2, P_3)$ *for all* $\sigma \in \mathfrak{S}_3$.
- *Associativity:*

$$\mathrm{cub}_D(P_1 + P_2, P_3, P_4) \cdot \mathrm{cub}_D(P_1, P_2, P_4) = \mathrm{cub}_D(P_1, P_2 + P_3, P_4) \cdot \mathrm{cub}_D(P_2, P_3, P_4).$$

- *For a Σ-cubical structure, assuming D symmetric.*
  Symmetry: $\mathrm{cub}_D(P_1, P_2, -P_1 - P_2) = \pm 1$ *(according to whether Z is symmetric or antisymmetric).*

- Associativity means that the cubical point $\sum n_i \widetilde{P}_i$ does not depend on the choices of cubes used to compute it
- N.B.: Z^m is a section of mD, and $\mathrm{cub}_{mD} = \mathrm{cub}_D^m$: cubical arithmetic of level n induces the cubical arithmetic of level nm.

Formulas 2

Theorem

$$\mathrm{cub}_D(P_1, P_2, P_3) = \frac{g_{D,P_1,P_2}(P_3)}{g_{D,P_1,P_2}(0_A)}$$

where g_{D,P_1,P_2} *is any function with divisor* $t^*_{P_1+P_2}D + D - t^*_{P_1}D - t^*_{P_2}D$.

Proposition

If we take g_{D,P_1,P_2} *normalised at* 0_A, *then*

- *Neutrality:* $g_{D,P_1,P_2}(0_A) = 1$.
- *Commutativity:* $g_{D,P_1,P_2}(P_3) = g_{D,P_2,P_3}(P_1) = g_{D,P_3,P_1}(P_2)$
- *Associativity:* $g_{D,P_1+P_2,P_3}g_{D,P_1,P_2} = g_{D,P_1,P_2+P_3}g_{D,P_2,P_3}$
- *For a* Σ*-cubical structure: (Anti)-symmetry:* $g_{D,P_1,P_2}(-P_1 - P_2) = \pm 1$.

Cubical arithmetic on elliptic curves $y^2 = x^3 + a_2x^2 + a_4x + a_6$

$$\mathrm{cub}_{(0_E)}(P_1,P_2,P_3) = \frac{\begin{vmatrix} 1 & x(P_1) & y(P_1) \\ 1 & x(P_2) & y(P_2) \\ 1 & x(P_3) & y(P_3) \end{vmatrix}}{(x(P_2)-x(P_1))(x(P_3)-x(P_1))(x(P_3)-x(P_2))}$$
$$= \frac{l_{P_1,P_2}(P_3)}{(x(P_3)-x(P_1))(x(P_3)-x(P_2))} = \frac{x(P_1+P_2)-x(P_3)}{l_{P_1,P_2}(-P_3)}$$

- Differential addition: $Z_1(\widetilde{P+Q})Z_1(\widetilde{P-Q}) = Z_1(\widetilde{P})^2 Z_1(\widetilde{Q})^2 (x(Q)-x(P))$
- Doubling: $Z_1(2\widetilde{P}) = Z_1(\widetilde{P})^4 2y(P)$
- Inverse: $Z_1(-\widetilde{P}) = -Z_1(\widetilde{P})$.

Proposition

Level 2 cubical arithmetic descends to the Kummer line.

Example (Montgomery model in level 2: $y^2 = x^3 + \mathcal{A}x^2 + x$)

- $Z(2\widetilde{P}) = 4X(\widetilde{P})Z(\widetilde{P})(X(\widetilde{P})^2 + \mathcal{A}X(\widetilde{P})Z(\widetilde{P}) + Z(\widetilde{P})^2)$
- $Z(\widetilde{P+Q})Z(\widetilde{P-Q}) = \left(X(\widetilde{Q})Z(\widetilde{P}) - X(\widetilde{P})Z(\widetilde{Q})\right)^2$

Computing pairings via cubical arithmetic

$$\begin{array}{llll}
\tilde{0}_A & \widetilde{P} & \widetilde{2P} & \ldots \quad \widetilde{nP} = \lambda_P^0 \tilde{0}_A \\
\widetilde{Q} & \widetilde{P+Q} & \widetilde{2P+Q} & \ldots \quad \widetilde{nP+Q} = \lambda_P^1 \widetilde{Q} \\
\widetilde{2Q} & \widetilde{P+2Q} & & \\
\ldots & \ldots & & \\
\widetilde{nQ} = \lambda_Q^0 \tilde{0}_A & \widetilde{P+nQ} = \lambda_Q^1 \widetilde{P} & &
\end{array}$$

For $P, Q \in A[n]$, $\mathcal{L}$ ample on A, $Z \in \Gamma(\mathcal{L})$:

$$e_{\mathcal{L}^{\otimes n}}(P,Q) = \frac{\lambda_P^1 \lambda_Q^0}{\lambda_Q^1 \lambda_P^0} = \frac{Z(\widetilde{nP+Q}) Z(\widetilde{nP})}{Z(\widetilde{nQ}) Z(\widetilde{Q+nP})}$$

Caveats

- In level 2 (X, Z)-cubical coordinates, cubical exponentiation $\ell \mapsto \ell\widetilde{P}$ can be computed via a Montgomery style ladder, using cubical doublings and cubical differential additions.
- Very similar to $x = (X : Z)$-only arithmetic

- We can have $\ell\widetilde{P} = \tilde{0}_E$ but $(\ell + 1)\widetilde{P} \neq \widetilde{P}$
- However, $\ell\widetilde{P} = \tilde{0}_E$ and $(\ell + 1)\widetilde{P} = \widetilde{P}$ implies $(m\ell + n)\widetilde{P} = n\widetilde{P}$ for all m, n.

- x-only arithmetic does not depend on the quadratic twist $By^2 = x^3 + a_2x^2 + a_4x + a_6$
- But (X, Z)-level 2 cubical arithmetic does depend on the twist!

Table of Contents

1 Introduction

2 What are bilinear and quadratic forms, actually?

3 Bilinear and quadratic forms on abelian varieties

4 Arithmetic structures on geometric objects from bilinear and quadratic forms

5 Algorithmic applications

Algorithmic applications

Given a model of an abelian variety $(A, \mathcal{L})$ with explicit formulas for the cubical arithmetic on $X_{\mathcal{L}}$, we have algorithms for:

- Computing the pairings $e_{\mathcal{L},\ell}$ (and variants)
  [Pope, Reijnders, R., Sferlazza, Smith 2025], [Lin, R., Zhao, Zheng 2025]
- Computing (polarised) isogenies $\phi : (A, \mathcal{L}^\ell) \to (B, \mathcal{M})$
  Work in progress with [Corte-Real De Santos, Dartois, Pope, Smith] for speeding up odd-degree isogenies
- Computing radical isogenies
  Work in progress with [Kunzweiler, Houben, Pope]
- Computing isogeny preimages, and cubical isogenies
- Computing functions with prescribed principal divisors
- Changing level

- N.B.: formulas for cubical arithmetic can be derived from sufficiently explicit formulas for the theorem of the square. In particular we have explicit formulas in the theta models (of even levels).
- Unfortunately a lot of this is still unpublished, but see also [R. 2024]

A toolbox: Excellent lifts

- Let $q = nq_0 : A \to B\mathbb{G}_m$ quadratic symmetric of odd level n, corresponding to a symmetric $\mathcal{L} = \mathcal{L}_0^n$ and associated torsor $X_{\mathcal{L}} \to A$
- Recall that q_0 induces $q_0 : A[n] \to B\mu_n$
- If $P \in A[n]$, an excellent lift is $\widetilde{P} \in X_{\mathcal{L}_0} : q_0(P) \simeq *$ a rigidification of μ_n-torsor

- Equivalently: $(a + bn)\widetilde{P} = a\widetilde{P}$ for all $a, b \in \mathbb{Z}$

$\Rightarrow$ Can be efficiently computed via cubical ladders*

- Then $\widetilde{P}^{\otimes n} \in X_{\mathcal{L}} : q(P) \simeq nq_0(P) \simeq 0$ is independent of $\widetilde{P}$ and gives the unique symmetric lift $g_P \in G(\mathcal{L})$ of P with $g_P^n = 1$.

- This gives an efficient way to compute the theta group arithmetic (and its action) in level n while working in level 1
- A similar strategy works for even n via $q_0 : A[n] \to B\mu_{2n}$

*The cubical ladder gives the μ_n-torsor as $\{x^n = c\}$, an excellent lift is then given by a choice of n-th root of c.

The Discrete Logarithm Problem

- Let $P \in E(\mathbb{F}_q)[n], Q = sP, n$ odd.

- Assume $\mu_n(\mathbb{F}_q) = 1$
- Then any μ_n-torsor has a unique $\mathbb{F}_q$-rational trivialisation
- This means that P, Q have unique $\mathbb{F}_q$-rational excellent lifts $\widetilde{P}, \widetilde{Q}$

- In fact we have a trivialisation $q_0 \mid E[n](\mathbb{F}_q) \simeq 0$ by taking the rational n-th root of the global trivialisation $q \mid E[n] \simeq 0$
- Thus the DLP lifts to $\widetilde{Q} = s\widetilde{P}$

$\Rightarrow$ Monodromy leak

- Leaking the result $(X(sP), Z(sP))$ of a Montgomery ladder $x(P) \mapsto x(sP)$ on a Montgomery curve is enough to recover s via a DLP and square root in $\mathbb{F}_q^*$
- See `https://jonathke.github.io/monoDOOM`

Perspectives

- Work out efficient arithmetic of the non symmetric biextension $X_\phi \to A_1 \times A_2$ associated to the bilinear form $b_\phi : A_1 \times A_2 \to B\mathbb{G}_m$ given by a polarized isogeny $\phi : (A_1, \lambda_1) \to (A_2, \lambda_2)$:

$$\begin{array}{ccccc} X_{\lambda_1} & \longleftarrow & X_\phi & \longrightarrow & X_{\lambda_2} \\ \downarrow & & \downarrow & & \downarrow \\ A_1 \times A_1 & \xleftarrow{\mathrm{Id}_{A_1} \times \widetilde{\phi}} & A_1 \times A_2 & \xrightarrow{\phi \times \mathrm{Id}_{A_2}} & A_2 \times A_2 \end{array}$$

  where the pullbacks are induced by factoring $b_\phi : A_1 \times A_2 \to B\mathbb{G}_m$ via:

$$\begin{array}{ccc} A_1 \times A_2 & \xrightarrow{\mathrm{Id}_{A_1} \times \widetilde{\phi}} & A_1 \times A_1 \\ {\scriptstyle \phi \times \mathrm{Id}_{A_2}} \downarrow & & \downarrow {\scriptstyle b_{\lambda_1}} \\ A_2 \times A_2 & \xrightarrow{b_{\lambda_2}} & B\mathbb{G}_m \end{array}$$

- Cryptographic applications of cubical isogenies? (e.g. sending the image of a cubical point?)
- Work out a theory of quadratic forms associated to sesquilinear/Hermitian biextensions, i.e. Hermitian forms with values in $B\mathbb{G}_m \otimes R$ (see work by [Stange] on this topic)
- Develop a theory of theta functions of level $1 + i$ for MIKE.