MARSEILLE, 10 NOVEMBER 2022

L.COLÒ I2M

ORIENTED SUPERSINGULAR ELLIPTIC CURVES & CLASS GROUP ACTIONS

LEONARDO COLÒ & DAVID KOHEL

Institut de Mathématiques de Marseille

Séminaire ATI - Arithmétique et Théorie de l'Information

ISOGENY GRAPHS

Definition

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

- 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 G an ℓ-isogeny graph, G_ℓ.

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).

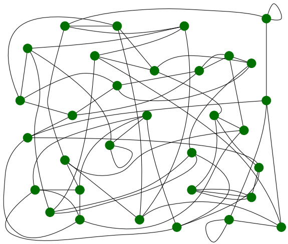
SUPERSINGULAR ISOGENY GRAPHS

L.COLÒ I2M

The supersingular isogeny graphs are remarkable because the vertex sets are finite : there are $(p+1)/12 + \epsilon_p$ curves. Moreover

- every supersingular elliptic curve can be defined over $\mathbb{F}_{p^2}$;
- all ℓ-isogenies are defined over $\mathbb{F}_{p^2}$;
- every endomorphism of E is defined over $\mathbb{F}_{p^2}$.

The lack of a commutative group acting on the set of supersingular elliptic curves/$\mathbb{F}_{p^2}$ makes the isogeny graph more complicated.



SUPERSINGULAR ISOGENY GRAPHS - SPECIAL VERTICES

Supersingular curves with j-invariants 0 and 1728 have extra automorphisms, besides $[\pm 1]$.

- E_{1728} is supersingular if $p \equiv 3 \mod 4$

$$\text{Aut}(E_{1728}) = \{[\pm 1], [\pm i]\} \qquad \text{End}(E_{1728}) = \mathbb{Z}\langle [i], \frac{1+\pi_p}{2} \rangle$$

  where $[i](x, y) = (-x, iy)$ for $i^2 = -1$ in $\mathbb{F}_{p^2}$ and $\pi_p(x, y) = (x^p, y^p)$ is Frobenius.

- E_0 is supersingular if $p \equiv 2 \mod 3$

$$\text{Aut}(E_0) = \{[\pm 1], [\pm \zeta_3], [\pm \zeta_3^2]\} \qquad \text{End}(E_0) = \mathbb{Z}\langle [\zeta_3], \pi_p \rangle$$

  where $[\zeta_3](x, y) = (\zeta_3 x, y)$ for $\zeta_3^2 + \zeta_3 + 1 = 0$ in $\mathbb{F}_{p^2}$.

Because of these extra automorphisms, supersingular isogeny graphs may fail to really be undirected graphs.
Since this issue occurs only at neighbours of E_0 and E_{1728}, we usually forget this subtlety.

ORIENTATIONS

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

Let $\phi : E \to F$ be an isogeny of degree ℓ. A K-orientation $\iota : K \hookrightarrow \mathsf{End}^0(E)$ determines a K-orientation $\phi_*(\iota) : K \hookrightarrow \mathsf{End}^0(F)$ on F, defined by

$$\phi_*(\iota)(\alpha) = \frac{1}{\ell}\, \phi \circ \iota(\alpha) \circ \hat{\phi}.$$

Conversely, given K-oriented elliptic curves (E, ι_E) and (F, ι_F) we say that an isogeny $\phi : E \to F$ is K-oriented if $\phi_*(\iota_E) = \iota_F$, i.e., if the orientation on F is induced by ϕ.

ORIENTED ISOGENY GRAPHS - VERTICES & EDGES

L.COLÒ I2M

Two K-oriented curves are isomorphic if and ony if there exists a K-oriented isomorphism between them. We denote $G_S(E,K)$ the S-isogeny graph of K-oriented supersingular elliptic curves over $\mathbb{F}_{p^2}$ whose vertices are isomorphism classes of K-oriented supersingular elliptic curves $/\mathbb{F}_{p^2}$ and whose edges are equivalence classes of K-oriented isogenies of degree in S.

Proposition*

The only vertices of $G_\ell(E,K)$ with extra automorphisms are (E,ι) where either

- $E = E_{1728}$ and $\iota(i) = [\pm i]$ or
- $E = E_0$ and $\iota(\zeta_3) = [\pm\zeta_3]$.

Then (E,ι) has out-degree $\ell+1$, except at the oriented curves with extra automorphisms, in which case thise degree is $2(\ell+1-r_\ell)/|\mathrm{Aut}(E)|+r_\ell$ where $|\mathrm{Aut}(E)|r_\ell$ is the number of elements of $\mathcal{O}$ of norm ℓ.

*Arpin, S. and Chen, M. and Lauter, K.E. and Scheidler, R. and Stange, K.E. and Tran, H.T.N. - Orientations and cycles in supersingular isogeny graphs

Oriented isogeny graphs - structure

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.

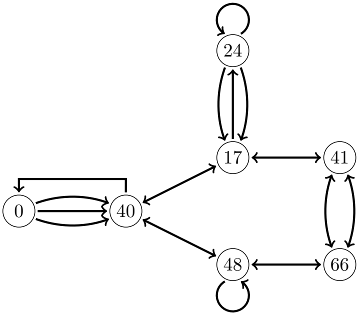
$G_\ell(E, K)$ consists of connected components, each of which is a volcano.

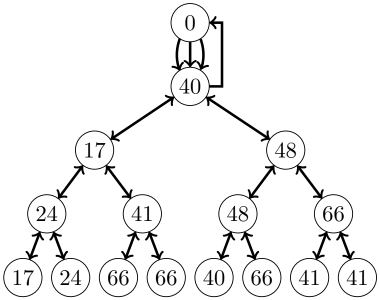
- The crater consists of K-oriented elliptic curves which are $\mathcal{O}$-primitive for some fixed ℓ-fundamental order $\mathcal{O}$ of K.
- Oriented curves at depth k are primitively oriented by orders of index ℓ^k in $\mathcal{O}$.
- We recover the standar terminology for oriented isogenies:
  - If $\mathcal{O} = \mathcal{O}'$ we say that ϕ is horizontal;
  - If $\mathcal{O} \supsetneq \mathcal{O}'$ we say that ϕ is ascending;
  - If $\mathcal{O} \subsetneq \mathcal{O}'$ we say that ϕ is descending.

ORIENTED ISOGENY GRAPHS - AN EXAMPLE

L.COLÒ I2M

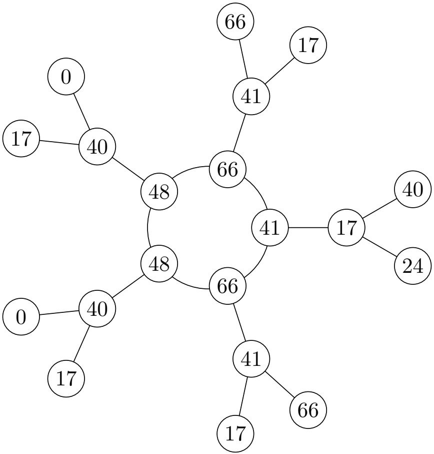
Let $E_0/\mathbb{F}_{71}$ be the supersingular elliptic curve with $j(E) = 0$, oriented by the order $\mathcal{O}_K = \mathbb{Z}[\omega]$, where $\omega^2 + \omega + 1 = 0$. The unoriented 2-isogeny graph is the finite graph on the left.
The orientation by $K = \mathbb{Q}[\omega]$ differentiates vertices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





ORIENTED ISOGENY GRAPHS - YET ANOTHER EXAMPLE

We let again $p = 71$ and we consider the isogeny graph oriented by $\mathbb{Z}[\omega_{79}]$ where ω_{79} generates the ring of integers of $\mathbb{Q}(\sqrt{-79})$.



ISOGENY CHAINS

Definition

An ℓ-isogeny chain of length n from E_0 to E is a sequence of isogenies of degree ℓ:

$$E_0 \xrightarrow{\phi_0} E_1 \xrightarrow{\phi_1} E_2 \xrightarrow{\phi_2} \dots \xrightarrow{\phi_{n-1}} E_n = E.$$

The ℓ-isogeny chain is without backtracking if $\texttt{ker}\,(\phi_{i+1} \circ \phi_i) \neq E_i[\ell],\ \forall i$. The isogeny chain is descending (or ascending, or horizontal) if each ϕ_i is descending (or ascending, or horizontal, respectively).

The dual isogeny of ϕ_i is the only isogeny ϕ_{i+1} satisfying $\texttt{ker}\,(\phi_{i+1} \circ \phi_i) = E_i[\ell]$. Thus, an isogeny chain is without backtracking if and only if the composition of two consecutive isogenies is cyclic.

Lemma

The composition of the isogenies in an ℓ-isogeny chain is cyclic if and only if the ℓ-isogeny chain is without backtracking.

PRIMITIVE ORIENTATIONS

- $\mathsf{SS}(p) = \{$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.

An element of $\mathsf{SS}_{\mathcal{O}}^{pr}(p)$ consists of

- A supersingular elliptic curve $E/\overline{\mathbb{F}}_p$;
- a primitive orientation $\iota : \mathcal{O} \hookrightarrow \mathsf{End}(E)$;
- a structure of a p-orientation which is a homomorphism $\rho : \mathcal{O} \to \overline{\mathbb{F}}_p$.

Note that $\mathsf{End}(E)$ is equipped with a p-orientation $\rho : \mathsf{End}(E) \hookrightarrow \overline{\mathbb{F}}_p$.

We denote by $\mathsf{SS}_{\mathcal{O}}(\rho)$ the set of oriented supersingular elliptic curves with ρ induced by ι and $\mathsf{End}(E)/\mathfrak{P} \hookrightarrow \overline{\mathbb{F}}_p$, and $\mathsf{SS}_{\mathcal{O}}(\overline{\rho})$ the opposite p-orientation class.

THE SET OF PRIMITIVE p-ORIENTED CURVES

Since $K \hookrightarrow \mathfrak{A}$, then

- If p splits in K then $\mathsf{SS}_{\mathcal{O}}^{pr}(p)$ is empty.
- If p ramifies in K then $\rho = \overline{\rho}$ and then

$$\mathsf{SS}_{\mathcal{O}}^{pr}(p) = \mathsf{SS}_{\mathcal{O}}^{pr}(\rho) = \mathsf{SS}_{\mathcal{O}}^{pr}(\overline{\rho})$$

- If p is inert in K then $\mathsf{SS}_{\mathcal{O}}(p)$ decomposes in

$$\begin{aligned}\mathsf{SS}_{\mathcal{O}}^{pr}(p) &= \mathsf{SS}_{\mathcal{O}}^{pr}(\rho) \cup \mathsf{SS}_{\mathcal{O}}^{pr}(\overline{\rho}) \\ &= \mathsf{SS}_{\mathcal{O}}^{pr}(\rho) \cup \mathsf{SS}_{\mathcal{O}}^{pr}(\rho)^{\sigma}\end{aligned}$$

CLASS GROUP ACTION

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

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

Proposition

The set $\mathsf{SS}_{\mathcal{O}}^{pr}(\rho)$ is a torsor for the class group $\mathcal{C}\ell(\mathcal{O})$.

In particular, for fixed primitive p-oriented supersingular elliptic curve E, we obtain a bijection of sets:

$$\begin{aligned} \mathcal{C}\ell(\mathcal{O}) &\longrightarrow \mathsf{SS}_{\mathcal{O}}^{pr}(\rho) \\ [\mathfrak{a}] &\longmapsto [\mathfrak{a}] \cdot E \end{aligned}$$

EFFECTIVE CLASS GROUP ACTION

L.COLÒ I2M

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.

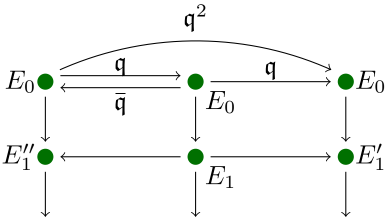
Definition

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 $\psi_i : E_i \to F_i$

$$\begin{array}{ccccccccc}
E_0 & \xrightarrow{\phi_0} & E_1 & \xrightarrow{\phi_1} & E_2 & \xrightarrow{\phi_2} & \cdots & \xrightarrow{\phi_{n-1}} & E_n \\
\downarrow{\scriptstyle \psi_0} & & \downarrow{\scriptstyle \psi_1} & & \downarrow{\scriptstyle \psi_2} & & & & \downarrow{\scriptstyle \psi_n} \\
F_0 & \xrightarrow{\phi'_0} & F_1 & \xrightarrow{\phi'_1} & F_2 & \xrightarrow{\phi'_2} & \cdots & \xrightarrow{\phi'_{n-1}} & F_n
\end{array}$$

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.

DIFFERENTIATING CONJUGATE IDEAL CLASSES



$E_i' \neq E_i''$ if and only if $\mathfrak{q}^2 \cap \mathcal{O}_i$ is not principal and the probability that a random ideal in $\mathcal{O}_i$ is principal is $1/h(\mathcal{O}_i)$. In fact, we can do better; we write $\mathcal{O}_K = \mathbb{Z}[\omega]$ and we observe that if $\mathfrak{q}^2$ was principal, then

$$q^2 = \mathsf{N}(\mathfrak{q}^2) = \mathsf{N}(a + b\ell^i\omega)$$

since it would be generated by an element of $\mathcal{O}_i = \mathbb{Z} + \ell^i\mathcal{O}_K$. Now

$$\mathsf{N}(a + b\ell^i) = a^2 \pm abt\ell^i + b^2 s\ell^{2i} \quad \text{where} \quad \omega^2 + t\omega + s = 0$$

Thus, as soon as $\ell^{2i} \gg q^2$, we are guaranteed that $\mathfrak{q}^2$ is not principal.

AN EQUIVALENCE OF CATEGORIES

Quadratic forms (a, b, c)	Ideal classes $\left[(a, \frac{-b+\sqrt{\Delta}}{2})\right]$	K-lattices $a\mathbb{Z} + \frac{-b\sqrt{\Delta}}{2}\mathbb{Z}$
Ideal classes $[\mathfrak{a}] = [(\alpha, \beta)]$	Quadratic forms $\frac{N(\alpha x - \beta y)}{N(\mathfrak{a})}$	K-lattices $\alpha\mathbb{Z} + \beta\mathbb{Z}$
K-lattices $\omega_1\mathbb{Z} + \omega_2\mathbb{Z}$	Quadratic forms $\frac{N(\omega_1 x - \omega_2 y)}{N(\omega_1)}$	Ideal classes (ω_1, ω_2)

INITIALIZING THE LADDER - AN EXAMPLE

L.COLÒ I2M

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:

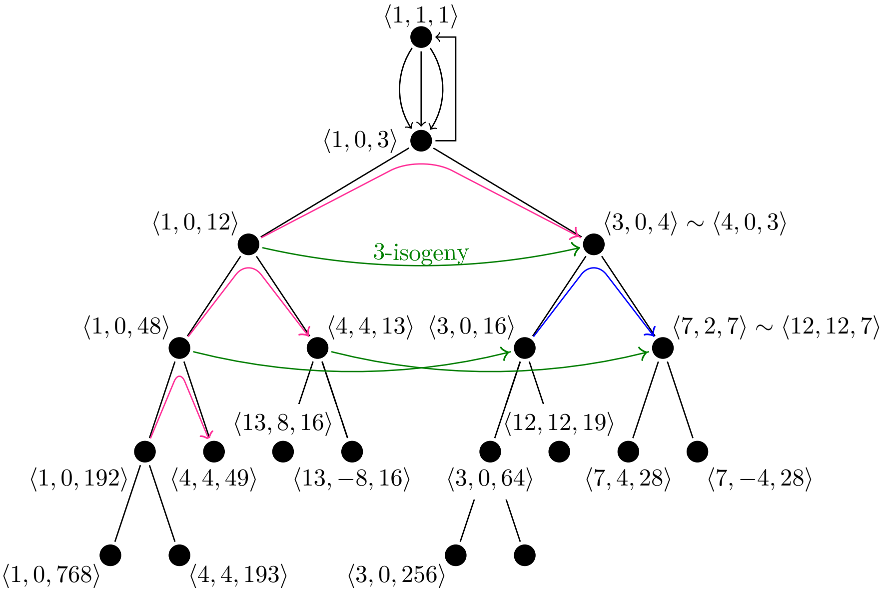
$$\{\langle 1, 0, 48\rangle, \langle 3, 0, 16\rangle, \langle 4, 4, 13\rangle, \langle 7, 2, 7\rangle\}.$$

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

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

are reduced.

INITIALIZING THE LADDER - A PICTURE

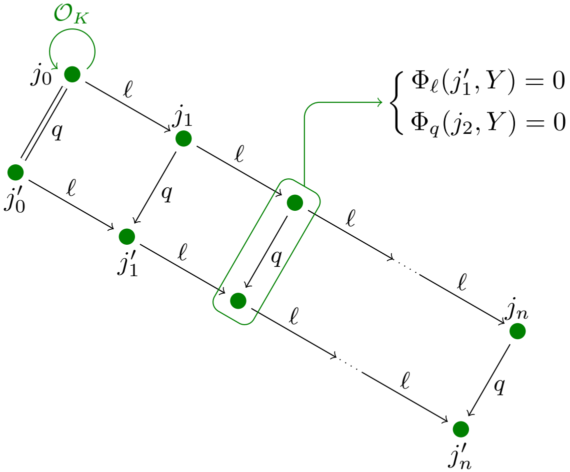


INITIALIZING THE LADDER - A TABLE

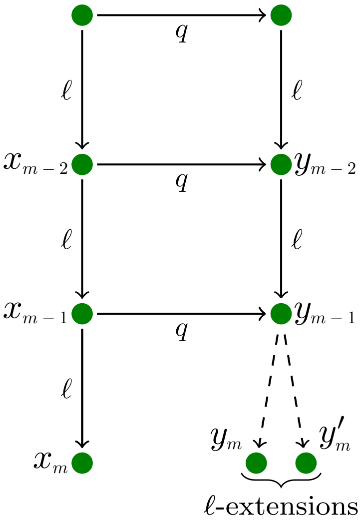
L.COLÒ I2M

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



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

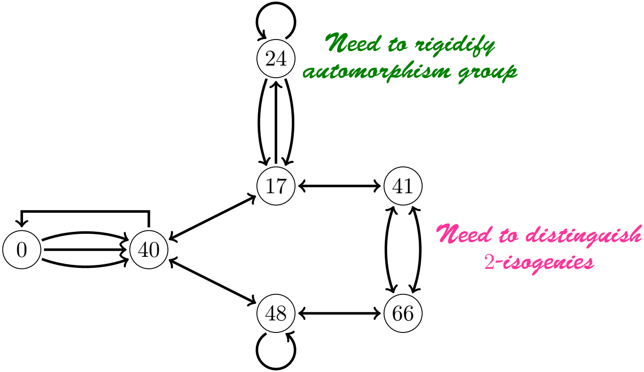
There are multiple reasons to add level structure to our construction:

- 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

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

L.COLÒ I2M

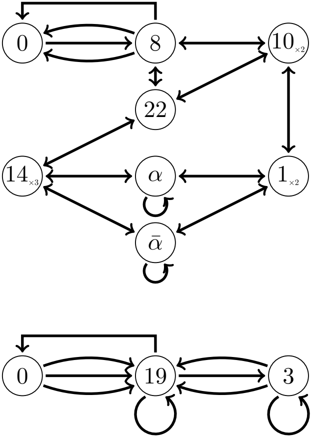
There are multiple reasons to add level structure to our construction:

- 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 $\mathcal{C}\ell(\mathcal{O}, \Gamma)$).
- q-modular polynomial of higher level are smaller.

ISOGENY GRAPHS WITH LEVEL STRUCTURE

L.COLÒ I2M

For any congruence subgroup Γ of level coprime to the characteristic, we have a covering $G_S(E,\Gamma) \to G_S(E)$ whose vertices are pairs $(E,\Gamma(P,Q))$ of supersingular elliptic curves/$\mathbb{F}_{p^2}$ and a Γ-level structure, and edges are isogenies $\psi : (E,\Gamma(P,Q)) \to (E',\Gamma(P',Q'))$ such that $\psi(\Gamma(P,Q)) = \Gamma(P',Q')$.



Eg. $\Gamma_0(N)$-structures.
Vertices (E,G) with $G \leq E[N]$ of order N
End$(E,G) = \{\alpha \in \text{End}(E) \mid \alpha(G) \subseteq G\}$ isomorphic to Eichler order.

On the left the $\Gamma_0(3)$ supersingular 2-isogeny graph.

$14 \leftrightarrow \{(E_0,G_1),(E_0,G_2),(E_0,G_3)\}$ where G_1,G_2,G_3 maps to each other under the automorphism of E_0; they define 3 isogenies to E_3.

ORIENTED ISOGENY GRAPHS WITH LEVEL STRUCTURE

We will write $G_S(\mathsf{SS}_K(p,\Gamma))$ or $G_S(\mathsf{SS}_{\mathcal{O}}(p,\Gamma))$ for the supersingular isogeny graphs oriented by K with Γ-level structure.

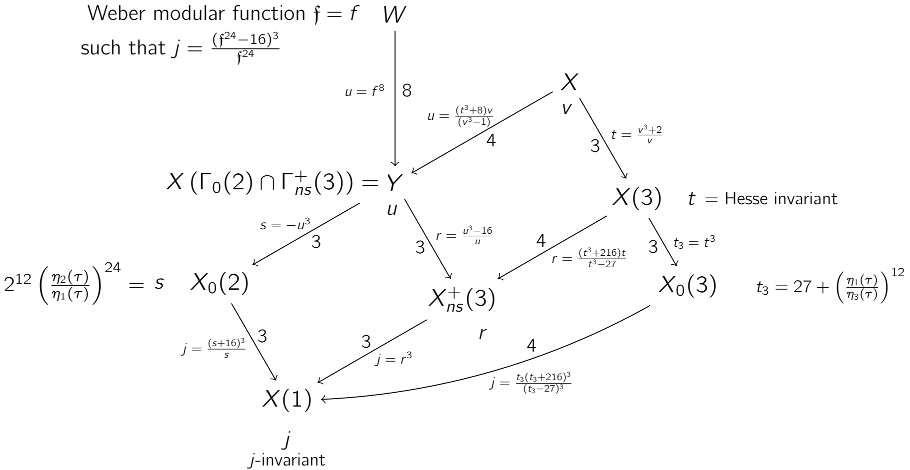
Once again we have covers

$$G_S(\mathsf{SS}_K(p,\Gamma)) \to G_S(E,K) \qquad G_S(\mathsf{SS}_{\mathcal{O}}(p,\Gamma)) \to G_S(E,\mathcal{O})$$

The action of ideals through isogenies lets us define an action on $G_S(\mathsf{SS}_{\mathcal{O}}(p,\Gamma))$ by a ray class group $\mathcal{C}\ell(\mathcal{O},\Gamma)$

$$\begin{aligned} \mathcal{C}\ell(\mathcal{O},\Gamma) \times \mathsf{SS}_{\mathcal{O}}(p,\Gamma) &\longrightarrow \mathsf{SS}(p,\Gamma) \\ ([\mathfrak{a}],(E,\Gamma(P,Q))) &\longrightarrow (\phi_{\mathfrak{a}}(E),\Gamma(\phi_{\mathfrak{a}}(P),\phi_{\mathfrak{a}}(Q))) \end{aligned}$$

SOME MODULAR CURVES OF INTEREST



WEBER INITIALIZATIONS

Let u be a supersingular value of the Weber function,

$$r = u^3 \qquad t = -u^8 \qquad s = t^3$$

along the chain $\mathcal{W}_8 \to Y \to X_0(2) \to X(1)$. we get

$$\Psi_2(x,y) = (x^2 - y)y + 16x \qquad \Psi_3(x,y) = x^4 - x^3y^3 + 8xy + y^4$$

The elliptic curves associated to Weber invariants are the fiber in the family:

$$y^2 + xy = x^3 - \frac{1}{u^{24} - 64}x$$

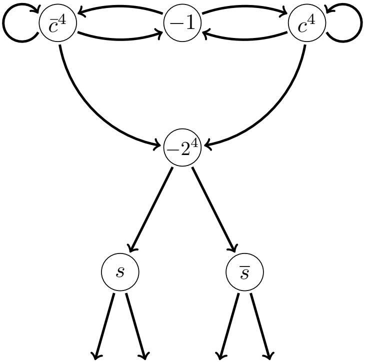
over u on the Weber curve.

The initial values with which to build the public ℓ-isogeny chains are

D	j_0	s_0	t_0	D	j_1	s_1	t_1
-3	0	-2^4	$-(\sqrt[3]{2})^4$	-12	$2^4 15^3$	-2^8	$-(\sqrt[3]{2})^8$
-4	12^3	2^3	2	-16	66^3	2^9	2^3
-7	-15^3	-1	-1	-28	255^3	-2^{12}	-2^4
-8	20^3	2^6	2^2	-32	j_1	t_1^3	$2^3(\sqrt{2}+1)$

WEBER INITIALIZATIONS - DISCRIMINANT -7

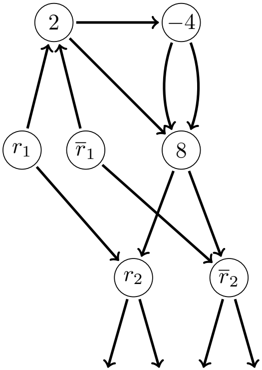
Endomorphism ring is small: generated by an endomorphism of degree 2 we avoid any pathologies associated with the extra automorphisms.



- $t_0 = -1$ and c root of $x^2 - x + 2$.
- c^4 and $\bar{c}^4$ also t-values over $j = -15^3$.
- $\Psi_2(-1, c^4) = \Psi_2(-1, \bar{c}^4) = 0$, the two extensions correspond to the horizontal 2-isogenies.
- $\Psi_2(c^4, c^4) = \Psi_2(c^4, -2^4) = 0$: the former enters a cycle the latter induces a descending isogeny.

Initialization: $(t_0, t_1, t_2, \dots)$ beginning with $(-1, c^4, -2^4, \dots)$.
Successive solutions to $\Psi_2(t_i, t_{i+1}) = 0$ are necessarily descending.
Extension: random choice of root t_{i+1} of $\Psi_2(t_i, x)$.

WEBER INITIALIZATIONS - DISCRIMINANT -4

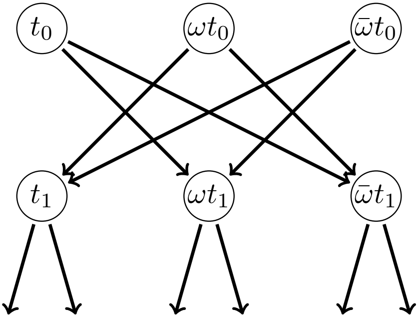


- t-invariants over $j = 12^3$ fall in two orbits of points, $\{2, 2\omega, 2\omega^2\}$ of multiplicity 2, and $\{-4, -4\omega, -4\omega^2\}$ of multiplicity 1.
- These points at the surface are linked by a 2-isogeny and to 2-depth 1, to $t = 8$.
- $\Psi_2(\omega x, \omega^2 y) = \omega\Psi_2(x, y)$: the choice of representative in the orbit gives rise to one of three distinct components of the 2-isogeny graph.

Initialization: $(t_0, t_1, t_2, \dots) = (2, 8, 8c, \dots)$ where c is a root of $x^2 - 8x - 2$.
Extension: random selection of a root t_{i+1} of $\Psi_2(t_i, x)$.

The full 2-isogeny graph has ascending edges from the depth one to $t_0 = 2$
If an isogeny is descending its only extension to a 2-isogeny chain is descending

WEBER INITIALIZATIONS - DISCRIMINANT -3

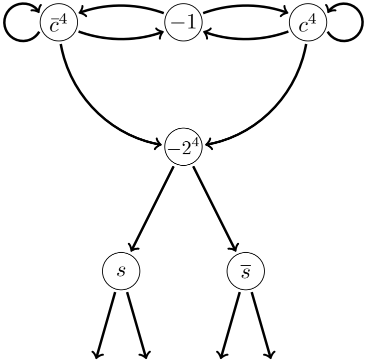


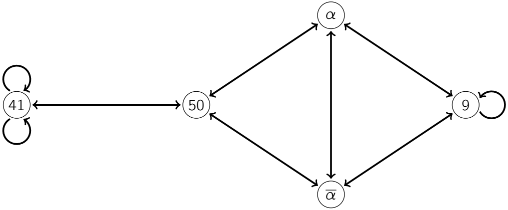
- $t_0 = -(\sqrt[3]{2})^4 = -2\sqrt[3]{2}$.
- $\{t_0, t_0\omega, t_0\omega^2\}$ are t-values over $j = 0$, each of multiplicity 3
- $t_1 = -t_0^2$, and $\Psi_2(t_0, t_1\omega) = \Psi_2(t_0, t_1\omega^2) = 0$,

Since 2 is inert, every path from t_0 is descending, so we may initialize the 2-isogeny chain with $(t_0, t_1\omega)$.

There are additional t-invariants at each depth > 0 which admit ascending and descending isogenies.
Any descending isogenies must rejoin this graph of descending isogenies from the surface.

WEBER INITIALIZATIONS - COVERING GRAPHS





THANK YOU FOR YOUR ATTENTION