

Cubical arithmetic on abelian varieties: introduction and applications

2025/02/06 — Biextension reading group

Damien Robert

Équipe Canari, Inria Bordeaux Sud-Ouest



université
de BORDEAUX

Inria

Table of Contents

- 1 Cubical arithmetic
- 2 Constructing functions with prescribed divisors, applications to pairings
- 3 Computing isogenies
- 4 Isogeny preimages, and radical isogenies
- 5 The monodromy leak
- 6 Perspectives

References

- [Gro72] Grothendieck, Groupes de Monodromie en Géométrie Algébrique (SGA 7) (1972) VII, VIII. Biextensions
 - [Bre83] Breen, Fonctions thêta et théoreme du cube (1983)
Symmetric biextensions and cubical torsor structures
 - [Mor85] Moret-Bailly, Pinceaux de variétés abéliennes (1985)
Cubical torsor structures
-
- 😊 Breen's introduction gives a very nice high level overview
 - 😞 Very abstract (the case of a bitorsor on an arbitrary topos...)
 - 😞 Not a single explicit formula
-
- **This talk:** a “gentle introduction” to cubical arithmetic
 - **Algorithmic applications:** from explicit cubical formulas on a model we obtain pairings and isogeny formulas!
 - More details in [Rob24]

Cubical structure associated to a divisor

- A/k a commutative algebraic group, D a divisor on A .
- $p_i : A^3 \rightarrow A$ the projections, $p_{ij} := p_i + p_j$,
 $p_{123} := p_1 + p_2 + p_3 : (P_1, P_2, P_3) \mapsto P_1 + P_2 + P_3$.

Definition (Cubical structure)

A cubical structure on D is a rational function g_D on A^3 such that:

- g_D has for divisor $p_{123}^*D - p_{12}^*D - p_{13}^*D - p_{23}^*D + p_1^*D + p_2^*D + p_3^*D$;
- Neutral point: $g_D(0, 0, 0) = 1$.
- Commutativity: For all $\sigma \in \mathfrak{S}_3$, $g_D(\sigma(P_1, P_2, P_3)) = g_D(P_1, P_2, P_3)$.
- Associativity:

$$g_D(P_1 + P_2, P_3, P_4)g_D(P_1, P_2, P_4) = g_D(P_1, P_2 + P_3, P_4)g_D(P_2, P_3, P_4).$$

Example

The trivial cubical structure: $D = 0$ and $g_D = 1$.

We will use symmetric cubical structures [Bre83, § 5]: D a symmetric divisor, $g_D(P_1, P_2, -P_1 - P_2) = 1$.

Cubical points and cubical arithmetic

- \mathcal{L} line bundle, $Z \in \Gamma(\mathcal{L})$ a section, D the divisor of zeroes of Z
- A **cubical point** \widetilde{P} above a point $P \in A$ is a choice of coordinate $Z(\widetilde{P}) \in \mathbb{G}_m(k) = k^*$
(This assumes that P is neither a pole or zero of Z)

Definition (Cubical arithmetic)

Given a cube $0, P_1, P_2, P_3, P_2 + P_3, P_1 + P_3, P_1 + P_2, P_1 + P_2 + P_3$, a choice of 7 out of 8 cubical points determine the 8th one via

$$\frac{Z(P_1 + \widetilde{P_2} + P_3)Z(\widetilde{P_1})Z(\widetilde{P_2})Z(\widetilde{P_3})}{Z(\widetilde{0})Z(\widetilde{P_2 + P_3})Z(\widetilde{P_1 + P_3})Z(\widetilde{P_1 + P_2})} = g_D(P_1, P_2, P_3)$$

Example

- **Differential additions:** $0, P, Q, -Q, 0, P - Q, P + Q, P$
 $\Rightarrow \widetilde{P + Q}$ from $\widetilde{P}, \widetilde{Q}, \widetilde{P - Q}$
- **Doublings:** $2\widetilde{P}$ from \widetilde{P} (special case of a differential addition with $\widetilde{Q} = \widetilde{P}$).


- We can also use **translated cubes**:

$$\frac{Z(R + P_1 + P_2 + P_3)Z(R + P_1)Z(R + P_2)Z(R + P_3)}{Z(\tilde{R})Z(R + P_2 + P_3)Z(R + P_1 + P_3)Z(R + P_1 + P_2)} = \frac{g_D(P_1, P_2, P_3 + R)}{g_D(P_1, P_3, R)}$$

- 8 points $P_1, P_2, P_3, P_4; P'_1, P'_2, P'_3, P'_4$ are part of a translated cube iff there exists Q such that

$$P_1 + P_2 + P_3 + P_4 = 2Q \text{ and } P'_i = Q - P_i.$$

(Then the P_i are in the numerator and the P'_i in the denominator in the above formula.)

-  The general function $g_{D, P_1, P_2, P_3}(R)$ given for a translated cube in [Rob24] is wrong: it has the correct divisor but is not normalised correctly. The explicit formulas in that paper are correct (at least the implementation gives the correct results!)

Multiscalar exponentiations

- Consider an m -dimensional **hypercube** generated by $0, P_1, P_2, \dots, P_m$
- Assume that cubical points have been chosen for all **squares** $\tilde{0}, \tilde{P}_i, \tilde{P}_j, \widetilde{P_i + P_j}$
- Then we can use cubes to fill out the hypercube and obtain $P_1 + \widetilde{\cdot} + P_m$
- More generally using cubes we can compute $n_1 P_1 + \widetilde{\cdot} + n_m P_m$ for all $n_i \in \mathbb{Z}$.

Proposition

The resulting cubical point $\sum n_i \tilde{P}_i$ does not depend on the choice of intermediate cubes used.

Proof.

By the commutativity and associativity assumptions on g_D . □

- Cubical multidimensional ladder: $O_m(\log \max n_i)$
- **Homogeneity:** $\tilde{P}_i \mapsto \lambda_i \star \tilde{P}_i, \widetilde{P_i + P_j} \mapsto \lambda_{ij} \star \widetilde{P_i + P_j}$,

$$\sum n_i \tilde{P}_i \mapsto \prod_i \lambda_i^{n_i^2} \prod_{i < j} \lambda_{ij}^{n_i n_j} \star \sum n_i \tilde{P}_i$$

Cubical arithmetic on abelian varieties

Theorem (Grothendieck, Breen)

If A/k is an abelian variety, then for every divisor D there is a unique (once $\widetilde{\mathcal{O}}_A$ is fixed) cubical structure on D . This cubical structure is symmetric if D is symmetric.

Proof.

Cohomological arguments and the fact that A has no non constant global sections.

Explicit construction of g_D :

$$g_D(P_1, P_2, P_3) = \frac{g_{D, P_1, P_2}(P_3)}{g_{D, P_1, P_2}(0)}$$

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

Corollary

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

- $g_{D, P_1, P_2}(P_3) = g_{D, P_2, P_3}(P_1) = g_{D, P_3, P_1}(P_2)$ (commutativity)
- $g_{D, P_1+P_2, P_3} g_{D, P_1, P_2} = g_{D, P_1, P_2+P_3} g_{D, P_2, P_3}$ (associativity).

Representing cubical points and extra arithmetic

- If (X_1, \dots, X_m) are a basis of $\Gamma(\mathcal{L})$, then $Z(\tilde{P})$ determines $X_i(\tilde{P})$ via $X_i(\tilde{P}) = x_i(P)Z(\tilde{P})$ where $x_i = X_i/Z$ is a function on A .
- A choice of cubical point is thus a choice of **affine coordinates** $(X_1(\tilde{P}), \dots, X_m(\tilde{P}))$ above the **projective coordinates** $(X_1(P) : \dots : X_m(P))$ of P
This allows to define \tilde{P} whenever P is not a base point of D
- **Inversion:** If \mathcal{L} is symmetric, a (symmetric) cubical structure also determines $-\tilde{P}$ from \tilde{P}
- **Translation by a point T of n -torsion:** If $D = n\Theta_A, \Theta_A$ a principal polarisation (we will say D is of level n), then we also have a **translation map** $M_{\tilde{T}} : \tilde{P} \mapsto \widetilde{P + T}$.
- $M_{\tilde{T}}$ is linear in the X_i and only depends on the choice of \tilde{T} .
- [Mor85, § 3, § 4]: The biextension associated to the cubical structure is trivial when restricted to $A[n] \times A$, from which we recover the theta group $G(D)$ and its linear action on $\Gamma(D)$

Analytic cubical points

- Let $A = \mathbb{C}^g / (\mathbb{Z}^g + \Omega \mathbb{Z}^g)$ a principally polarised complex abelian variety;
- The addition law on A lifts to the addition law on $(\mathbb{C}^g, +)$
- The analytic period matrix Ω defines a canonical level structure on $A[n]$ for all n (in a compatible way)
- Let Θ_Ω be the principal polarisation associated to Ω , and $D = n\Theta_\Omega$.
Basis of $\Gamma(A, D)$: the analytic theta functions $\theta_i(z_P, \Omega/n)$
- $P \in A$ 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 \check{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 on 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!
- Multiexponentiation: recover the $\theta_i(\sum_j n_j z_j)$.
- Explicit cubical formulas: Riemann relations (for analytic or algebraic theta functions)
- Cubical structure = algebraic consequences of our analytic structure

Elliptic curves (level 1)

- Level 1: $D = (0_E), Z_1$ with a zero of order 1 at $O = 0_E$.
- Cubical point: $\tilde{P} = (P, Z_1(\tilde{P}))$.
- $Z_1(0_E) = 0$. \tilde{O} defined by $(Z/(x/y))(\tilde{O}) = 1$.
- $g_{(0_E)}(P_1, P_2, P_3) = \frac{l_{P_1, P_2}(P_3)}{(x(P_3) - x(P_1))(x(P_3) - x(P_2))} = \frac{x(P_1 + P_2) - x(P_3)}{l_{P_1, P_2}(-P_3)}$
- Differential addition: $Z_1(\widetilde{P+Q})Z_1(\widetilde{P-Q}) = Z_1(\tilde{P})^2 Z_1(\tilde{Q})^2 (x(Q) - x(P))$
- Doubling: $Z_1(2\tilde{P}) = Z(\tilde{P})^4 2y(P)$
- Inverse: $Z_1(-\tilde{P}) = -Z_1(\tilde{P})$.

Example

Let $P = (x(P), y(P))$, $Z_1(\tilde{P}) = 1$. Then $Z_1(n\tilde{P}) = \psi_n(P)$, ψ_n the division polynomial.

And in level 3, if $\tilde{P} = (x(P), y(P), 1)$,

$$n\tilde{P} = (\phi_n(P)\psi_n(P), \omega_n(P), \psi_n^3(P)),$$

with ϕ_n, ω_n the extended division polynomials.

Elliptic curves (level 2)

- Level 2: $D = 2(0_E)$, with sections $X_2, Z_2 = Z_1^2$
- Cubical point: $\tilde{P} = (X_2(\tilde{P}), Z_2(\tilde{P}))$
- $\tilde{O} = (1, 0)$.
- Symmetry: $Z_2(-\tilde{P}) = Z_1^2(-\tilde{P}) = Z_2(\tilde{P})$.

- $g_D = g_{(0_E)}^2$ depends only on the x -coordinates of the $P_i, P_i + P_j$

⇒ Cubical arithmetic in level 2 valid on cubes on the Kummer line $E/\pm 1$.

- N.B.: for x -only arithmetic, knowing $x(P_1), x(P_2), x(P_3), x(P_1 + P_2), x(P_1 + P_3)$ is enough to recover $x(P_2 + P_3), x(P_1 + P_2 + P_3)$ (see [LR16]) so does not quite require the full cube.

Formulas on elliptic curves

Example (Montgomery model in level 2: $y^2 = x^3 + Ax^2 + x$)

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

⇒ The standard Montgomery ladder gives (almost) the cubical ladder $\tilde{P} \mapsto n\tilde{P}$

- $T = (0 : 1)$ 2-torsion, $\tilde{T} = (0, 1)$, $\widetilde{P+T} = (Z_2(\tilde{P}), X_2(\tilde{P}))$.
- Montgomery curves have **very efficient** cubical formulas!

Example (Elliptic nets = cubical arithmetic in level 1 [Stao8])

- Given $\tilde{P}_i, \widetilde{P_i + P_j}$, the elliptic net $W(n_1, \dots, n_m)$ is simply $Z_1(\sum n_i \tilde{P}_i)$
- Amazingly, knowing sufficiently many of these Z_1 is enough to recover all of them (via the elliptic net recurrence relation)

Summary

- Cubical point \tilde{P} = point P with additional marking (in \mathbb{G}_m)
 - Cubical arithmetic: coherent way to keep track of this marking
- ⇒ New algorithmic tools!

Going further

- The “correct point of view” is that of cubical isomorphisms of fppf-torsors (this makes the cubical arithmetic well defined on any point)
- Cubical point \tilde{P} = choice of rigidification of our torsor at P ; cubical coordinates = encoding of this rigidification
- Moret-Bailly: “au royaume des torseurs, il n’y a pas de signe”
Contrast this with the sign ambiguity inherent in the Weil pairing, even [Gro72] has sign mistakes!
- Grothendieck-Breen’s theorem holds for abelian schemes A/S and semi-abelian schemes (and more) over a normal base: equivalence of categories between cubical torsors and rigidified torsors
- Allows to study degenerations of abelian varieties
- Cubical arithmetic induces theta group and biextension arithmetic, the algebraic structures behind isogenies and pairings respectively.
- **Universality**: [Bre83, Theorem 8.9]: the cubical structure on \mathcal{L} encodes all the quadratic information associated to the polarisation \mathcal{L}

Table of Contents

- 1 Cubical arithmetic
- 2 Constructing functions with prescribed divisors, applications to pairings
- 3 Computing isogenies
- 4 Isogeny preimages, and radical isogenies
- 5 The monodromy leak
- 6 Perspectives

Cubical functions

- E elliptic curve, $D = (0_E)$
 - $\tilde{R} \mapsto Z(\tilde{R} + \sum n_i \tilde{P}_i)$ is a "function" with divisor $t_{\sum n_i P_i}^* D$.
 - Depends on the choices of $\tilde{P}_i, \widetilde{P_i + P_j}$.
 - But also of $\tilde{R}, \widetilde{R + P_i}$
- ⇒ Not a genuine function. **Cubical function.**
- But combining these cubical functions we can get genuine elliptic functions.

Example

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

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 $\tilde{P}_1, \tilde{P}_2, \widetilde{P_1 + P_2}$.

Cubical functions for pairings

- $P \in E[\ell](k), Q \in E(k)$
- Tate pairing: $f_{\ell,P}((Q) - (0_E))$ with $f_{\ell,P}$ a function of divisor $\ell D - \ell t_P^* D$
- Cubical function: $\tilde{Q} \mapsto \left(\frac{Z(\tilde{Q})}{Z(\widetilde{P+Q})} \right)^\ell$
- Not a genuine function!
- Instead rewrite the divisor as $t_{\ell P} D + (\ell - 1)D - \ell t_P^* D$ and use:

$$f_{\ell,P}(Q) = \frac{Z(\ell\tilde{P} + \tilde{Q})Z(\tilde{Q})^{\ell-1}}{Z(\widetilde{P+Q})^\ell}$$

Theorem

- The Tate pairing is given by

$$e_{T,\ell}(P, Q) = \frac{Z(\ell\tilde{P} + \tilde{Q})}{Z(\ell\tilde{P})} \left(\frac{Z(\tilde{P})Z(\tilde{Q})}{Z(\widetilde{P+Q})Z(\tilde{O})} \right)^\ell$$

- The Weil pairing is given by

$$e_{W,\ell}(P, Q) = \frac{Z(\ell\tilde{P} + \tilde{Q})Z(\ell\tilde{Q})}{Z(\ell\tilde{P})Z(\ell\tilde{Q} + \tilde{P})}$$

Double and add algorithm

- We can normalize our functions by setting $Z(P \widetilde{+} Q) = Z(\tilde{P}) = Z(\tilde{Q}) = 1$
- $f_{m,P}((Q) - (0)) = \frac{Z(m\tilde{P} + \tilde{Q})}{Z(m\tilde{P})}$
- Double and add: $\frac{Z((m_1+m_2)\tilde{P} + \tilde{Q})}{Z((m_1+m_2)\tilde{P})} = \frac{Z(m_1\tilde{P} + \tilde{Q})}{Z(m_1\tilde{P})} \cdot \frac{Z(m_2\tilde{P} + \tilde{Q})}{Z(m_2\tilde{P})} \cdot \frac{Z((m_1+m_2)\tilde{P} + \tilde{Q})Z(\tilde{Q})}{Z((m_1\tilde{P} + \tilde{Q})Z(m_2\tilde{P} + \tilde{Q}))}$
- We recover the double and add formula for Miller's algorithm:

$$f_{m_1+m_2,P}(Q) = f_{m_1,P}(Q)f_{m_2,P}(Q)g_{D,m_1P,m_2P}(Q).$$

- The cubical arithmetic allows to compute $Z(m\tilde{P} + \tilde{Q})$ and $Z(m\tilde{P})$ separately!
- Much more flexible!
- These are not genuine functions, so not defined using only x, y coordinates!

Alternate formulas for the Weil pairing

- If $h_{\ell,P}$ is a function with divisor $[\ell]^*(D - t_P^*D)$, then the (original definition of the) Weil pairing $e_{W,\ell}(P, Q)$ is given by $h_{\ell,P}(Q + R)/h_{\ell,P}(R)$ for any point R
- Cubical function $\tilde{R} \mapsto Z(\ell\tilde{R})/Z(\ell\tilde{R} + \tilde{P})$
- Keeping track of the projective factors, we see that we can build the genuine $h_{\ell,P}$ as

$$h_{\ell,P}(R) = \frac{Z(\ell\tilde{R})Z(\ell\tilde{P} + \tilde{R})}{Z(\ell\tilde{R} + \tilde{P})Z(\tilde{R})}$$

- Using this Weil pairing alternate formula with $R = 0$, we find again

$$e_{W,\ell}(P, Q) = \frac{Z(\ell\tilde{P} + \tilde{Q})Z(\ell\tilde{Q})}{Z(\ell\tilde{P})Z(\ell\tilde{Q} + \tilde{P})}$$

- Notice how we can compute $h_{\ell,P}$ efficiently via the cubical ladder! By contrast Miller's algorithm for $h_{\ell,P}$ needs the coordinates of the ℓ -torsion points $T \in E[\ell]$ and of P_0 such that $\ell P_0 = P$; and cannot use a double and add method because the points on the support of the divisor $[\ell]^*(D - t_P^*D) = \sum_{T \in E[\ell]} ((T) - (T - P_0))$ only have multiplicity one.
- Extends to Weil-Cartier pairings $e_\phi(P, Q)$ by using cubical isogeny formulas $\tilde{\phi}$ for ϕ .
- But not clear how to compute $\tilde{\phi}\tilde{P} + \tilde{Q}$ without knowing a preimage $Q_0 \in \phi^{-1}(Q)$ and using $\tilde{\phi}(\tilde{P} + \tilde{Q}_0)$

Summary

- The cubical arithmetic allows us to easily build functions with prescribed divisors
- We can use intermediate cubical functions in our computations, as long as the end result is a genuine elliptic function
- Greater flexibility!
- New insights: Doliskani's probabilistic supersingularity test is a self pairing test: all points on E have trivial self Tate pairing if E is supersingular.
- Faster pairing formulas for Montgomery curves

Going further:

- If P is of ℓ -torsion, and we choose cubical points $\tilde{P}, \tilde{Q}, \widetilde{P+Q}$, we have $\ell\tilde{P} = \lambda_P \star \tilde{O}$, $\ell\tilde{P} + \tilde{Q} = \lambda_{P,Q} \star \tilde{Q}$, with $\lambda_P, \lambda_{P,Q} \neq 1$ in general
- The pairing formulas show that these monodromy values (in \mathbb{G}_m) give the Tate and Weil pairings
- The mathematical framework for the monodromy interpretation of the pairings is Mumford's notion of biextension (see [Gro72; Stao8, Chapter 14])
- [Rob24]: monodromy interpretation of the Ate and optimal Ate pairings on abelian varieties
- Cubical arithmetic induces (and is finer) than biextension arithmetic
- This gives some extra flexibility in our arithmetic for pairing computations: we just need formulas that are valid for the biextension arithmetic, even if they are not valid for the cubical arithmetic.

Table of Contents

- 1 Cubical arithmetic
- 2 Constructing functions with prescribed divisors, applications to pairings
- 3 Computing isogenies
- 4 Isogeny preimages, and radical isogenies
- 5 The monodromy leak
- 6 Perspectives

- $E_1/k : y_1^2 = x_1^3 + ax_1 + b_1$ elliptic curve, $K = \langle T \rangle$ cyclic kernel of order ℓ , $E_2 = E_1/K$
- $x_2(P) := \sum_{i=0}^{\ell-1} (x_1(P + iT) - \sum_{i=1}^{\ell-1} x_1(iT))$
- $y_2(P) := \sum_{i=0}^{\ell-1} (y_1(P + iT) - \sum_{i=1}^{\ell-1} y_1(iT))$
- x_2 has for polar divisor $\sum_{i=0}^{\ell-1} 2(iT)$ and is invariant by the translation by T , hence defines a section of $2(0_{E_2})$ on E_2
- Likewise, y_2 defines a section of $3(0_{E_2})$ on E_2
- The Weierstrass equation between x_2, y_2 can be found by evaluating on a few points or working in the formal group of E_1 .

Vélu's formulas in higher dimension?

- $(A_1, \Theta_{A_1})/k$ ppav of dimension g , $K = \langle T_1, \dots, T_g \rangle \subset A_1[\ell]$ isotropic kernel of rank g ,
 $\phi : A_1 \rightarrow A_2 = A_1/K$
- ϕ is an ℓ -isogeny: $\phi^* \Theta_{A_2} = \ell \Theta_{A_1}$
- $x_1, \dots, x_m \in \Gamma(n\Theta_{A_1})$ system of coordinates of level n on A_1
- $x'_i(P) = \sum_{T \in K} x_i(P + T) + \text{constant}$
- x'_i invariant by translation by $T \in K$, so defines a **coordinate** on A_2
- We just need to evaluate on a few points and recover the equations for A_2 ...
Except this does not seem to work?
- $x_i = X_i/X_0$. Putting everything in the same denominator, the trace x'_i has **degree** ℓ^g on A_1 , so is of degree ℓ^{g-1} on A_2
Here the degree is taken with respect to $n\Theta_{A_1}$ and $n\Theta_{A_2}$ respectively
- More precisely: $\sum_{T \in K} t_T^* n\Theta_{A_1} \sim \ell^g \Theta_{A_1}$
- This divisor is invariant by translation by $T \in K$, so descends to a divisor $\sim \ell^{g-1} n\Theta_{A_2}$ on A_2 , but it is of **too large degree** (unless $g = 1$)

Cubical Vélú's formulas in higher dimension

- Rather than taking a trace of the affine coordinates $x_i = X_i/X_0$, we want to take a trace on the projective coordinates X_i directly
- For instance the trace of X_i^ℓ gives $X'_i(P) = \sum_{T \in K} X_i^\ell(P + T)$.
- This is of **correct degree**!
- But the coordinates $(X_i(P + T))$ are only defined up to projective factors λ_T that depends on $T \in K$!
- The values $X_i^\ell(P + T)$ do not make sense!
- Except it does as a coordinate $X_i^\ell(\widetilde{P + T})$ on a **cubical point**.
- Taking a **cubical trace** works!

Technical details: theta groups and the cubical arithmetic

- We need to build a divisor Θ_ϕ on A_1 such that:
 - ① Θ_ϕ is invariant by translation by K
 - ② $\Theta_\phi \sim \ell n \Theta_{A_1}$
- **Descent theory**: (symmetric) lifts \tilde{K} of K in the theta group $G(\ell n \Theta_{A_1}) \Leftrightarrow$ (symmetric) divisors Θ_ϕ
- Symmetric Θ_ϕ **unique** (up to linear equivalence) if n even and ℓ odd
- [Rob21]: explicit formulas of the action of $G(\ell n \Theta_{A_1})$ on $\Gamma(\ell n \Theta_{A_1})$ allows to take the trace of actions under \tilde{K} and compute the isogeny ϕ
- These explicit formulas exist in the **theta model** [LR12; CR15; LR22]
- [Rob24]: the cubical arithmetic on level n allows to recover the theta group action of level ℓn
- Cubical arithmetic \Rightarrow explicit isogeny formulas

Excellent cubical lifts

Proposition

$T \in A[\ell]$, ℓ odd. \tilde{T} a cubical point above T . TFAE:

- 1 $(\ell j + i)\tilde{T} = i\tilde{T}$ for all $i, j \in \mathbb{Z}$
- 2 $\ell\tilde{T} = \tilde{O}$ and $(\ell + 1)\tilde{T} = \tilde{T}$
- 3 $(\ell' + 1)\tilde{T} = -\ell'\tilde{T}$ for $\ell = 2\ell' + 1$

A point \tilde{T} satisfying these properties is said to be an *excellent cubical lift* of T , there are ℓ of them: if \tilde{T} is excellent then $\zeta \star \tilde{T}$ is too for $\zeta \in \mu_\ell$

- $T \in A[\ell]$, \tilde{T} arbitrary cubical lift
- $\ell\tilde{T} = \lambda_0 \star \tilde{O}$, $(\ell + 1)\tilde{T} = \lambda_0 \lambda_1 \star \tilde{T}$
- $(\ell' + 1)\tilde{T} = \alpha \star -\ell'\tilde{T}$
- $\lambda_1 = e_{T,\ell}(T, T)$ (non reduced Tate pairing)
- $\lambda_0^2 = \lambda_1^\ell$, $\lambda_1 = \alpha^2$, $\lambda_0 = \alpha^\ell$
- The excellent lifts are given by $\gamma \star \tilde{T}$ for $\gamma^\ell = \alpha$

Theta group action from excellent lifts

- If $T \in A[\ell]$, a cubical point \tilde{T} of level n induces a cubical point $\tilde{T}^{\otimes \ell}$ of level $n\ell$, hence an element $g_T \in G(\ell n \Theta_A)$ of the theta group
- \tilde{T} and $\zeta \star \tilde{T}$ induce the same point $\tilde{T}^{\otimes \ell}$ for $\zeta \in \mu_\ell$
- The excellent lifts \tilde{T} all induce the unique symmetric element g_T of order ℓ in $G(\ell n \Theta_A)$
- Excellent lift of K : $\tilde{K} = \langle \tilde{T}^{\otimes \ell} \mid T \in K \rangle$ (subgroup of $G(\ell n \Theta_A)$ since K is isotropic).

Definition

If $P \in A$, $\widetilde{P+T}$ is an excellent lift relative to \tilde{P} and \tilde{T} (for \tilde{T} excellent) if $\tilde{P} + \ell\tilde{T} = \tilde{P}$.
In that case, $\tilde{P} + (j\ell + i)\tilde{T} = \tilde{P} + i\tilde{T}$

- There are ℓ possible relative excellent lifts $\widetilde{P+T}$ that all induce the same point $\widetilde{P+T}^{\otimes \ell}$
- The action of $g_T \in G(\ell n \Theta_A)$ is given by

$$\tilde{T}^{\otimes \ell} \cdot \tilde{P}^{\otimes \ell} = \widetilde{P+T}^{\otimes \ell}$$

- N.B.: if $P, Q \in A[\ell]$, \tilde{P}, \tilde{Q} excellent lift, then one can take $\widetilde{P+Q}$ excellent relative to both (\tilde{Q}, \tilde{P}) and (\tilde{P}, \tilde{Q}) (i.e. $\ell\tilde{P} + \tilde{Q} = \tilde{Q}$ and $\tilde{P} + \ell\tilde{Q} = \tilde{P}$) iff P, Q are isotropic for the Weil pairing.

Cubical isogeny formulas

Theorem

Let $X_i \in \Gamma(n\Theta_{A_1})$. Fix *excellent lifts* \tilde{T} for $T \in K$ and $\widetilde{P+T}$ relative to \tilde{P} .

Then

$$X'_i(P) = \sum_{T \in K} X_i^\ell(\widetilde{P+T})$$

gives a coordinate on $A_2 = A_1/K$.

- Recovering equations for A_2 from the X'_i will depend on the type of *model* we seek
- The action of $G(n\Theta_{A_1})$ on the X_i allows us to recover the action of $G(n\Theta_{A_2})$ on the X'_i (assume $\ell \wedge n = 1$ for simplicity), hence (for instance) a *theta model of level n* for A_2
- Flexible: if $\ell = \sum a_u^2$, we can use $X'_i(P) = \sum_{T \in K} \prod_u X_i(a_u(\tilde{P} + \tilde{T}))$
N.B.: $P \mapsto X_i(a_u P)$ is of degree a_u^2
- Cubical isogeny $\tilde{\phi}$: compatibility between cubes of level $n\ell$ on A_1 and cubes of level n on A_2

Summary

- Generalisation of Vélú's formula to higher dimension via cubical traces
- Flexible framework (choice of coordinate to put in the trace)

Going further:

- The mathematical framework for computing isogenies is descent theory, hence theta groups
- Amazing fact: cubical arithmetic in level n allows to compute the theta group action in level $n!$
- Isogenies lift to cubical isogenies (compatible with cubes) and cubical traces naturally compute cubical isogenies
- Compatibility of pairings and isogenies is a special case of the compatibility of cubical isogenies and cubical arithmetic

Table of Contents

- 1 Cubical arithmetic
- 2 Constructing functions with prescribed divisors, applications to pairings
- 3 Computing isogenies
- 4 Isogeny preimages, and radical isogenies
- 5 The monodromy leak
- 6 Perspectives

Preimages

- $\phi : E_1 \rightarrow E_2$ isogeny of elliptic curves (for simplicity) with cyclic kernel $K = \langle T \rangle$ of order ℓ
- We saw how to compute isogeny images $P \mapsto \phi(P)$
- **Goal:** compute isogeny preimages: $\phi^{-1}(Q)$
- For ease of notations: let $\hat{\phi} : E_2 \rightarrow E_1$ be the contragredient isogeny, we will compute the preimages $\hat{\phi}^{-1}(P) \subset E_2$
- **Radical isogenies:** the preimages $T_2 \in \hat{\phi}^{-1}(T)$ are in bijection with the non-backtracking isogenies $\phi_2 : E_2 \rightarrow E_3$

Torsors

- $\phi/k : E_1 \rightarrow E_2, P \in E_1(k)$
 - If $\hat{\phi}^{-1}(P)$ contains a rational point $Q \in E_2(k)$, then the fiber is in bijection with $\text{Ker } \hat{\phi}$ via $\hat{\phi}^{-1}(P) = Q + \text{Ker } \hat{\phi}$
 - It certainly contains such a point over the separable closure of k (assume ϕ separable)
- $\Rightarrow \hat{\phi}^{-1}(P)$ is an (étale) $\text{Ker } \hat{\phi}$ -torsor
- If $\text{Ker } \phi = \langle T \rangle$ with $T \in E_1(k)$, then $\text{Ker } \phi \simeq \mathbb{Z}/\ell\mathbb{Z}$, so $\text{Ker } \hat{\phi} \simeq \mu_\ell$ (via the Weil-Cartier pairing)
 - $\hat{\phi}^{-1}(P)$ is an (étale) μ_ℓ -torsor
- \Rightarrow Hilbert 90: we have an isomorphism of schemes over k : $\hat{\phi}^{-1}(P) \simeq \{x^\ell = C\}$

Theorem

By the geometric interpretation of the Tate pairing, $C = e_{T,\ell}(T, P)$ (non reduced Tate pairing)

- **Goal:** make this isomorphism explicit

Cubical arithmetic for preimages

- Goal: compute $\hat{\phi}^{-1}(P)$, $\phi : E_1 \rightarrow E_2$ with kernel $K = \langle T \rangle$
- Fix an excellent lift \tilde{T}
- Fix \tilde{P} and an excellent lift $\widetilde{P+T}$ relative to \tilde{P} and \tilde{T} .
 - ➊ Start with an arbitrary lift $\widetilde{P+T}$
 - ➋ Compute $\tilde{P} + \ell\tilde{T} = \lambda_P\tilde{P}$
N.B.: λ_P is the Tate pairing of P with T !
 - ➌ Then $\lambda_P^{1/\ell} \star \widetilde{P+T}$ is an excellent lift relative to \tilde{P}, \tilde{T}
- Construct the cubical points $\tilde{P} + i\tilde{T}$ for $i = 0, \dots, \ell - 1$
- These give the coordinates (in level $n\ell$) of a point $Q \in \hat{\phi}^{-1}(P)$!
- The ℓ choices for $\lambda_P^{1/\ell}$ give the ℓ preimages.

Descending level

Theorem

If X_1, \dots, X_n are a basis of section of level n on E_1 , then the $X_m(\tilde{P} + i\tilde{T})$ form a basis of sections of level ℓn on E_2 , evaluated on Q

- We want to describe Q with coordinates X'_i of level n
- Goal: take linear combinations of the $X_m(\tilde{P} + i\tilde{T})$ of the form $X'_m(Q)X_0'^{\ell-1}(Q)$.
- We recover projective coordinates of level n for Q
- Method: use descent through a well chosen isogeny

Descending level on an abelian variety

- Write $\ell = 1 + a^2 + b^2 + c^2 + d^2$ and take $F : A^5 \rightarrow A^5$ given by the matrix

$$\begin{pmatrix} 1 & a & b & c & d \\ a & -1 & 0 & 0 & 0 \\ b & 0 & -1 & 0 & 0 \\ c & 0 & 0 & -1 & 0 \\ d & 0 & 0 & 0 & -1 \end{pmatrix}$$

- The kernel of F is given by the image of $A[\ell]$ into A^5 via $P \mapsto (P, aP, bP, cP, dP)$
- There is a block diagonal matrix $M = \begin{pmatrix} 1 & 0 \\ 0 & M_2 \end{pmatrix}$ such that $t_F MF = \ell \text{Id}$.
- So F is an ℓ -isogeny $(A, \Theta_A)^5 \rightarrow (A, \Theta_A) \times (A^4, \Theta')$ (Θ' non principal non product polarisation)
- Applying the **isogeny formulas** to F allows to recover the level n coordinates on A by **projecting to the left factor**
- N.B: here we are already in level ℓn on the domain so the isogeny formulas are simple. The kernel is of size ℓ^{2g} but half of the points give a trivial action, so we take a trace under ℓ^g terms.
- Complexity for descending from level ℓn to level n : $O(\ell^g)$

Multiradical isogenies

- A of dimension g , $K = \langle T_1, \dots, T_g \rangle$, $\phi : A \rightarrow B$
- $\ell^{g(g+1)/2}$ choice of excellent lifts for $\widetilde{T_i}, \widetilde{T_i + T_j} \Rightarrow$ all our possible $\ell^{g(g+1)/2}$ multiradical isogenies (after descending back to level n)
- These involve the (sqrt of the) "self" Tate pairings $e_{T,\ell}(T_i, T_j)$ (ℓ odd)
- If $P \in A$, ℓ^g choices for $\widetilde{P + T_i} \Rightarrow$ all ℓ^g possible preimages $Q \in \hat{\phi}^{-1}(P)$ (after descending back to level n)
- These involves the Tate pairings $e_{T,\ell}(T_i, P)$

Summary

- Cubical arithmetic allows to go up and down in level, not only on the same abelian variety but also across an isogeny
- Explicit algorithms to compute preimages and radical isogenies
- The Tate pairings naturally appear in these algorithms

Open questions:

- Interpretation of the cubical coordinates of the neutral points of 0_A and 0_B as modular forms (in the spirit of [KNRR21])?
- Simpler descent formulas?
- Radical SqrtVelu formulas?
- In progress: explicit radical formulas for Montgomery curves

Table of Contents

- 1 Cubical arithmetic
- 2 Constructing functions with prescribed divisors, applications to pairings
- 3 Computing isogenies
- 4 Isogeny preimages, and radical isogenies
- 5 The monodromy leak
- 6 Perspectives

Cubical arithmetic and DLP

- $P \in E(\mathbb{F}_q)$ a point of ℓ -torsion, $Q = s \cdot P$
- **DLP**: given (P, Q) recover s
- Assume $\ell \nmid q - 1$, then $\mu_\ell \cap \mathbb{F}_q = \{1\}$
(Otherwise use pairings to reduce the DLP to \mathbb{F}_q^*)
- Then there is only one **canonical excellent lift** $\hat{P} := \tilde{P}$ above P with coordinates in \mathbb{F}_q (there is only one rational root of $x^\ell = e_{T,\ell}(P, P)$)
- \hat{P}, \hat{Q} are **easy to compute**
- We have $s \cdot \hat{P} = \hat{Q}$
- This lifts the DLP to a **cubical DLP**
- Now assume that someone **leaks** $(\tilde{P}, \tilde{Q} = s \cdot \tilde{P})$ for some cubical point (not canonical) \tilde{P} above P
- Write $\tilde{P} = \lambda \star \hat{P}$
- Then $\tilde{Q} = s \cdot \tilde{P} = \lambda^{s^2} \star s \cdot \hat{P} = \lambda^{s^2} \star \hat{Q}$.
- We know (λ, λ^{s^2}) . A DLP in \mathbb{F}_q^* allows to recover s^2 , hence s (modulo the multiplicative order of λ).
- If λ has large enough order, we obtain s .
- This assumes $q - 1$ has not too many factor so that there are not too many sqrt of s^2 to check.

The monodromy leak

- For the attack to work, we need someone to leak $\tilde{P}, \tilde{Q} = s \cdot \tilde{P}$
 - How would that be possible? Nobody uses cubical arithmetic for standard ECC, right?
 - Actually, many implementations use the **Montgomery ladder**.
 - And this is (almost!) the cubical ladder.
-
- **Montgomery ladder**: Start from $(X(P), Z(P) = 1)$ and compute $(X(sP), Z(sP))$
 - Then output $x(sP) = X(sP)/Z(sP)$. If division not in **constant time**, this leaks $Z(sP)$.
 - Hence this leaks $s \cdot \tilde{P}$ for $\tilde{P} = (x(P), 1)$
 - N.B.: Montgomery ladder is not quite the **cubical ladder**, so we solve a different **degree two equation** to recover s .

The general DLP:

- If we have only (P, Q) , we take **arbitrary choices** of \tilde{P}, \tilde{Q} .
- We have $\tilde{Q} = t \cdot \tilde{P}$ for some $t \equiv s \pmod{\ell}$ (if \tilde{P} is chosen to have order $\ell(q-1)$)
- Apply the **monodromy leak attack** to recover t modulo $q-1$
- **Problem**: ℓ is coprime to $q-1$, so this gives zero information on $s \pmod{\ell}$.
- The **monodromy leak only works** when we know that $0 < t < \ell$!

Table of Contents

- 1 Cubical arithmetic
- 2 Constructing functions with prescribed divisors, applications to pairings
- 3 Computing isogenies
- 4 Isogeny preimages, and radical isogenies
- 5 The monodromy leak
- 6 Perspectives

- DLP, pairing inversion from the cubical point of view?
- Cubical arithmetic allows to reduce the elliptic curve DLP to a DLP between “quasi”-cyclic matrices of size $\ell \times \ell$. Not very useful but gives new point of view on pairings attacks (take an eigenvalue of these matrices to reduce to a DLP in dimension 1)
- Investigate the arithmetic of non symmetric biextensions induced by (non symmetric) isogenies
- R -sesquilinear pairings [Sta24] from the cubical point of view? (Replace \mathbb{G}_m torsors by $\mathbb{G}_m^{\otimes R}$ -torsors?)
- Related: computing multidimensional endomorphism ladders $\sum \alpha_i \tilde{P}_i$?
- Self pairings [CHM+23] from the cubical point of view?
- [Bre83]: if we have a symmetric cubical torsor structure on (G, \mathcal{L}) , $G \subset A[n]$, then there is a canonical trivialisation of the induced cubical structure on $[2n]^* \mathcal{L}$.
- Similarity with self pairings: if P is of n -torsion, then the self pairing $e(P, P)$ lives in μ_{2n} .

Bibliography

- [Bre83] L. Breen. Fonctions thêta et théoreme du cube. Vol. 980. Springer, 1983 (cit. on pp. 3, 4, 14, 42).
- [CHM+23] W. Castryck, M. Houben, S.-P. Merz, M. Mula, S. v. Buuren, and F. Vercauteren. “Weak instances of class group action based cryptography via self-pairings”. In: Annual International Cryptology Conference. Springer, 2023, pp. 762–792 (cit. on p. 42).
- [CR15] R. Cosset and D. Robert. “An algorithm for computing (ℓ, ℓ) -isogenies in polynomial time on Jacobians of hyperelliptic curves of genus 2”. In: Mathematics of Computation 84.294 (Nov. 2015), pp. 1953–1975. doi: [10.1090/S0025-5718-2014-02899-8](https://doi.org/10.1090/S0025-5718-2014-02899-8) (cit. on p. 25).
- [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 pp. 3, 14, 20).
- [KNRR21] M. Kirschmer, F. Narbonne, C. Ritzenthaler, and D. Robert. “Spanning the isogeny class of a power of an elliptic curve”. In: Mathematics of Computation 91.333 (Sept. 2021), pp. 401–449. doi: [10.1090/mcom/3672](https://doi.org/10.1090/mcom/3672). arXiv: [2004.08315](https://arxiv.org/abs/2004.08315) (cit. on p. 37).
- [LR12] D. Lubicz and D. Robert. “Computing isogenies between abelian varieties”. In: Compositio Mathematica 148.5 (Sept. 2012), pp. 1483–1515. doi: [10.1112/S0010437X12000243](https://doi.org/10.1112/S0010437X12000243). arXiv: [1001.2016](https://arxiv.org/abs/1001.2016) [[math.AG](https://arxiv.org/archive/math)] (cit. on p. 25).
- [LR16] D. Lubicz and D. Robert. “Arithmetic on Abelian and Kummer Varieties”. In: Finite Fields and Their Applications 39 (May 2016), pp. 130–158. doi: [10.1016/j.ffa.2016.01.009](https://doi.org/10.1016/j.ffa.2016.01.009) (cit. on p. 12).
- [LR22] D. Lubicz and D. Robert. “Fast change of level and applications to isogenies”. In: Research in Number Theory (ANTS XV Conference) 9.1 (Dec. 2022). doi: [10.1007/s40993-022-00407-9](https://doi.org/10.1007/s40993-022-00407-9) (cit. on p. 25).
- [Mor85] L. Moret-Bailly. Pinceaux de variétés abéliennes. Société mathématique de France, 1985 (cit. on pp. 3, 9).
- [Rob21] D. Robert. “Efficient algorithms for abelian varieties and their moduli spaces”. HDR thesis. Université Bordeaux, June 2021. url: <http://www.normalesup.org/~robert/pro/publications/academic/hdr.pdf>. Slides: [2021-06-HDR-Bordeaux.pdf](https://arxiv.org/abs/2021-06-HDR-Bordeaux.pdf) (11h, Bordeaux). (Cit. on p. 25).
- [Rob24] D. Robert. “Fast pairings via biextensions and cubical arithmetic”. Apr. 2024 (cit. on pp. 3, 6, 20, 25).
- [Stao8] 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 pp. 13, 20).
- [Sta24] K. E. Stange. “Sesquilinear pairings on elliptic curves”. In: arXiv preprint arXiv:2405.14167 (2024) (cit. on p. 42).