MARSEILLE, 31 MAY 2021

L. COLÒ I2M

A MODULAR APPROACH TO OSIDH

LEONARDO COLÒ & DAVID KOHEL
Institut de Mathématiques de Marseille

Arithmetic, Geometry, Cryptography and Coding Theory 2021

Definition

Given an elliptic curve E over k, and a finite set of primes S, we can associate an isogeny graph $\Gamma = (E, S)$

- whose vertices are elliptic curves isogenous to E over $\bar{k}$, and
- whose edges are isogenies of degree $\ell \in S$.

The vertices are defined up to $\bar{k}$-isomorphism and the edges from a given vertex are defined up to a $\bar{k}$-isomorphism of the codomain.

If $S = \{\ell\}$, then we call Γ an ℓ-isogeny graph.

For an elliptic curve E/k and prime $\ell \neq \texttt{char}(k)$, the full ℓ-torsion subgroup is a 2-dimensional $\mathbb{F}_\ell$-vector space:

$$E[\ell] = \left\{P \in E[\bar{k} \,\middle|\, \ell P = O]\right\} \simeq \mathbb{F}_\ell^2$$

Consequently, the set of cyclic subgroups is in bijection with $\mathbb{P}^1(\mathbb{F}_\ell)$, which in turn are in bijection with the set of ℓ-isogenies from E.

Thus, the ℓ-isogeny graph of E is $(\ell + 1)$-regular (as a directed multigraph).

ORIENTED ISOGENY GRAPHS

Let $\mathcal{O}$ be an order in an imaginary quadratic field K. An $\mathcal{O}$*-orientation* on a supersingular elliptic curve E is an inclusion $\iota : \mathcal{O} \hookrightarrow \mathsf{End}(E)$, and a K*-orientation* is an inclusion $\iota : K \hookrightarrow \mathsf{End}^0(E) = \mathsf{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$. An $\mathcal{O}$-orientation is *primitive* if $\mathcal{O} \simeq \mathsf{End}(E) \cap \iota(K)$.

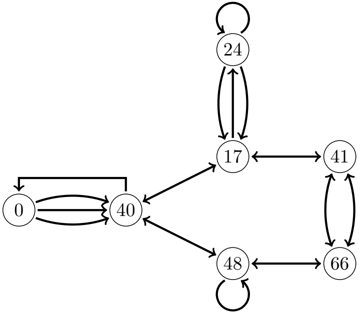
Theorem

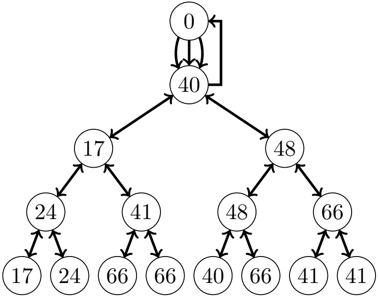
The category of K-oriented supersingular elliptic curves (E, ι), whose morphisms are isogenies commuting with the K-orientations, is equivalent to the category of elliptic curves with CM by K.

The orientation by a quadratic imaginary field gives to supersingular isogeny graphs the rigid structure of a volcano. It also differentiates vertices in the descending paths from the crater, determining an infinite graph.

ORIENTED ISOGENY GRAPHS - AN EXAMPLE

Let $E_0/\mathbb{F}_{71}$ be the supersingular elliptic curve with $j(E) = 0$, oriented by the order $\mathcal{O}_K = \mathbb{Z}[\omega]$, where $\omega^2 + \omega + 1 = 0$. The unoriented 2-isogeny graph is the finite graph on the left.
The orientation by $K = \mathbb{Q}[\omega]$ differentiates vertices in the descending paths from E_0, determining an infinite graph shown here to depth 4:





CLASS GROUP ACTION

- $\mathsf{SS}(p) = \{$supersingular elliptic curves over $\overline{\mathbb{F}}_p$ up to isomorphism$\}$.
- $\mathsf{SS}_{\mathcal{O}}(p) = \{\mathcal{O}$-oriented s.s. elliptic curves over $\overline{\mathbb{F}}_p$ up to K-isomorphism$\}$.
- $\mathsf{SS}_{\mathcal{O}}^{pr}(p) =$subset of primitive $\mathcal{O}$-oriented curves.

The set $\mathsf{SS}_{\mathcal{O}}(p)$ admits a transitive group action:

$$\mathcal{C}\ell(\mathcal{O}) \times \mathsf{SS}_{\mathcal{O}}(p) \longrightarrow \mathsf{SS}_{\mathcal{O}}(p) \qquad ([\mathfrak{a}]\,, E) \longmapsto [\mathfrak{a}] \cdot E = E/E[\mathfrak{a}]$$

Proposition

The class group $\mathcal{C}\ell(\mathcal{O})$ acts faithfully and transitively on the set of $\mathcal{O}$-isomorphism classes of primitive $\mathcal{O}$-oriented elliptic curves.

In particular, for fixed primitive $\mathcal{O}$-oriented E, we obtain a bijection of sets:

$$\mathcal{C}\ell(\mathcal{O}) \longrightarrow \mathsf{SS}_{\mathcal{O}}^{pr}(p) \qquad [\mathfrak{a}] \longmapsto [\mathfrak{a}] \cdot E$$

EFFECTIVE CLASS GROUP ACTION

The theory of complex multiplication relates the geometry of isogenies to the arithmetic Galois action on elliptic curves in characteristic zero, mediated by the map of $\mathcal{C}\ell(\mathcal{O})$ into each.

Over a finite field, we use the geometric action by isogenies to recover the class group action. In particular we describe the action of $\mathcal{C}\ell(\mathcal{O})$ on ℓ-isogeny chains in the *whirlpool*.

Suppose that (E_i, ϕ_i) is a descending ℓ-isogeny chain with

$$\mathcal{O}_K \subseteq \mathsf{End}(E_0), \dots, \mathcal{O} = \mathbb{Z} + \ell^n \mathcal{O}_K \subseteq \mathsf{End}(E_n).$$

If $\mathfrak{q}$ is a split prime in $\mathcal{O}_K$ over $q \neq \ell, p$, then the isogeny

$$\psi_0 : E_0 \to F_0 = E_0/E_0[\mathfrak{q}]$$

can be extended to the ℓ-isogeny chain by pushing forward the cyclic group $C_0 = E_0[\mathfrak{q}]$:

$$C_0 = E_0[\mathfrak{q}], C_1 = \phi_0(C_0), \dots, C_n = \phi_{n-1}(C_{n-1}),$$

and defining $F_i = E_i/C_i$.

LADDERS

This construction motivates the following definition.

Definition

An ℓ-ladder of length n and degree q is a commutative diagram of ℓ-isogeny chains (E_i, ϕ_i), (F_i, ϕ_i') of length n connected by q-isogenies $\psi_i : E_i \to F_i$

$$\begin{tikzcd} E_0 \arrow[r, "\phi_0"] \arrow[d, "\psi_0"'] & E_1 \arrow[r, "\phi_1"] \arrow[d, "\psi_1"'] & E_2 \arrow[r, "\phi_2"] \arrow[d, "\psi_2"'] & \cdots \arrow[r, "\phi_{n-1}"] & E_n \arrow[d, "\psi_n"'] \\ F_0 \arrow[r, "\phi_0'"'] & F_1 \arrow[r, "\phi_1'"'] & F_2 \arrow[r, "\phi_2'"'] & \cdots \arrow[r, "\phi_{n-1}'"'] & F_n \end{tikzcd}$$

If ψ_0 is as above ($(\psi_0) = E_0[\mathfrak{q}]$), the ladder encodes the action of $\mathcal{C}\ell(\mathcal{O})$ on ℓ-isogeny chains, and consequently on elliptic curves at depth n.

INITIALIZING THE LADDER

We characterize the initialization phase of ladder construction = construction of q-isogenies of ℓ-isogeny chains for level one, $\Gamma = \mathsf{PSL}_2(\mathbb{Z})$.

The structure of oriented isogeny graphs (of level one) depends only on the class groups $\mathcal{C}\ell(\mathcal{O}_n)$ (at level n) and the quotient maps $\mathcal{C}\ell(\mathcal{O}_n) \to \mathcal{C}\ell(\mathcal{O}_{n-1})$. The quotient maps determine the edges of the ℓ-isogeny graph (between level n and $n-1$) and the class of the prime ideals over $q \neq \ell$ in $\mathcal{C}\ell(\mathcal{O}_n)$ determine edges between vertices at level n.

We assume we are given a descending modular ℓ-isogeny chain, beginning with an initial modular point associated to a CM point with CM order $\mathcal{O}_K$. In order to initialize a q-ladder, at small distance m from the initial point, we can identify a reduced ideal class in $\mathcal{C}\ell(\mathcal{O}_m)$ which lies in the same class in $\mathcal{C}\ell(\mathcal{O}_m)$.

INITIALIZING THE LADDER - AN EXAMPLE

Suppose $D_K = -3$, and $\ell = 2$; we note that for all $n \geq 3$, that

$$\mathcal{C}\ell(\mathcal{O}_n) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$$

and in particular, $\mathcal{C}\ell(\mathcal{O}_n)[2]$ consist of the classes of binary quadratic forms

$$\{\langle 1, 0, |D_K|\ell^{2(n-1)}\rangle, \langle |D_K|, 0, \ell^{2(n-1)}\rangle, \langle \ell^2, \ell^2, n_1\rangle, \langle \ell^2|D_K|, \ell^2|D_K|, n_2\rangle\}.$$

where $\ell^4 - 4\ell^2 n_1 = \ell^4|D_K|^2 - 4\ell^2|D_K|n_2 = -\ell^{2n}|D_K|$, whence

$$n_1 = 1 + \ell^{2(n-2)}|D_K| \text{ and } n_2 = |D_K| + \ell^{2(n-2)}.$$

For $n = 3$, the form $\langle 12, 12, 7\rangle$ reduces to $\langle 7, 2, 7\rangle$ and the reduced representatives are:

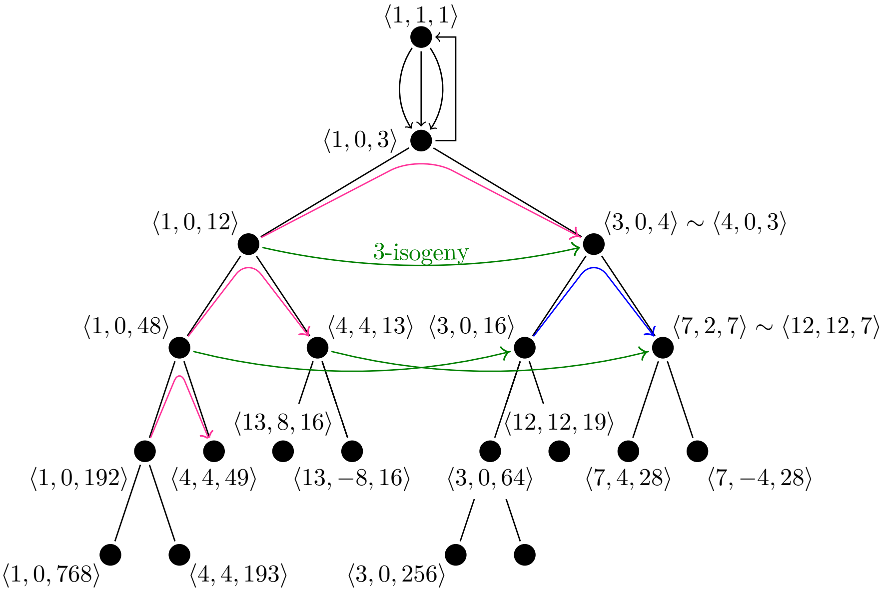
$$\{\langle 1, 0, 48\rangle, \langle 3, 0, 16\rangle, \langle 4, 4, 13\rangle, \langle 7, 2, 7\rangle\}.$$

but for for $n \geq 4$, since $12 < n_2$, the forms

$$\{\langle 1, 0, 3 \cdot 4^{n-2}\rangle, \langle 3, 0, 4^{n-2}\rangle, \langle 4, 4, n_1\rangle, \langle 12, 12, n_2\rangle\}$$

are reduced.

INITIALIZING THE LADDER - A PICTURE

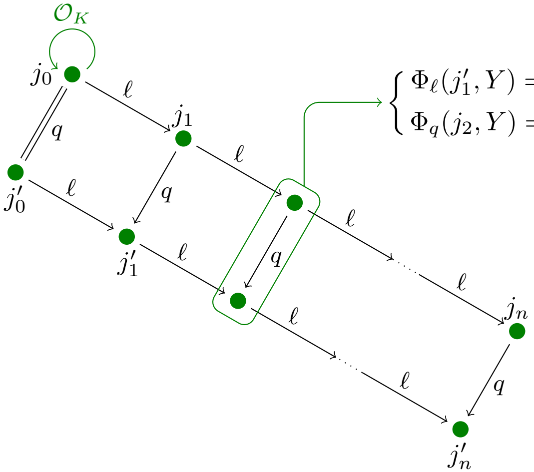


INITIALIZING THE LADDER - A TABLE

L.COLÒ I2M

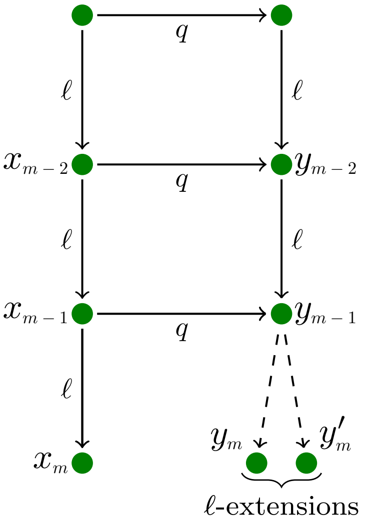
q	m	f_m	$[f_m]$	$[f_{m-1}]$
7	4	$\langle 7, 4, 28\rangle$	$[\langle 7, 4, 28\rangle]$	$[\langle 7, 2, 7\rangle]$
13	4	$\langle 13, 8, 16\rangle$	$[\langle 13, 8, 16\rangle]$	$[\langle 4, 4, 13\rangle]$
19	5	$\langle 19, 14, 43\rangle$	$[\langle 19, 14, 43\rangle]$	$[\langle 12, 12, 19\rangle]$
31	4	$\langle 31, 10, 7\rangle$	$[\langle 7, 4, 28\rangle]$	$[\langle 7, 2, 7\rangle]$
37	4	$\langle 37, 34, 13\rangle$	$[\langle 13, -8, 16\rangle]$	$[\langle 4, 4, 13\rangle]$
43	5	$\langle 43, 14, 19\rangle$	$[\langle 19, -14, 43\rangle]$	$[\langle 12, 12, 19\rangle]$
61	4	$\langle 61, 56, 16\rangle$	$[\langle 13, -8, 16\rangle]$	$[\langle 4, 4, 13\rangle]$
67	6	$\langle 67, 24, 48\rangle$	$[\langle 48, -24, 67\rangle]$	$[\langle 12, 12, 67\rangle]$
73	5	$\langle 73, 40, 16\rangle$	$[\langle 16, -8, 49\rangle]$	$[\langle 4, 4, 49\rangle]$
79	4	$\langle 79, 38, 7\rangle$	$[\langle 7, 4, 28\rangle]$	$[\langle 7, 2, 7\rangle]$
97	5	$\langle 97, 56, 16\rangle$	$[\langle 16, 8, 49\rangle]$	$[\langle 4, 4, 49\rangle]$
103	4	$\langle 103, 46, 7\rangle$	$[\langle 7, -4, 28\rangle]$	$[\langle 7, 2, 7\rangle]$
109	4	$\langle 109, 70, 13\rangle$	$[\langle 13, 8, 16\rangle]$	$[\langle 4, 4, 13\rangle]$
127	4	$\langle 127, 116, 28\rangle$	$[\langle 7, 4, 28\rangle]$	$[\langle 7, 2, 7\rangle]$

COMPLETING SQUARES OF ISOGENIES



$$\begin{cases} \Phi_\ell(j_1', Y) = 0 \\ \Phi_q(j_2, Y) = 0 \end{cases}$$

EXTENDING THE LADDER



Let $\ell = 2$.

- The two ℓ-extensions are determined by a quadratic polynomial (deduced from y_{m-1}, y_{m-2}:

$$\phi_\ell(y) = 0$$

  We can solve for y_m, y'_m, its roots.

- We have a degree $q + 1$ polynomial $\phi_q(y) = 0$ determined by x_m but we do note need to compute it. It suffices

$$\phi_q(y) \mod \phi_\ell(y)$$

  Indeed

$$\Phi_q(x, y) \equiv \phi_q(y) \mod (x - x_m, \phi_\ell(y))$$

ADDING LEVEL STRUCTURE

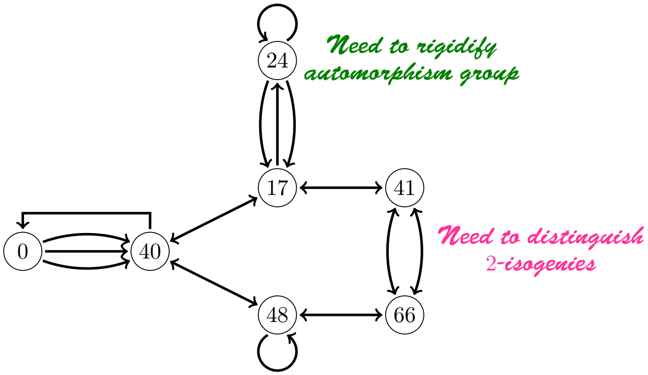
There are multiple reasons to add level structure to our construction:

- With an ℓ-level structure, the extension of ℓ-isogenies by modular correspondences allows one to automatically remove the dual isogeny (backtracking): there are ℓ rather than $\ell+1$ extensions.

ADDING LEVEL STRUCTURE

There are multiple reasons to add level structure to our construction:

- With an ℓ-level structure, the extension of ℓ-isogenies by modular correspondences allows one to automatically remove the dual isogeny (backtracking): there are ℓ rather than $\ell + 1$ extensions.
- The modular isogeny chain is a potentially-non injective image of the isogeny chain.



ADDING LEVEL STRUCTURE

L.COLÒ I2M

There are multiple reasons to add level structure to our construction:

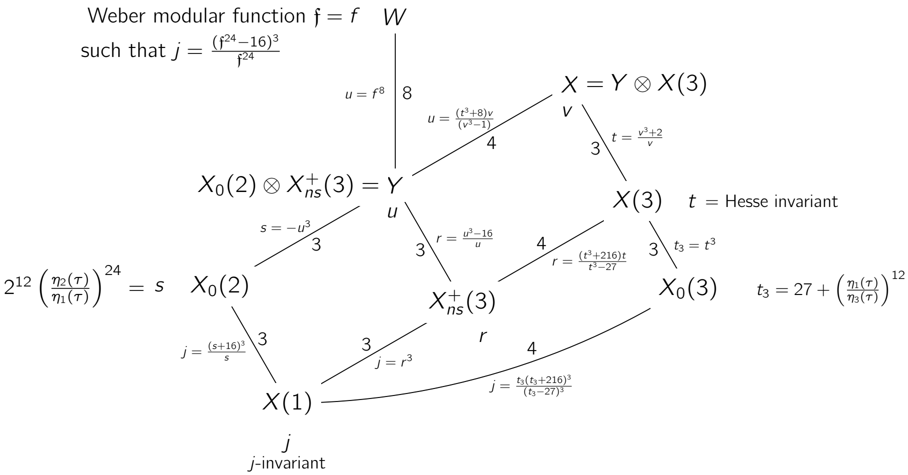
- With an ℓ-level structure, the extension of ℓ-isogenies by modular correspondences allows one to automatically remove the dual isogeny (backtracking): there are ℓ rather than $\ell + 1$ extensions.
- The modular isogeny chain is a potentially-non injective image of the isogeny chain.
- Rigidifying automorphisms should also shorten the distance to which we need to go in order to differentiate 2 points (two torsion of $\mathcal{C}\ell(\mathcal{O})$ may lift to non 2-torsion point in $\mathcal{C}\ell(\mathcal{O}, \Gamma)$).

ADDING LEVEL STRUCTURE

There are multiple reasons to add level structure to our construction:

- With an ℓ-level structure, the extension of ℓ-isogenies by modular correspondences allows one to automatically remove the dual isogeny (backtracking): there are ℓ rather than $\ell + 1$ extensions.
- The modular isogeny chain is a potentially-non injective image of the isogeny chain.
- Rigidifying automorphisms should also shorten the distance to which we need to go in order to differentiate 2 points (two torsion of $\mathcal{C}\ell(\mathcal{O})$ may lift to non 2-torsion point in $\mathcal{C}\ell(\mathcal{O}, \Gamma)$).
- q-modular polynomial of higher level are smaller.

SOME MODULAR CURVES OF INTEREST FOR OSIDH



Future directions:

- Implementation and algorithmic optimization.
- Explicit realization of the class group action.

THANK YOU FOR YOUR ATTENTION