Cubical arithmetic: an introduction

2025/09/11 — Leuven Isogeny Days

Damien Robert

Équipe Canari, Inria Bordeaux Sud-Ouest

Every talk needs at least one joke

1. Those who know how to do it, **do it**.
2. Those who don't, **teach it**.
3. Those who can't even teach, **teach teaching**.

Every talk needs at least one joke

1. Those who know how to do cryptography, **do protocols**.
2. Those who don't, **find algorithms**.
3. Those who can't even find algorithms give a tutorial on cubical arithmetic…

Every talk needs at least one joke

1. Those who know how to do cryptography, **do protocols**.
2. Those who don't, **find algorithms**. ⇐ This was me in my PhD.
3. Those who can't even find algorithms give a tutorial on cubical arithmetic... ⇐ This is me now.

Every talk needs at least one joke

This is me in 20 years:

Back in my day, we used to learn about theta functions directly from Mumford's On the equations defining abelian varieties!

(Back In My Day Meme)

History

- Mumford defines the notion of biextensions in [Mum69]
- Grothendieck gives a detailed study of biextensions in [Gro72, pp. VII, VIII]. Key tool for his proof of the semistable reduction theorem.
- Breen defines symmetric biextensions and cubical torsor structures in [Bre83]
- Moret-Bailly (implicitely) introduces multi-extension and hypercube structures in [Mor85]

- Biextensions are well known by mathematicians (cubical structures slightly less so)
- Example: Edixhoven and Lido reinterpretation of quadratic Chabauty via the Poincaré biextension [EL23].
- Biextensions and cubical structures are also useful in the theory of p-adic heights Moret-Bailly, Pazuki, …

- Not used in cryptography…
- Except by Stange: elliptic nets gives the Poincaré biextension cocycle on elliptic curves [Sta08, Chapters 14-15]
- This gives a conceptual link between elliptic nets and pairings. But this result is **hidden** in her PhD…

- R.: cubical arithmetic for cryptography [Rob24]
- Reinterpretation of elliptic nets and "affine lifts of theta null points" as different ways of computing the cubical arithmetic
- See [PRRSS25, Appendix] for a down to earth introduction to cubical arithmetic.

Table of Contents

Elliptic Curves / Abelian varieties

- An abelian variety A is an arithmetic and geometric object.
- Elliptic curve cryptography only relies on the arithmetic:
  $E(\mathbb{F}_q)$ is a finite commutative group
- But this group law comes from geometry

Corollary

- *Compact representations*
- *Efficient formulas*
- *Different models (curves equations, points representationss)*
- *Twists (⇒ work in smaller fields)*
- *Automorphisms, Endomorphisms, Frobenius to speed up the scalar multiplication*
- *The cohomological bazooka (point counting)*

- N.B.: Isogenies are geometric group morphisms
- A geometric map $\phi : A \to B$ is already a group morphism (up to a translation)

Arithmetic beyond the group law: pairings

- There is a richer arithmetic on A than just the addition law: pairings
- Weil pairings:
$$e_\ell : A[\ell] \times \widehat{A}[\ell] \to \mu_\ell$$
- Polarised Weil pairings:
$$e_{\mathcal{L},\ell} : A[\ell] \times A[\ell] \to \mu_\ell,$$
where $\phi_{\mathcal{L}} : A \to \widehat{A}$ is a polarisation.

Question 1: is there a geometric structure underlying pairings?

Biextensions

- A biextension $Y \to A \times B$ is a geometric object above $A \times B$ (a $\mathbb{G}_m$-torsor)

It has a biextension arithmetic structure:

- Each slice $Y \mid A \times \{Q\}$ is a commutative group: an extension of A by $\mathbb{G}_m$
- Likewise for the slices $Y \mid \{P\} \times B$
- These partial group laws are compatible with each other

- Pairings arise naturally from the biextension arithmetic, via monodromy (Grothendieck for the Weil pairing, Stange for the Tate pairing)

- Poincaré biextension: $Y \to A \times \widehat{A}$
- Polarised biextensions: $Y_{\mathcal{L}} \to A \times A$

Algorithmic consequences

- To compute pairings we just need biextension exponentiations (two for the Weil pairing, one for the Tate pairing)

Corollary

- *Double and add*
- *Biextension twists to work with smaller fields*
- *Automorphisms / Frobenius to speed up these exponentiations*

- These algorithmic improvements were already known (Miller's algorithm, twisted pairings, Ate/optimal ate pairings…)
- But the arithmetico-geometric point of view gives more conceptual/simplified arguments [LRZZ25]

- New: other models for biextensions?
- Miller's algorithm is double and add in a specific representation of biextension elements. Are there different models giving faster formulas?

- N.B.: every automorphism of A extends uniquely to $Y_{\mathcal{L}}$: $\mathrm{Aut}(Y_{\mathcal{L}}) = \mathrm{Aut}(A)$.

$\Rightarrow$ There are no "pure" biextension automorphisms.

$\Rightarrow$ Biextension twists are induced by the twists of A

Biextensions in practice

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:

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

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

- Similar formulas for $g_{P,Q_1} \star_2 g_{P,Q_2}$
- Compatibility:

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

Biextensions in practice

For a polarised abelian variety $(A, \mathcal{L})$, $Y_{\mathcal{L}}$ the biextension associated to $\mathcal{L}$ above $A \times A$:

- Theorem of the square: $\mathcal{L}_{P+Q} \otimes \mathcal{L} \simeq \mathcal{L}_P \otimes \mathcal{L}_Q$
- An element of $Y_{\mathcal{L}}$ is a choice of isomorphism
- Biextension arithmetic = arithmetic of the isomorphisms of the theorem of the square

For more on biextensions, see Stange's invited talks at ANTS 2024 and AGCT 2025.

Table of Contents

Polarisations

- In practice we work with (principally) polarised abelian varieties $(A, \phi_{\mathcal{L}})$
- The polarisation $\phi_{\mathcal{L}} : A \to \widehat{A}$ is induced by an (ample) line bundle $\mathcal{L}$
- Two algebraically equivalent line bundles $\mathcal{L} \sim \mathcal{L}'$ give the same polarisation $\phi_{\mathcal{L}}$
  If $\mathcal{L}$ is ample (or just non degenerate), $\mathcal{L} \sim \mathcal{L}' \Leftrightarrow \mathcal{L}' = t_P^* \mathcal{L}$

- $\mathcal{L}$ is a geometric object
- It gives coordinates on A, hence projective embeddings $A \hookrightarrow \mathbb{P}^N$ (if $\mathcal{L}$ is very ample)

Example

The same abelian surface A can be a product of two elliptic curves or a Jacobian of a genus 2 hyperelliptic curve depending on the principal polarisation

Question 2: is there an arithmetic structure on $\mathcal{L}$, lifting the arithmetic on A?

Arithmetic from line bundles?

Question 2: is there an arithmetic structure on $\mathcal{L}$, lifting the arithmetic on A?

- Obviously, $\mathcal{L}$ gives the pairings $e_{\mathcal{L},\ell}$!
- And isotropy of a kernel $K \subset A[\ell]$ for the Weil pairing $e_{\mathcal{L},\ell}$ is an important condition to get a polarised isogeny $\phi : (A, \mathcal{L}^\ell) \to (B, \mathcal{M})$

- But the "true" geometric object behind these pairings is the biextension $\Upsilon_{\mathcal{L}}$
- And indeed, $\mathcal{L}$ induces $\Upsilon_{\mathcal{L}}$ via the line bundle

$$m^* \mathcal{L} \otimes \epsilon^* \mathcal{L} \otimes \pi_1^* \mathcal{L}^{-1} \otimes \pi_2^* \mathcal{L}^{-1},$$

  where $m : A \times A \to A$ is the addition law, $\pi_i : A \times A \to A$ are the projections, and $\epsilon : A \times A \to A$ is the constant 0_A.

- The biextension arithmetic is an arithmetic above $A \times A$
- Is there an arithmetic directly above A?

Line bundles

A is smooth, hence the following are equivalent:

- A Weil divisor Θ_A on A, up to linear equivalence
- A Cartier divisor on A, i.e. a section of $K(A)/O_A$
- An invertible sheaf $\mathscr{L}$ on A, i.e. a sheaf locally isomorphic to O_A.
- A line bundle $\widetilde{X}_{\mathscr{L}}$ on A, i.e a space $\widetilde{X}_{\mathscr{L}} \to A$ locally isomorphic to $A \times \mathbb{A}^1 \to A$
- A $\mathbb{G}_m$-torsor $\mathfrak{L}$ on A. Its total space is $X_{\mathscr{L}} = \widetilde{X}_{\mathscr{L}} \setminus 0$
- A map $A \to B\mathbb{G}_m$, where $B\mathbb{G}_m = [k/\mathbb{G}_m]$ is the moduli stack of $\mathbb{G}_m$-torsors

To D we associate the invertible sheaf $O_A(-D)$. Conversely an invertible sheaf $\mathscr{L}$ has a meromorphic section, which gives a divisor D. $\widetilde{X}_{\mathscr{L}}$ is the total space of $\mathscr{L}$, $\mathscr{L}$ is the sheaf of sections of $\widetilde{X}_{\mathscr{L}} \to A$. The torsor $\mathfrak{L}$ is the isom-sheaf $\mathrm{Isom}(O_A, \mathscr{L})$, conversely $\mathscr{L} = O_A \times_{\mathbb{G}_m} \mathfrak{L}$.
Locally means for the Zariski, étale, fppf or fpqc topology (by Hilbert 90).

Cubical points

- 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 are of the form $\lambda \widetilde{P}$ for $\lambda \in \mathbb{G}_m$
- If $\mathcal{L}$ is very ample, and $X_0, \dots X_N \in \Gamma(A, \mathcal{L})$ is a basis of sections, we have a commutative diagram

$$\begin{tikzcd} X_{\mathcal{L}} \arrow[r, hook] \arrow[d] & \mathbb{A}^{N+1} \setminus \{(0, \dots, 0)\} \arrow[d] \\ A \arrow[r, hook] & \mathbb{P}^N \end{tikzcd}$$

- 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 $\mathcal{L}$ is not very ample, as long as P is not a base point of $\mathcal{L}$

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

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.

- 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.

- 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) $\frac{Z_1}{x/y}(\tilde{0}_E) = 1$.

☹ I am normalising P by fixing $Z(P) = 1$

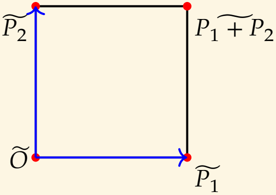
☺ I am rigidifying my étale $\mathbb{G}_m$-torsor at P!

(Drake Hotline Bling meme)

Cubical arithmetic: a degenerate case

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

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



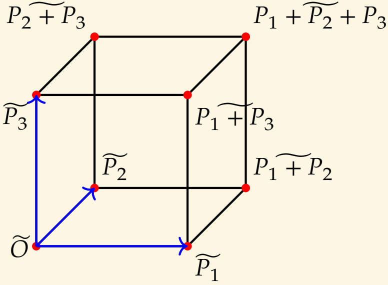
- $\widetilde{P_1 + P_2}$ is uniquely determined by $\widetilde{P_1}, \widetilde{P_2}$ (and $\widetilde{O}$)
- The squared structure also determines $-\widetilde{P}$

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
  $\mathscr{L}_{P_1+P_2+P_3} \otimes \mathscr{L}_{P_1} \otimes \mathscr{L}_{P_2} \otimes \mathscr{L}_{P_3} \simeq \mathscr{L} \otimes \mathscr{L}_{P_2+P_3} \otimes \mathscr{L}_{P_1+P_3} \otimes \mathscr{L}_{P_1+P_2}$
- Given $Z \in \Gamma(A, \mathscr{L})$ with associated divisor D, the isomorphism comes from a function cub_D:

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

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: $y^2 = x^3 + Ax^2 + x$)

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

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!

Complex abelian varieties

- $A = \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$ a principally polarised complex abelian variety, Θ_Ω the principal polarisation associated to Ω
- The addition law on A lifts to the addition law on $(\mathbb{C}^g, +)$

- Basis of $\Gamma(A, n\Theta_\Omega)$: the analytic theta functions $\theta_i(z_P, \Omega/n), i \in \mathbb{Z}^g/n\mathbb{Z}^g$
- $P \in A$ is represented by the projective coordinates $(\theta_i(P))$
- If $z_P \in \mathbb{C}^g$ is above P, we can represent z_P by the affine coordinates $(\theta_i(z_P))$.
- A choice of $z_P \Rightarrow$ a choice of cubical point $\widetilde{P}$

- Knowing $(\theta_i(z_1)), (\theta_i(z_2))$ does not allow to find $\theta_i(z_1 + z_2)$.
- But if we have an analytic cube $0, z_1, z_2, z_3, z_2 + z_3, z_1 + z_3, z_1 + z_2, z_1 + z_2 + z_3$, the knowledge ou the $(\theta_i(z_j)), (\theta_i(z_j + z_k))$ is enough to recover the coordinates $(\theta_i(z_1 + z_2 + z_3))$: this is precisely the cubical law!
- Explicit cubical formulas: Riemann relations (for analytic or algebraic theta functions)

- Cubical structure = algebraic consequences of our analytic structure

We have an exact sequence $0 \to \Lambda \to \mathbb{C}^g \xrightarrow{\pi} A \to 0$, and the cubical structure on $\pi^*\mathcal{L}$ is trivial over $\mathbb{C}^g$. The theory of descents of cubical structures of [Bre83, Proposition 3.10] gives an algebraic construction of theta functions, which gives an alternative to Mumford's construction via the theta group action.

Polarised biextensions from the Poincaré biextension

- Canonical Poincaré biextension $\mathcal{Y} \to A \times \widehat{A}$
- $Q \in \widehat{A} \mapsto \mathcal{Y} \mid A \times \{Q\} \in \mathrm{Ext}^1(A, \mathbb{G}_m)$ is an isomorphism:
  $\widehat{A} = \mathrm{Hom}(A, B\mathbb{G}_m) \simeq \mathrm{Ext}^1(A, \mathbb{G}_m)$

- $\mathcal{Y}_{\mathcal{L}}$ is the pullback of the Poincaré biextension $\mathcal{Y} \to A \times \widehat{A}$ by $\mathrm{Id} \times \phi_{\mathcal{L}}$
- It only depends on the polarisation $\phi_{\mathcal{L}}$, i.e. the algebraic class of $\mathcal{L} \in NS(A)$
- There is a unique biextension structure on $\mathcal{Y}_{\mathcal{L}}$ Grothendieck

Extra technical details

Theta groups

- Two kind of theta groups: commutative and non commutative

- If $\mathcal{M} \in \mathrm{Pic}^0(A)$ is algebraically equivalent to 0, $G(\mathcal{M})$ is a commutative theta group: an extension of A by $\mathbb{G}_m$
- If $\mathcal{M}$ corresponds to $Q \in \widehat{A}$, $G(\mathcal{M})$ is precisely the slice $Y \mid A \times \{Q\}$ of the Poincaré biextension

- If $\mathcal{L}$ is ample, $G(\mathcal{L})$ is a non commutative extension of $K(\mathcal{L}) := \mathrm{Ker}\, \phi_{\mathcal{L}} \subset A$ by $\mathbb{G}_m$
- $G(\mathcal{L})$ is the arithmetico-geometric structure classifying the descents of $\mathcal{L}$ to isogeneous abelian varieties $A \to B$
- There is an action of $G(\mathcal{L})$ on $\Gamma(\mathcal{L})$ lifting the translation action by $K(\mathcal{L})$ on A
- The Weil pairing $e_{\mathcal{L},\ell}$ is the commutator pairing on $G(\mathcal{L}^\ell)$

- A symmetric theta structure is a choice of symplectic basis on $K(\mathcal{L})$ and of rigidifications of μ_2-torsors (given by suitable 2-Tate pairings) associated to this basis.

$\Rightarrow$ Compatibility of symmetric theta structures with isogenies

Cubical arithmetic

- $X_{\mathcal{L}} \to A$ depends on the isomorphism class of $\mathcal{L}$
- There is a unique cubical structure on $X_{\mathcal{L}}$ Breen
- The biextension $Y_{\mathcal{L}}$ comes from the line bundle $m^* \mathcal{L} \otimes \epsilon^* \mathcal{L} \otimes \pi_1^* \mathcal{L}^{-1} \otimes \pi_2^* \mathcal{L}^{-1}$

- $Y_{\mathcal{L}}$ is trivial on $A \times K(\mathcal{L}) = \mathrm{Ker}\, \phi_{\mathcal{L}}$ (since $\phi_{\mathcal{L}} = 0$ on $K(\mathcal{L})$)
- This formally defines the theta group $G(\mathcal{L})$ and its action on $\Gamma(\mathcal{L})$
- The cubical point of view unifies biextensions and both flavors of theta groups

$\Rightarrow$ Cubical arithmetic induces the biextension arithmetic and the theta group arithmetic along with its action on sections.

$\Rightarrow$ There is a well defined cubical translation for cubical points $\widetilde{P}$ above $P \in K(\mathcal{L})$.

$\Rightarrow$ We can define a symmetric theta structure in term of choices of suitable cubical points $\widetilde{P}$ above a basis of $K(\mathcal{L})$

Table of Contents

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 $Y_{\mathcal{L}} \to A \times A$
- 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 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

- $Z \in \Gamma(A, \mathcal{L})$ 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`

Perspectives

- Find cubical formulas in more models
- Currently: cubical arithmetic in level-1 on elliptic curves (in the Weierstrass model), and level-n cubical arithmetic on abelian varieties via level-n theta functions (n even)
- **Question**: level-1 cubical arithmetic on more models? E.g.:
  - Jacobians / Jacobians of hyperelliptic curves?
  - Level-2 theta models?
    (This would allow to extend the ThetaCGL hash function [KMM+25] to any dimension)

- Stange sesquilinear biextensions, which give sesquilinear pairings [Sta24]
- **Question**: sesquilinear cubical arithmetic?

- Isogeny formulas for $\phi : (A, \mathcal{L}^\ell) \to (B, \mathcal{M})$ allow to move between the symmetric biextensions $\Upsilon_{\mathcal{M}} \to B \times B$, $\Upsilon_{\mathcal{L}^\ell} \to A \times A$, and the non symmetric biextension $\Upsilon_\phi \to A \times B$
- Isogenies lift to cubical isogenies
- **Question**: algorithmic applications?

- **Question**: New insights on ECC DLPs?

Cryptography from biextensions?

- $Y \to E \times E$ the biextension associated to (0_E)
- Can be seen as a family of commutative groups $G_Q := Y \mid E \times \{Q\}$ (extensions of E by $\mathbb{G}_m$), parametrised by points $Q \in E$
- The biextension arithmetic induces group morphisms $G_{Q_1} \times_E G_{Q_2} \to G_{Q_1+Q_2}$
- The action by $\mathbb{G}_m$ on Y and a choice of rigidification of $Y \mid \{0_E\} \times \{0_E\}$ induces compatible canonical isomorphisms $G_{0_E} \simeq E \times \mathbb{G}_m$ and $G_Q \mid \{0_E\} \simeq \mathbb{G}_m$

- **Question**: can we exploit this cryptographically?

Hypercube structures

The analogies:

- Squared structure = group extension of A by $\mathbb{G}_m \simeq$ linear map $A \to \mathbb{G}_m$
- Biextension of $A_1 \times A_2$ by $\mathbb{G}_m \simeq$ bilinear map $A_1 \times A_2 \to \mathbb{G}_m$
- Cubical structure on A by $\mathbb{G}_m \simeq$ quadratic map $A \to \mathbb{G}_m$

extend to higher degree Moret-Bailly:

- 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.

Question: is there a natural geometric object that has a $(n+1)$-hypercube structure, $n > 2$?

Bibliography

[Bre83] L. Breen. Fonctions thêta et théoreme du cube. Vol. 980. Springer, 1983 (cit. on pp. 6, 27).

[Dec24] T. Decru. "Radical Vélu N-Isogeny Formulae". In: Annual International Cryptology Conference (Eurocrypt). Springer. 2024, pp. 107–128 (cit. on p. 35).

[EL23] B. Edixhoven and G. Lido. "Geometric quadratic Chabauty". In: Journal of the Institute of Mathematics of Jussieu 22.1 (2023), pp. 279–333 (cit. on p. 6).

[Gro72] A. Grothendieck. Groupes de Monodromie en Géométrie Algébrique (SGA 7). Séminaire de Géométrie Algébrique du Bois Marie - 1967–69. Vol. 288. Lecture Notes in Mathematics. Springer-Verlag, 1972 (cit. on p. 6).

[KMM+25] S. Kunzweiler, L. Maino, T. Moriya, C. Petit, G. Pope, D. Robert, M. Stopar, and Y. B. Ti. "Radical 2-isogenies and cryptographic hash functions in dimensions 1, 2 and 3". In: Public-Key Cryptography – PKC 2025. Vol. 15676, Lecture Notes in Computer Science. Springer, May 2025, pp. 265–299. doi: https://doi.org/10.1007/978-3-031-91826-1_9 (cit. on p. 40).

[LRZZ25] J. Lin, D. Robert, C.-A. Zhao, and Y. Zheng. "Biextensions in pairing-based cryptography". Apr. 2025 (cit. on pp. 11, 38).

[Mor85] L. Moret-Bailly. Pinceaux de variétés abéliennes. Société mathématique de France, 1985 (cit. on p. 6).

[Mum69] D. Mumford. "Bi-extensions of formal groups". In: Algebraic geometry 307-322 (1969) (cit. on p. 6).

[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 pp. 6, 38).

[Rob24] D. Robert. "Fast pairings via biextensions and cubical arithmetic". Apr. 2024 (cit. on p. 6).

[Sta08] K. Stange. "Elliptic nets and elliptic curves". PhD thesis. Brown University, 2008. url: https://repository.library.brown.edu/studio/item/bdr:309/PDF/ (cit. on p. 6).

[Sta24] K. E. Stange. "Sesquilinear pairings on elliptic curves". In: arXiv preprint arXiv:2405.14167 (2024) (cit. on p. 40).

[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. 34).