Animating quadratic and bilinear forms on abelian varieties

2025/12/16 — Canari Seminar

Damien Robert

Équipe Canari, Inria Bordeaux Sud-Ouest

Table of Contents

Linear and quadratic maps

X, Y, Z abelian groups

- An affine map $\phi : X \to Z$ is a map of degree ≤ 1:

$$\phi(x+y) - \phi(x) - \phi(y) + \phi(0) = 0 \quad \forall x, y \in X.$$

- A quadratic map $\phi : X \to Z$ is a map of degree ≤ 2:

$$\phi(x+y+z) - \phi(y+z) - \phi(x+z) - \phi(x+y) + \phi(x) + \phi(y) + \phi(z) - \phi(0) = 0 \quad \forall x, y, z \in X.$$

- More generally a map $\phi : X \to Z$ is of degree $\leq n$ if $\Theta_{n+1}(\phi) : X^{n+1} \to Z$ is zero for an appropriate Θ_{n+1}.

- If q is quadratic, $q = q_0 + q_1 + q_2$ where $q_0 = q(0)$ and q_i is homogeneous of degree i:

$$q_i(nx) = n^i q_i(x).$$

- By translating, we may assume that ϕ is normalised: $\phi(0) = 0$.
- For instance, ϕ is normalised of degree 1 iff it is linear.

Bilinear maps

- $b : X \times Y \to Z$ is bilinear if $b(x, \cdot)$ and $b(\cdot, y)$ are linear for all $x \in X, y \in Y$.
- Equivalently $\Theta_{2,2}(b) = 0$ for an appropriate $\Theta_{2,2} : X^2 \times Y^2 \to Z$.
- b is induced by a linear map $X \otimes_{\mathbb{Z}} Y \to Z$ via the composition $X \times Y \to X \otimes_{\mathbb{Z}} Y \to Z$.
- A bilinear map $b : X \times X \to Z$ is symmetric if $b(x,y) = b(y,x) \quad \forall x, y \in X$.

- If $q : X \to Z$ is quadratic, we can associate a symmetric bilinear form $b_q : X \times X \to Z$ via

$$b_q(x,y) := \Theta_2 q(x,y) = q(x+y) + q(0) - q(x) - q(y).$$

- In fact, q is quadratic iff b_q is bilinear.
  And more generally $\phi : X \to Z$ is of degree $\leq n$ iff $\Theta_n(\phi) : X^n \to Z$ is n-multilinear.
- Conversely, given a bilinear $b : X \times X \to Z$, we can associate a quadratic form $q_b : X \to Z, q_b(x) = b(x,x)$.
- These are not inverse of each other!
- $b \to q \to b'$ gives the symmetrisation of b:

$$b'(x,y) = b(x,y) + b(y,x)$$

- $q \to b \to q'$ gives $q' = 2q_2$, where q_2 is the homogeneous degree 2 part of q
- Even if we restrict to homogeneous normalised q, there will be trouble if 2 is not inversible …

Abelian varieties

If A/k is an abelian variety, there seems to exists a strong analogy between:

- Polarisations $\Phi : A \to \hat{A}$ and symmetric bilinear morphisms $A \times A \to \mathbb{G}_m$
- Line bundles $\mathcal{L} \in \mathrm{Pic}(A)$ over A and quadratic maps $A \to \mathbb{G}_m$
- Furthermore, $\mathcal{L} \in \widehat{A} = \mathrm{Pic}^0(A)$ "corresponds" to a linear morphisms $A \to \mathbb{G}_m$.
- More generally a morphism $A \to \hat{B}$ "corresponds" to a bilinear map $A \times B \to \mathbb{G}_m$.

A slight subtlety is that seeing $\mathcal{L}$ in $\mathrm{Pic}(A)$ means we work up to isomorphism, in the analogy this corresponds to working with q up to translation.

One can fix the isomorphism class of $\mathcal{L}$ by rigidifying it at 0_A; this corresponds to normalising q.

Duality

- Define the dual of X as $\widehat{X} = \mathrm{Hom}(X, Z)$, then by definition an element $Q \in \widehat{X}$ is a linear map $X \to Z$.
- A bilinear map $b : X \times X \to Z$ is the same thing as a linear map $\Phi_b : X \to \widehat{X}$, via

$$\Phi_b(x) = b(x, \cdot), \quad b(x_1, x_2) = \Phi_b(x_1)(x_2).$$

  Φ_b is the polarisation associated to b.
- Assume that X is isomorphic to its bidual, via the natural map $i : X \to \widehat{\widehat{X}}, i(x) : \psi \mapsto \psi(x)$. Then b is symmetric iff Φ_b is symmetric: $\Phi_b^\vee : X \simeq \widehat{\widehat{X}} \to \widehat{X}$ is equal to Φ_b.
- If $q : X \to Z$ is quadratic, its associated bilinear form b_q corresponds to

$$\Phi_q : X \to \widehat{X}, x \mapsto t_x^* q - q + [q(0) - q(x)]$$

  where $t_x^* q : y \mapsto q(x + y)$.

- An abelian variety A is bidual, and a morphism $\Phi : A \to \hat{A}$ is a polarisation precisely when it is symmetric.
- If $\mathcal{L}$ is a line bundle on A, the associated polarisation is $\Phi_{\mathcal{L}} : A \to \widehat{A}, P \mapsto t_P^* \mathcal{L} \otimes \mathcal{L}^{-1}$.

Morphisms

- A bilinear form $b : X \times Y \to Z$ induces linear maps $\phi_{X,b} : X \to Y^\vee, x \mapsto b(x, \cdot)$ and $\phi_{Y,b} : Y \to X^\vee, y \mapsto b(\cdot, y)$.
- By biduality, $\phi_{Y,b} : Y \to X^\vee$ is the dual of $\phi_{X,b} : X \to Y^\vee$.

- Canonical bilinear form:

$$b_X : X \times X^\vee \to Z, (x, \psi) \mapsto \psi(x).$$

- We can recover b from $\phi_{Y,b}$ or $\phi_{X,b}$ via

$$b = (\mathrm{Id} \times \phi^*_{Y,b}) b_X = (\phi_{X,b} \times \mathrm{Id})^* b_Y.$$

- $\mathrm{Bilinear}(X \times Y, Z) \simeq \mathrm{Hom}(X, Y^\vee) \simeq \mathrm{Hom}(Y, X^\vee)$
- Via this bijection, b_X is the bilinear map $X \times X^\vee \to Z$ associated to $\mathrm{Id} : X \to X$.

- A morphism $\phi : A \to B^\vee$ corresponds by duality to a morphism $\phi^\vee : B \to A^\vee$.
- This should give a "bilinear structure" on $A \times B$:

$$\mathrm{Hom}(A, B^\vee) \simeq \mathrm{Hom}(B, A^\vee) = ?$$

- We do have the Weil-Cartier pairing:

$$e_\phi : \mathrm{Ker}\,\phi \times \mathrm{Ker}\,\phi^\vee \to \mathbb{G}_m.$$

Poincaré polarisation

- The bilinear map b_X induces a canonical "universal" quadratic form on $X \times X^\vee$:

$$q_P(x,\psi) = \psi(x).$$

  In particular, $\psi \in X^\vee$ is recovered as $\psi = q_P \mid X \times \{\psi\}$
- Associated bilinear form b_P:

$$b_P((x_1,\psi_1),(x_2,\psi_2)) = \psi_1(x_2) + \psi_2(x_1)$$

- Polarisation: $\Phi_P : X \times X^\vee \to X^\vee \times X, (x,\psi) \mapsto (\psi, x)$ via the biduality $X \simeq \widehat{\widehat{X}}$.
- If $b : X \times X \to Z$ bilinear form associated to a polarisation $\Phi_b : X \to \widehat{X}$, then $q_b = (\mathrm{Id} \times \Phi_b)^* q_P$ and $b(x,y) + b(y,x) = (\mathrm{Id} \times \Phi_b)^* b_P$.

- Symmetric Poincaré line bundle P on $A \times \widehat{A}$ (birigidified at 0), given by applying the universal property of $\widehat{A}$ to $\mathrm{Id} : \widehat{A} \to \widehat{A}$.
- Associated polarisation

$$\Phi_P : A \times \widehat{A} \to \widehat{A} \times A, (P,Q) \mapsto (Q,P)$$

  .
- If $\mathcal{L} \in \mathrm{Pic}^0(A)$, $\mathcal{L} = P \mid A \times \{\mathcal{L}\}$.
- If $\Phi : A \to \widehat{A}$ is a polarisation, we get a symmetric line bundle on A via $\mathcal{L}' = (\mathrm{Id} \times \Phi)^* P$.
- If $\Phi = \Phi_{\mathcal{L}}$ for a symmetric $\mathcal{L}$, then $\mathcal{L}' = \mathcal{L}^{\otimes 2}$.
  (Recall that if q is symmetric, $q' = 2q$.)

Linear maps and (anti)symmetric line bundles

- A quadratic form $q : X \to Z$ is of degree ≤ 1 iff $b_q = 0$ iff $\Phi_q = 0$
- A line bundle $\mathcal{L} \in \mathrm{Pic}(A)$ is algebraically equivalent to 0, i.e. belongs to $\mathrm{Pic}^0(A)$ iff $\Phi_{\mathcal{L}} = 0$

- Assume q is normalised: $q = q_1 + q_2$ where q_1 is linear and q_2 homogeneous of degree 2.
- Then q is symmetric (i.e. $\forall x, q(-x) = q(x)$) iff $q = q_2$.
- And q is antisymmetric (i.e. $\forall x, q(-x) = -q(x)$) iff $q = q_1$, i.e. is linear
- For any normalised q, $q(x) + q(-x)$ (resp. $q(x) - q(-x)$) is symmetric (resp. antisymmetric).
- $q(nx) = \frac{n^2+n}{2} q(x) + \frac{n^2-n}{2} q(-x)$.
  $q(nx) = n^2 q(x)$ if q is symmetric, $q(nx) = nq(x)$ if q is antisymmetric.

- If $\mathcal{L}$ is a line bundle on A, it is symmetric (resp. anti-symmetric) iff $[-1]^*\mathcal{L} \simeq \mathcal{L}$ (resp. $[-1]^*\mathcal{L} \simeq \mathcal{L}^{-1}$).
- $\mathcal{L} \otimes [-1]^*\mathcal{L}$ is always symmetric and $\mathcal{L} \otimes [-1]^*\mathcal{L}^{-1}$ always antisymmetric.
- $\mathcal{L}$ is antisymmetric iff $\mathcal{L} \in \mathrm{Pic}^0(A)$.
- $[n]^*\mathcal{L} \simeq \mathcal{L}^{\otimes,(n^2+n)/2} \otimes ([-1]^*\mathcal{L})^{\otimes,(n^2-n)/2}$
  $[n]^*\mathcal{L} \simeq \mathcal{L}^{\otimes,n^2}$ if $\mathcal{L}$ is symmetric, $[n]^*\mathcal{L} \simeq \mathcal{L}^{\otimes,n}$ if $\mathcal{L}$ is antisymmetric.

Torsors

- If X' is a X-torsor (i.e. there is a free and transitive group action of X on X'), we can say that $q : X' \to Z$ is quadratic whenever:

$$q(w+x+y+z) - q(w+x+y) - q(w+y+z) - q(w+z+x) + q(w+x) + q(w+y) + q(w+z) - q(w) = 0 \quad \forall w \in X', x,y,z \in X.$$

- It suffices to check that there is one $w \in X'$, such that

$$q(w+x+y+z) + q(w+z) - q(w+x+z) - q(w+y+z) = q(w+x+y) + q(w) - q(w+x) - q(w+y) \quad \forall x,y,z \in X$$

- We can then define a bilinear form on X via

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

this does not depend on w!

- If A' is an A-torsor, $\mathcal{L}$ a line bundle on A', we can define a polarisation

$$\Phi_{\mathcal{L}} : A \to Pic^0(A') \simeq Pic^0(A), \quad \Phi_{\mathcal{L}}(P) = t^*_{A',P}\mathcal{L} \otimes \mathcal{L}^{-1},$$

where $t_{A',P}$ is the translation action of $P \in A$ on A'.
- Example: if $A = \mathrm{Jac}(C) = \mathrm{Pic}^0(C)$ is a Jacobian of a curve of genus g, the Theta divisor $\Theta_g \subset \mathrm{Pic}^{g-1}(C)$ ($\Theta_g =$ locus of effective divisors of degree $g-1$) induces a principal polarisation on $\mathrm{Jac}(C)$.

Arithmetic consequences

- Because $[2] : \mathbb{G}_m \to \mathbb{G}_m, x \mapsto x^2$ is not surjective (only surjective étale locally), a polarisation $\Phi : A \to \widehat{A}$ may not be induced by a line bundle $\mathcal{L}$ on A (it is only induced étale locally)

- Tate: if A/K is principally polarised, Ш(A/K) is a square.
- Poonen-Stoll: explicit example of $C/\mathbb{Q}$ such that Ш$(\mathrm{Jac}(C)/\mathbb{Q})$ is not a square.
- But we just saw that a Jacobian is principally polarised.
- Different notion of principal polarisations! For Tate it comes from a rational line bundle.
- In the first case the Cassel-Tate pairing is alternating, in the second only antisymmetric.

Some mysteries

- Let $\Phi : A \to \widehat{A}$ be a principal polarisation (i.e. Φ is an isomorphism and is induced by an ample line bundle $\mathscr{L}$)
- We think of Φ as a unimodular positive definite symmetric bilinear form b_Φ
- The Weil pairings $e_{\Phi,[n]} : A[n] \times A[n] \to \mu_n$ should be incarnations of b.
- But they are antisymmetric, not symmetric

- If $A = \mathbb{C}^g/\Lambda$ is a complex abelian variety, a polarisation ϕ can be described by a positive definite Hermitian form H on $\mathbb{C}^g$ such that $\Im H \mid \Lambda \times \Lambda \subset \mathbb{Z}$.
- But H is Hermitian and $E = \Im H$ is symplectic, none are symmetric.
- However, a choice of line bundle $\mathscr{L}$ inducing ϕ is the same as a choice of quasi-character χ for H:

$$\chi(\lambda_1 + \lambda_2) = \chi(\lambda_1)\chi(\lambda_2)e^{i\pi E(\lambda_1,\lambda_2)} \quad \forall \lambda_1, \lambda_2 \in \Lambda$$

- $\chi : \Lambda \to \mathbb{G}_m$ is quadratic.

Table of Contents

Bilinear maps on abelian varieties

- Goal: associate to a line bundle $\mathcal{L}$ on A a quadratic form $q : A \to \mathbb{G}_m$, and to a polarisation $\phi : A \to \widehat{A}$ a bilinear form $b : A \times A \to \mathbb{G}_m$.
- Here $A, \mathbb{G}_m$ are group schemes, so q, b should be morphisms of group schemes.
- And they should satisfy the appropriate version of bilinearity/quadracity.

- A is not a group, it is a group object in the category of schemes
- But schemes embed fully faithfully into the presheaf topos on affine schemes.
- In fact, if X is a scheme, $R \mapsto X(R)$ is an fppf-sheaf.
- A group object G in the category of sheafs is the same thing as giving a group structure on each $G(R)$ such that $\phi : R \to S$ induces a group morphism $G(\phi) : G(R) \to G(S)$.
- Similarly, we can define bilinearity and quadracity pointwise.

Internal logic of a topos

- Recall: we can see $A, \mathbb{G}_m$ as abelian sheafs for the fppf topology
- Sheafs form a topos: in the internal logic of a topos they behave like a set!
- The internal logic is like a compiler, that translates internal statements into external statements.
- For instance, if $\phi : F \to G$ is a morphism of sheafs, it translates the internal surjectivity statement

$$\forall y \in G, \exists x \in F \mid \phi(x) = y$$

  into the external epimorphism statement:
  "For all sections $y \in G(U)$, there is a covering $U = \bigcup U_i$ such that there exists a section $x_i \in F(U_i)$ where $\phi(x_i) = y \mid U_i$".
- We can prove internally that a composition $\phi_2 \circ \phi_1$ of two surjective morphisms $\phi_1 : F \to G$ and $\phi_2 : G \to H$ is surjective: "$\forall z \in H, \exists y \in G \mid \phi_2(y) = z$, and $\exists x \in F \mid \phi_1(x) = y$, so $\phi_2(\phi_1(x)) = z$". The compiler translate this into the usual external proof using coverings of coverings.
- Caveat: the internal logic of a topos is intuitionistic logic: for a proposition P, $P \vee \neg P$ is not always true.
- Intuitionistic logic is constructive, this is the logic given by the Curry-Howard correspondance. One needs to add continuations as first class citizen to recover classical logic.

Bilinear and quadratic forms on an abelian variety via topos

- We can define linear, bilinear and quadratic forms in a topos by using the same definitions as for standard groups, expressed in the internal logic of the topos.
- $b : A \times B \to \mathbb{G}_m$ is bilinear iff:

$$\forall a_1, a_2 \in A, b_1, b_2 \in B, b(a_1 + a_2, b_1 + b_2) = b(a_1, b_1) \times b(a_1, b_2) \times b(a_2, b_1) \times b(a_2, b_2).$$

- This is a statement in a cartesian theory, hence in particular a geometric theory.
- This recovers the pointwise definition: $b : A(R) \times B(R) \to \mathbb{G}_m(R)$ should be bilinear (in a compatible way) for all R

  Recall that the fppf topos has enough points.
- A bilinear map $A \times B \to \mathbb{G}_m$ could also be defined as a linear map $A \otimes B \to \mathbb{G}_m$.

- Unfortunately, for abelian varieties, there are no bilinear maps $A \times B \to \mathbb{G}_m$: A, B are proper while $\mathbb{G}_m$ is affine, so any such map would be constant.
- Likewise, all maps $A \to \mathbb{G}_m$ are constant, so there are no non trivial linear or quadratic maps.
- This "naive" approach does not explains the analogy.

Animating bilinear and quadratic maps

- There are no bilinear maps $A \times B \to \mathbb{G}_m$ when we embed $A, B, \mathbb{G}_m$ into a category of sheafs of sets.
- We will instead embed them into the larger category of sheafs of spaces, or rather sheafs of anima (the ∞-category of homotopy types of spaces)
- Bilinear or quadratic maps on animated abelian groups (i.e. abelian groups in anima) may be seen as higher order bilinear or quadratic forms.

- Let Ani be the ∞-category of anima, i.e. ∞-groupoids
(This is the $(\infty, 1)$-category of $(\infty, 0)$-categories).
- An ∞-groupoid is a Kan complex (up to inverting weak equivalences), i.e. the homotopy type of a space
- An ∞-category is a quasi-category, i.e. a weak Kan complex (up to inverting weak equivalences)
- The bible on this is Lurie's books: Higher Topos Theory, Higher Algebra, Spectral schemes.

The animation of a category

- The term animation (due to Clausen) was introduced in Česnavičius-Scholze [ČS24]. The authors describe the animation of a locally strongly finitely presentable category C, relying heavily on Lurie's work on ∞-locally presentable categories.
- If C is a category of algebraic structures (i.e. of rings, groups, modules, ...), then $\mathsf{Ani}(C)$ is the ∞-category of these algebraic structures in Ani (animated rings, animated groups, animated modules)...
- Ani itself is the animation of Set: the trivial algebraic structure.

Locally strongly finitely presentable categories

The following are equivalent for a category C

- C is the category of models for an algebraic theory, i.e. there exists a category T with finite products such that $C = \mathrm{Hom}_{\prod}(T, \mathrm{Set})$.
- C is the category of models for a finite product sketch.
- C is the free cocompletion of a small category C_0 with finite coproducts under sifted colimits: $C = \mathrm{sInd}(C_0)$
- C has all small colimits, the category C^{sfp} of strongly finitely presentable objects (also called compact projective objects) is essentially small, and any object in C is a sifted colimit of the canonical diagram of strongly finitely presentable objects mapping into it.
- C^{sfp} has finite coproducts, and the restricted Yoneda embedding $C \hookrightarrow [C^{sfp\circ}, \mathrm{Set}]$ identifies C with the category of finite-product-preserving functors $C^{sfp\circ} \to \mathrm{Set}$.

- A sifted colimit is a colimit of a diagram $D \to C$ where D is sifted, i.e. the associated colimits commute with finite products in Set.
- This is a generalisation of an inductive colimit $D \to C$ where D is required to be filtered, i.e. so that the associated colimits commute with all finite limits in Set.
- A reflexive coequalizer (i.e. the quotient of an equivalence relation) is a sifted colimit. A good rule of thumb is "sifted colimits = inductive colimits + reflexive coequalizer" (but see [ARV10] for caveats).
- $x \in C$ is strongly finitely presentable if $\mathrm{Hom}(x, \cdot)$ commutes with sifted colimit.

Modulo size issues, in the above one can take $C_0 = C^{sfp}$ and $T = C^{sfp\circ}$.

Locally finitely presentable categories

The following are equivalent for a category C

- C is the category of models for an essentially algebraic theory, i.e. there exists a category T with finite limits such that $C = \mathrm{Hom}_{lex}(T, \mathrm{Set})$.
- C is the category of models for a finite limit sketch.
- C is the free cocompletion of a small category C_0 with finite colimit under filtered colimits: $C = \mathrm{Ind}(C_0)$
- C has all small colimits, the category C^{fp} of finitely presentable objects (also called compact objects) is essentially small, and any object in C is a filtered colimit of the canonical diagram of locally finitely presentable objects mapping into it.
- C^{fp} has finite colimits, and the restricted Yoneda embedding $C \hookrightarrow [C^{fp\circ}, \mathrm{Set}]$ identifies C with the category of finite-limit-preserving functors $C^{fp\circ} \to \mathrm{Set}$.

Modulo size issues, in the above one can take $C_0 = C^{fp}$ and $T = C^{fp\circ}$.

Properties of a locally strongly finitely presentable category

- If $C = \mathtt{sInd}(C^{sfp})$ is locally strongly finitely presentable, it is locally finitely presentable: $C = \mathtt{Ind}(C^{fp})$
- The finitely presentable objects C^{fp} are the coequalizers (or even reflexive coequalizers) of objects in C^{sfp}
- A functor $F : C \to D$ preserving sifted colimits (resp. filtered colimits) is the same thing as a functor $F : C^{sfp} \to D$ (resp. $F : C^{fp} \to D$): C is the free completion of C^{sfp} under sifted colimit (resp. filtered colimits).
- And F preserve all colimits (i.e. is right exact) iff $F \mid C^{sfp}$ preserve finite coproducts (or $F \mid C^{fp}$ preserve finite colimits).
- $C = \mathtt{Hom}_{\prod}(C^{sfp\circ}, \mathtt{Set}) = \mathtt{Hom}_{lex}(C^{fp\circ}, \mathtt{Set}) = \mathtt{Hom}_{cont}(C^{\circ}, \mathtt{Set})$.

Examples of locally strongly finitely presentable categories

- Every algebraic theory gives a locally strongly finitely presentable category
- Main examples: Set, Groups, Abelian groups, (commutative) Rings, Modules over a ring
- In all these examples, strongly finitely presentable object / compact projective objects are the retract of finite free objects, i.e. the Cauchy completion of finite free objects.
- Finite free rings: $R = \mathbb{Z}[x_1, \dots, x_m]$.
- Finite free modules: $M = R^m$.

Animating a locally strongly finitely presentable category

- If $C = \mathsf{sInd}(C^{sfp})$ is locally strongly finitely presentable, $\mathsf{Ani}(C)$ is the free completion of C^{sfp} under sifted colimit in the $(\infty, 2)$-category of $(\infty, 1)$-categories.
- If $D \in \mathsf{Ani}$ is a ∞-category with sifted colimits, a functor $F : \mathsf{Hom}_{sifted}(\mathsf{Ani}(C), D)$ is the same thing as a functor $C^{sfp} \to D$.
- In an ∞-category sifted colimits are generated by filtered colimits and geometric realisations, i.e. colimits indexed by Δ° (reflexive coequalizers are colimits indexed by $\tau_{\leq 1}\Delta^\circ$).

- $\mathsf{Ani}(C)$ is the ∞-category of functors $\mathsf{Hom}_{\prod}(C^{sfp\circ}, \mathsf{Ani})$.
- This is also the category of simplicial objects in C up to inverting weak equivalences.
- A functor $F : C \to D$ of locally strongly finitely presentable categories that preserves sifted colimits lifts to a functor $\mathsf{Ani}(F) : \mathsf{Ani}(C) \to \mathsf{Ani}(D)$.
- Given $G : D \to E$, there is a natural transformation

$$\mathsf{Ani}(G) \circ \mathsf{Ani}(F) \to \mathsf{Ani}(G \circ F),$$

which is an equivalence if $F(C^{sfp}) \subset \mathsf{Ind}\, D^{sfp}$ in D or $\mathsf{Ani}(G)(F(C^{sfp})) \subset E$ in $\mathsf{Ani}(E)$.

Animation: a summary

- A $(1,1)$-category is a category enriched over Set
- Set itself is the free completion of finite sets under 1-sifted colimits
- A $(\infty,1)$-category is a category enriched over Ani
- Ani itself is the free completion of finite sets under ∞-sifted colimits (i.e. inductive limits and geometric realisations).

- A locally strongly finitely presentable category C is the free completion of a small category C_0 with coproducts under 1-sifted colimits.
- $C = \mathrm{Hom}_{\prod}({C_0}^{\circ}, \mathrm{Set})$
- Its animation $\mathrm{Ani}(C)$ is the free completion of C_0 under 1-sifted colimits.
- $\mathrm{Ani}(C) = \mathrm{Hom}_{\prod}({C_0}^{\circ}, \mathrm{Ani})$

Animating an abelian category

- Dold-Kan correspondance: if $\mathcal{A}$ is an abelian category, $\mathrm{Ani}(\mathcal{A})$ is equivalent to the connective part $D_{\geq 0}(\mathcal{A})$ of the ∞-derived category of $D(\mathcal{A})$.
  (For cochains: $\mathrm{Ani}(\mathcal{A}) \simeq D^{\leq 0}(\mathcal{A})$),
- And $D(\mathcal{A})$ is recovered as the stabilisation $\mathrm{Stab}(\mathrm{Ani}(\mathcal{A}))$ of $\mathrm{Ani}(\mathcal{A})$

- If (X, τ) is a site, the animation of the sheaf topos $\mathrm{Sh}(X, \mathrm{Set})$ is the hypercompletion of the ∞-topos $\mathrm{Sh}_\infty(X, \mathrm{Ani})$
- And stabilisation commute with localisation:

$$\mathrm{Stab}(\mathrm{Sh}(X, \mathrm{Ani})) = \mathrm{Sh}(X, \mathrm{Spectra})$$

  where $\mathrm{Spectra} = \mathrm{Stab}(\mathrm{Ani})$ is the stable ∞-category of spectra.

The standard derived category

- $\mathcal{A}$ an abelian category. For simplicity $\mathcal{A} = \mathbb{Z} - modules$
- $C(\mathcal{A})$ the category of complexes on $\mathcal{A}$
- Unit interval: $I \in C(\mathcal{A})$: $I[0] = \mathbb{Z}[0] \oplus \mathbb{Z}[1], I[1] = [I]$ with $d[I] = [1] - [0]$.
- Homotopy: map $X \otimes I \to Y$
- $K(\mathcal{A})$: complexes up to homotopy equivalence
- $D(\mathcal{A})$: $K(\mathcal{A})$ localised in the quasi-isomorphisms (i.e. we invert “formally” the morphisms in $K(\mathcal{A})$ which induces isomorphisms on all H^i). Localisation means that in the map $i : K(\mathcal{A}) \to D(\mathcal{A})$ quasi-isomorphisms are sent to isomorphisms, and $D(\mathcal{A})$ is universal for this property.
- $K(\mathcal{A}), D(\mathcal{A})$ are triangulated categories: the distinguished triangles are given by (isomorphisms class of) mapping cones.

- If $F : \mathcal{A} \to \mathcal{B}$ is a left exact functor, the right derived functor RF (if it exists) is the right Kan extension of $F : K(\mathcal{A}) \to K(\mathcal{B}) \to D(\mathcal{B})$ along $i : K(\mathcal{A}) \to D(\mathcal{A})$: it is the universal functor $RF : D(\mathcal{A}) \to D(\mathcal{B})$ such that there is a natural transformation $RF \circ i \Rightarrow F$.

Internal logic of an ∞-topos

- The internal logic of an ∞-topos is described by HoTT: homotopy type theory
- In HoTT, all objects have a type: $a : A$ means that a has type A
- The main difference with standard type theory is that the identity type $\mathrm{Id}_A(a = b)$ is no longer a boolean `true/false` (i.e. the 0-category of -1-categories) but a type itself.
- One may interpret $\mathrm{Id}_A(a = b)$ as an Anima, a witness w for equality $a = b$ can be interpreted as a path from a to b, and then a witness in $\mathrm{Id}_{\mathrm{Id}_A}(w_1 = w_2)$ between two witnesses w_1, w_2 may be interpreted as an homotopy between w_1 and w_2 and so on.

Animating bilinear and quadratic forms

We can embed abelian schemes into the (stabilisation of the) ∞-topos of sheafs of anima, and look at animated bilinear and quadratic forms with values in $\mathrm{Ani}(\mathbb{G}_m)$.

Definition

- The dual abelian variety $\widehat{A}$ is the (appropriate truncation of) animated linear maps $\mathrm{Hom}(\mathrm{Ani}(A), \mathrm{Ani}(\mathbb{G}_m))$;
- The category of (symmetric) biextensions $\mathrm{BiExt}(A, B; \mathbb{G}_m)$ is the (appropriate truncation of) animated bilinear maps $\mathrm{Ani}(A) \times \mathrm{Ani}(B) \to \mathrm{Ani}(\mathbb{G}_m)$
- The category of cubical structures on A $\mathrm{Cube}(A, \mathbb{G}_m)$ is (the appropriate truncation of) animated quadratic maps $\mathrm{Ani}(A) \to \mathrm{Ani}(\mathbb{G}_m)$

For the truncation: we work over the suspension $\Sigma(\mathrm{Ani}(\mathbb{G}_m))$ and truncate to the connective part of the canonical t-structure of the stable ∞-category. We end up with ordinary categories.

One can see biextensions and cube structures as bilinear maps and quadratic maps with values in $B\mathbb{G}_m$ rather than in $\mathbb{G}_m$.

Bilinear and quadratic forms on an abelian variety via the derived category of fppf sheaves

Using the Dold-Kan correspondance, we can reinterpret these constructions in the derived category $D(Sh_{fppf})$ of fppf sheaves. (We work with cochains, so shift correspond to suspension and $\pi_i = H^{-i}$)

- Weil: the dual
$$\widehat{A} \simeq \tau_{\leq 0} R\,\mathrm{Hom}(A, \mathbb{G}_m[1])$$
In particular, $Q \in \widehat{A}$ induces a group extension $G(Q)$ of A by $\mathbb{G}_m$.
($G(Q)$ is necessarily commutative since the commutator pairing $A \times A \to \mathbb{G}_m$ is constant).
- Grothendieck: morphisms $\phi : A \to \hat{B}$ correspond bijectively to biextensions of $A \times B$ by $\mathbb{G}_m$, which in turn are given by
$$\tau_{\leq 0} R\,\mathrm{Hom}(A \otimes^L B, \mathbb{G}_m[1]).$$
- Breen: polarisations $\phi_{\mathcal{L}}$ on A corresponds to symmetric biextensions on $A \times A$ by $\mathbb{G}_m$, which “corresponds” to
$$\tau_{\leq 0} R\,\mathrm{Hom}(R\,\mathrm{Sym}^2 A, \mathbb{G}_m[1]).$$
- Breen: a line bundle $\mathcal{L}$ corresponds to a cubic structure on A by $\mathbb{G}_m$, which in turns “corresponds” to
$$\tau_{\leq 0} R\,\mathrm{Hom}(R\Gamma_2 A, \mathbb{G}_m[1]).$$
Here Γ_2 is the component of degree 2 of the divider power algebra

$F \mapsto \mathrm{Sym}^2 F$ and $F \mapsto \Gamma_2 F$ are quadratic rather than additive functors, so care must be taken when taking their derived version (we need to use simplicial resolutions).

Line bundles

- $B\mathbb{G}_m = [*/\mathbb{G}_m]$ is the classifying stack of $\mathbb{G}_m$-torsors: this is the delooping of $\mathbb{G}_m$.
- To give a line bundle $\mathscr{L}$ on a scheme X is the same thing as giving a map $X \to \mathbb{G}_m$.
- Under the Dold-Kan correspondance for cochains, the shift corresponds to the suspension Σ, aka to delooping, the inverse of the loop function Ω.
- Hence we have:

$$H^0 R\,\mathrm{Hom}(A, \mathbb{G}_m[1]) \simeq \mathrm{Ext}^1(A, \mathbb{G}_m) \simeq \mathrm{Hom}(A, B\mathbb{G}_m) \simeq \pi_0\,\mathrm{Hom}(\mathrm{Ani}(A), \Sigma\,\mathrm{Ani}(\mathbb{G}_m))$$

- Here $\mathrm{Hom}(A, B\mathbb{G}_m)$ denotes morphisms respecting the group law ("morphisms of Picard stacks")
- An element in $\mathrm{Hom}(A, B\mathbb{G}_m)$ corresponds to a line bundle $\mathscr{L}$ algebraically equivalent to 0: $\mathscr{L} \in \mathrm{Pic}^0(A)$
- We recover the isomorphism $\widehat{A} = \mathrm{Pic}^0(A) \simeq \mathrm{Ext}^1(A, \mathbb{G}_m)$, given concretely by the theta group: $\mathscr{L} \mapsto G(\mathscr{L})$

Biextensions and cubical structures

- Recall: biextensions and cube structures are bilinear maps and quadratic maps with values in $B\mathbb{G}_m$ rather than in $\mathbb{G}_m$
- But since we work in the internal logic of an ∞-topos, the bilinear equation $b(x+y,z)=b(x,z)+b(y,z)$ needs to be witnessed by a "path" satisfying some further coherency conditions

- A biextension is a "bilinear map" $b : A \times B \to B\mathbb{G}_m$, in particular we get a line bundle $\mathcal{L}$ above $A \times B$
- The bilinearity $\Theta_{2,2}(b)=0$ gives a section s on $\Theta_{2,2}(\mathcal{L})$ above $A^2 \times B^2$
- This section s has to satisfy some cocycle conditions

- A cubical structure is a "quadratic map" $q : A \to B\mathbb{G}_m$, in particular we get a line bundle $\mathcal{L}$ above A
- The quadraticity $\Theta_3(q)=0$ gives a section s on $\Theta_3(\mathcal{L})$ above A^3
- This section s has to satisfy some cocycle conditions
- Moret-Bailly the cocyle conditions are equivalent to the fact that, up to replacing A, G by $A' \twoheadrightarrow A$ and $\mathbb{G}_m \hookrightarrow G'$, there is a trivialisation t' of the induced G'-torsor $\mathcal{L}'$ on A' induced by $\mathcal{L}$ such that $\Theta_3(t')=s'$ where s' is the trivialisation on $\Theta_3(\mathcal{L}')$ induced by s.
  Similarly for biextensions.

Squared structures on line bundles

- Let's work out in more detail what a "linear map" $\phi : G \to B\mathbb{G}_m$ should be for a commutative group scheme G
- First we have a map to $B\mathbb{G}_m$, hence a line bundle $\mathcal{L}$ on G.
- Secondly we have $\Theta_2(\phi) = 0$, i.e. a squared structure.
- This is witnessed by a section s of $\Theta_2(\mathcal{L})$ above $G \times G$: for every $x, y \in G$, we have an isomorphism $t_x^* \mathcal{L} \otimes t_y^* \mathcal{L} \simeq t_{x+y}^* \mathcal{L} \otimes \mathcal{L}$
(Recall that $\Theta_2(f) : (x, y) \mapsto f(x+y) + f(0) - f(x) - f(y)$.)
- The coherence/cocycles conditions on s amount to the fact that s should induce a group structure on $\mathcal{L}$, which is a commutative group extension of G by $\mathbb{G}_m$.

- If A is an abelian variety, the fact that $\mathrm{Hom}(A, \mathbb{G}_m) = 0$ automatically give such a squared structure (uniquely!) for any $\mathcal{L} \in \mathrm{Pic}^0(A)$
- Similarly for biextensions and cube structures: a line bundle $\mathcal{L} \in \mathrm{Pic}(A)$ automatically has a unique cube structure.

Pairings from biextensions

- Once we have a cubical structure on A or biextension on $A \times B$, every equality inside $B\mathbb{G}_m$ in the internal logic give us a trivialisation of some line bundle, and equality between these equalities correspond to maps between these trivialisations, i.e. maps to $\mathbb{G}_m$, which satisfy some conditions.
- For instance, given a principal polarisation $b : A \times A \to B\mathbb{G}_m$, then nb is zero on $A[n] \times A$ and $A \times A[n]$. This gives two different trivialisations on $A[n] \times A[n]$, and the map between them is the Weil pairing $e_{b,n}$
- We can also write
$$nb(x,y) = b(nx,y) = b(x,ny) = 0$$
where the later equalities take place in the biextension associated to b. We recover Stange's interpretation of the Weil pairing as monodromy.
- Likewise, the Tate pairing "comes" from $b(nx,y) = 0$ for $x \in A[n]$.

- Note that, even if we have a symmetric biextension, the compatibility conditions "one level up" need not be symmetric.
- Indeed, symmetric biextensions on the trivial torsor are given by alternate forms $a(x_1,x_2)$. This biextension is a trivial symmetric biextension on X iff $a(x_1,x_2) = b(x_1,x_2) - b(x_2,x_1)$ for some bilinear form $b : X \times X \to \mathbb{G}_m$.

- Likewise, if $A = \mathbb{C}^g/\Lambda$, the cube structure induced by a line bundle $\mathcal{L}$ on A becomes trivial over $\mathbb{C}^g$. The cube structure on A is then encoded by the descent of the trivial cube structure on $\mathbb{C}^g$ along Λ.

- This recovers semi-characters and the theory of theta functions [Breen].

Table of Contents

The Poincaré biextension on an elliptic curve

Υ the biextension associated to (0_E) above $E \times E$:

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

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

- Biextension law:

$$g_{P_1,Q} \star_1 g_{P_2,Q} = g_{P_1+P_2,Q} := g_{P_1,Q}(\cdot) g_{P_2,Q}(\cdot + P_1)$$
$$= g_{P_1,Q}(\cdot) g_{P_2,Q}(\cdot) \frac{g_{P_1,P_2}(\cdot + Q)}{g_{P_1,P_2}(\cdot)}$$

N.B: the last equality is not obvious and result from cohomological arguments

- Similar formulas for $g_{P,Q_1} \star_2 g_{P,Q_2} = g_{P,Q_1+Q_2}$
- Bilinearity property: for every Q (resp. every P), $\star_1$ (resp. $\star_2$) gives a commutative group law on the $g_{P,Q}$ (=linearity on the left/right).
- Compatibility:

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

Pairings via biextensions

- If $P = 0_E$ or $Q = 0_E$, $(P+Q) + (0_E) - (P) - (Q) \sim 0$, 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!

- 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 $\mathscr{L}$ is a line bundle on A, seen as a fibration $\mathscr{L} \to A$ with fibers $\mathbb{A}^1$ rather than an invertible sheaf, we let $X_{\mathscr{L}} = \mathscr{L} \setminus 0$.
- Given $P \in A$, a cubical point $\widetilde{P}$ is an element $\widetilde{P} \in X_{\mathscr{L}}$ above P via the projection $X_{\mathscr{L}} \to A$
- All other cubical points are of the form $\lambda\widetilde{P}$ for $\lambda \in \mathbb{G}_m$ ($\mathscr{L}$ is a $\mathbb{G}_m$-torsor)
- If $\mathscr{L}$ is very ample, and $X_0, \dots X_N \in \Gamma(A, \mathscr{L})$ is a basis of sections, we have a commutative diagram

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

- A point $P \in A$ 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 affine coordinates:

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

- This also works to define cubical points $\widetilde{P}$ when $\mathscr{L}$ is not very ample, as long as P is not a base point of $\mathscr{L}$

- **Exercice**: what does a cubical point represent in the other equivalent descriptions of the line bundle $\mathscr{L}$?

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 $(x(P), y(P))$.

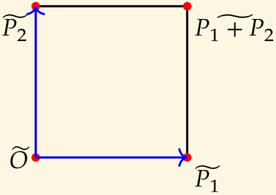
- A level 3 cubical point $\widetilde{P}$ is a choice of $(X_3(\widetilde{P}), Y_3(\widetilde{P}), Z_3(\widetilde{P}))$ above $(X_3(P) : Y_3(P) : Z_3(P))$.
  N.B: $D = 3(0_E)$ is very ample. Example: fix $\widetilde{O} = (0, 1, 0)$.

- 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 $\widetilde{O} = (0, 1)$.

- A level 1 cubical point $\widetilde{P}$ is a choice of $Z_1(P)$.
  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: a degenerate case

- Assume that $\mathscr{L}$ is algebraically equivalent to 0: $\phi_{\mathscr{L}} = 0$
  (If D is a divisor on E, this is equivalent to $\deg D = 0$)
- Then $X_{\mathscr{L}}$ is a commutative group, an extension of A by $\mathbb{G}_m$
- Reformulation: we have a squared structure on $X_{\mathscr{L}}$



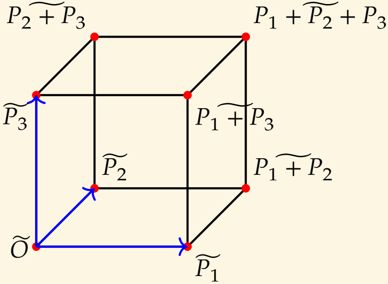
- $\widetilde{P_1 + P_2}$ is uniquely determined by $\widetilde{P_1}, \widetilde{P_2}$ (and $\widetilde{O}$)
- The squared structure also determines $-\widetilde{P}$

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
- We don't have a group / a squared structure anymore
- But we do have a cubical structure!



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

Corollary

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

The cubical structure does not determine $-\widetilde{P}$ anymore. But if $\mathcal{L}$ is symmetric there is a notion of Σ-cubical structure to define $-\widetilde{P}$ in a way compatible with the cubical arithmetic. This allows to define $\sum n_i \widetilde{P_i}$ for $n_i \in \mathbb{Z}$.

Formulas 1

- Cubical arithmetic arises from a canonical isomorphism
$\mathcal{L}_{P_1+P_2+P_3} \otimes \mathcal{L}_{P_1} \otimes \mathcal{L}_{P_2} \otimes \mathcal{L}_{P_3} \simeq \mathcal{L} \otimes \mathcal{L}_{P_2+P_3} \otimes \mathcal{L}_{P_1+P_3} \otimes \mathcal{L}_{P_1+P_2}$
- 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: (Anti)-symmetry:* $\mathrm{cub}_D(P_1, P_2, -P_1 - P_2) = \pm 1$.

- 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

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

- 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: $Z_1(2\widetilde{P}) = Z(\widetilde{P})^4 2y(P)$
- 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: $y^2 = x^3 + \mathcal{A}x^2 + x$)

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

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!

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 $e_{\mathcal{L},\ell}$
- Computing (polarised) isogenies $\phi : (A, \mathcal{L}^\ell) \to (B, \mathcal{M})$
- Computing isogeny preimages
- Computing radical isogenies
- Computing functions with prescribed divisors
- Changing level

- N.B.: formulas for cubical arithmetic can be derived from sufficiently explicit formulas for the theorem of the square

Algorithmic intuition

High level overview:

- The cubical structure on $X_{\mathcal{L}} \to A$ induces the biextension $Y_{\mathcal{L}} \to A \times A$
- In practice: represent $g_{P,Q}$ by the four cubical points $\widetilde{0_E}, \widetilde{P}, \widetilde{Q}, \widetilde{P+Q}$.
- Cubical arithmetic ⇒ biextension arithmetic ⇒ pairings

- This biextension $Y_{\mathcal{L}}$ is trivial over $K(\mathcal{L}) \times A$
- For formal reasons, this recovers the theta group $G(\mathcal{L})$ and its action on sections
- Cubical arithmetic ⇒ theta group arithmetic ⇒ isogenies

Unicity of cubical structures:

- Level-n cubical arithmetic on A induces level-$n\ell$ cubical arithmetic on A (and conversely) ⇒ change of level
- Level-$n\ell$ cubical arithmetic on A induces level-n cubical arithmetic on B, where B is ℓ-isogeneous to A ⇒ isogenies
- Level-n cubical arithmetic on A induces level-$n\ell$ cubical arithmetic on B, where B is ℓ-isogeneous to A ⇒ isogeny preimages

Example: Vélu's formulas

- $E_1/k : y_1^2 = x_1^3 + ax_1 + b_1$ elliptic curve
- $\phi : E_1 \to E_2 = E_1/K$, isogeny with kernel $K = \langle P \rangle$
- Vélu's formulas use traces:

$$x_2(P) := \sum_{i=0}^{\ell-1}(x_1(P+iT) - \sum_{i=1}^{\ell-1} x_1(iT), \quad y_2(P) := \sum_{i=0}^{\ell-1}(y_1(P+iT) - \sum_{i=1}^{\ell-1} y_1(iT)$$

- Recall that $x_1 = X/Z, y_1 = Y/Z$ are rational functions
- Cubical arithmetic allows us to directly take "cubical traces" of X, Y, Z

- Vélu's formulas do not extend directly to higher dimension (for degree reasons)
- But the cubical trace approach does!

- Cosset-Lubicz-R. isogeny formulas already used (without knowing!) "cubical traces" of theta functions
- Algorithms thoroughly optimised in [YOOKN25]
- Cubical point of view brings more flexibility ⇒ Corte-Real Santos et al 30% improvement for isogenies and 50% improvement for images compared to [YOOKN25] (work in progress)

Example: Radical isogeny formulas

- We have working radical isogeny formulas in various variants of the Montgomery model
- Speed up of $\approx 2\times$ to $\approx 2.5\times$ compared to Decru's formulas in [Dec24]
  (Depending on the model and whether ℓ is a sum of two squares or not)

- Works in x-only coordinates, using (X, Z)-cubical arithmetic
  (This is the main source of savings: we can use symmetry to only compute only half the points)
- Example: In the theta model, a ℓ-radical isogeny (for ℓ a sum of two squares) costs a ℓ-th root, and $1I + 6\ell M + O(\log \ell)M$ arithmetic operations
- And the "preimage" of a point through the dual isogeny costs a ℓ-th root, and $1I + 5\ell M + O(\log \ell)M$ arithmetic operations
- Decru: $3I + (16\ell - 25)M$

- Still a work in progress
- The difference of complexity for a prime $\ell \equiv 1 \pmod 4$ vs $\ell \equiv 3 \pmod 4$ comes from the way we compute the cubical descent of level from level 2ℓ to level 2.
- **Question**: Better descent of level formulas?

Cubical functions

- $Z \in \Gamma(A, \mathscr{L})$ with associated divisor D
- $\widetilde{R} \mapsto Z(\widetilde{R} + \sum n_i \widetilde{P}_i)$ is a "cubical function" with divisor $t^*_{\sum n_i P_i} D$.
- Depends on the choices of $\widetilde{P_i}, \widetilde{P_i + P_j}$, but also of $\widetilde{R}, \widetilde{R + P_i}$
- Combining these cubical functions we can get genuine elliptic functions, not depending on the choices of $\widetilde{R}, \widetilde{R + P_i}$

Cubical functions

Example

- $$R \mapsto g_{P_1,P_2}(R) = \frac{Z(R+\widetilde{P_1+P_2})Z(\widetilde{R})}{Z(\widetilde{R+P_1})Z(\widetilde{R+P_2})}$$

  is a genuine function g_{D,P_1,P_2} with divisor $t^*_{P_1+P_2}D + D - t^*_{P_1}D - t^*_{P_2}D$.
  It only depends on the choices of $\widetilde{P_1}, \widetilde{P_2}, \widetilde{P_1+P_2}$.

- $$R \mapsto \frac{Z(\ell\widetilde{P}+\widetilde{R})Z(\widetilde{R})^{\ell-1}}{Z(\widetilde{P+R})^{\ell}}$$

  is a genuine function $f_{D,\ell,P}$ with divisor $t_{\ell P}D + (\ell-1)D - \ell t^*_P D$.

- If $P \in A[\ell]$,
  $$R \mapsto \frac{Z(\ell\widetilde{R})Z(\ell\widetilde{P}+\widetilde{R})}{Z(\ell\widetilde{R}+\widetilde{P})Z(\widetilde{R})}$$

  is a genuine function with divisor $[\ell]^*(D - t^*_P D)$.
  (Compare with how we would compute this function with Miller's algorithm.)

Pairings via cubical arithmetic

- Up to $\approx 2\times$ faster pairing computation for isogeny based cryptography, compared to Miller's algorithm [PRRSS25]
- Pairings entirely on the Kummer line, using level 2 cubical arithmetic
- N.B.: since level 2 cubical arithmetic gives the pairings $e_{2(0_E),\ell} = e^2_{(0_E),\ell}$, a priori we only recover squared pairings.
- But we have a trick to recover the level -1 pairings $e_{(0_E),\ell}$ when ℓ is even (New: and also when ℓ is odd!)
- Potentially useful for pairings based cryptography too [LRZZ25]

The Discrete Logarithm Problem

- One can reduce DLPs on A/k to cubical DLPs (via "excellent cubical lifts")
- Conversely, cubical DLPs reduce to DLPs on A and k^*
- (Similarly for biextensions and theta groups DLPs)

- With extra information, cubical DLPs may only need DLPs in k^*

$\Rightarrow$ Monodromy leak

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

Higher degree and higher level

- We can also animate degree n and multilinear forms.
- n-multi-extension of $\prod A_i$ by $\mathbb{G}_m \simeq n$-multilinear map $\prod A_i \to \mathbb{G}_m$
- $(n+1)$-hypercube structure on A by $\mathbb{G}_m \simeq$ degree n map $A \to \mathbb{G}_m$

- A n-bilinear map $b : A^n \to \mathbb{G}_m$ gives a degree n function

$$q : A \to \mathbb{G}_m, q(x) \mapsto b(x, \dots, x)$$

- Conversely a degree n function gives a symmetric n-bilinear map $A^n \to \mathbb{G}_m$
- The same holds for n-multi-extensions and $(n+1)$-hypercube structures.

- Unfortunately on abelian varieties, a tri-extension is trivial (it is induced by a biextension), so there are no interesting hypercube structures [Grothendieck].
- If $\pi : X \to S$ is a proper flat morphism of relative dimension n, then the determinant functor $R\pi_*$ has a $(n+2)$-hypercube structure which gives a multilinear pairing $\mathrm{Pic}(X)^{n+1} \to \mathrm{Pic}(S)$ [Deligne]

- We could also look at higher level bilinear and quadratic forms, i.e. with values in $B^2\mathbb{G}_m$ rather than $B\mathbb{G}_m$.
- This would give us quadratic forms in gerbes rather than in torsors.

Bibliography

[ARV10] J. Adámek, J. Rosicky, and E. M. Vitale. "What are sifted colimits?" In: Theory and Applications of Categories [electronic only] 23 (2010), pp. 251–260 (cit. on p. 19).

[ČS24] K. Česnavičius and P. Scholze. "Purity for flat cohomology". In: Annals of Mathematics 199.1 (2024), pp. 51–180 (cit. on p. 18).

[Dec24] T. Decru. "Radical Vélu N-Isogeny Formulae". In: Annual International Cryptology Conference (Eurocrypt 2024). Springer. 2024, pp. 107–128 (cit. on p. 48).

[LRZZ25] J. Lin, D. Robert, C.-A. Zhao, and Y. Zheng. "Biextensions in pairing-based cryptography". Accepted for publication at Designs, Codes and Cryptography. Oct. 2025 (cit. on p. 51).

[PRRSS25] G. Pope, K. Reijnders, D. Robert, A. Sferlazza, and B. Smith. "Simpler and Faster Pairings from the Montgomery Ladder". Accepted for publication at IACR Communications in Cryptology (CiC). Apr. 2025 (cit. on p. 51).

[YOOKN25] R. Yoshizumi, H. Onuki, R. Ohashi, M. Kudo, and K. Nuida. "Efficient theta-based algorithms for computing (ℓ, ℓ)-isogenies on Kummer surfaces for arbitrary odd ℓ". In: International Conference on Post-Quantum Cryptography. Springer. 2025, pp. 3–37 (cit. on p. 47).