Marseille, 19 May 2022

L.COLÒ I2M

A MODULAR APPROACH TO OSIDH

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 $G = (E, S)$

- 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 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).

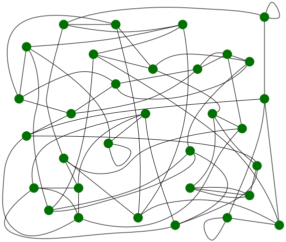
SUPERSINGULAR ISOGENY GRAPHS

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 $p \equiv 3 \mod 4$

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

  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 $p \equiv 2 \mod 3$

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

  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

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

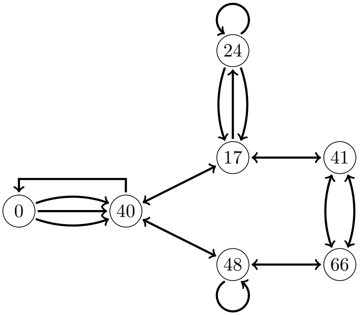
ORIENTED ISOGENY GRAPHS - STRUCTURE

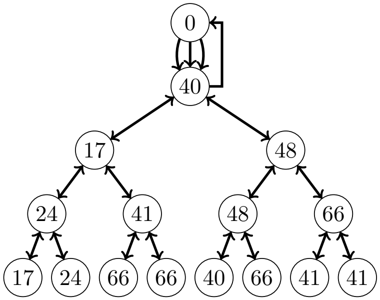
The orientation by a quadratic imaginary field gives to supersingular isogeny graphs the rigid structure of a volcano. It also differentiates vertices in the descending paths from the crater, determining an infinite graph.

$G_\ell(E, K)$ 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.

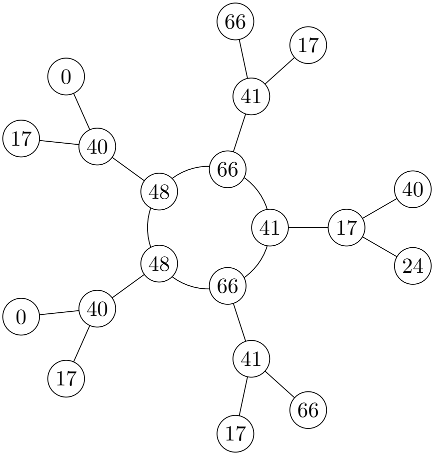
Let $E_0/\mathbb{F}_{71}$ be the supersingular elliptic curve with $j(E)=0$, oriented by the order $\mathcal{O}_K=\mathbb{Z}[\omega]$, where $\omega^2+\omega+1=0$. The unoriented 2-isogeny graph is the finite graph on the left.
The orientation by $K=\mathbb{Q}[\omega]$ differentiates vertices in the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

L.COLÒ I2M

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.

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 $F_i = E_i/C_i$.

This construction motivates the following definition.

Definition

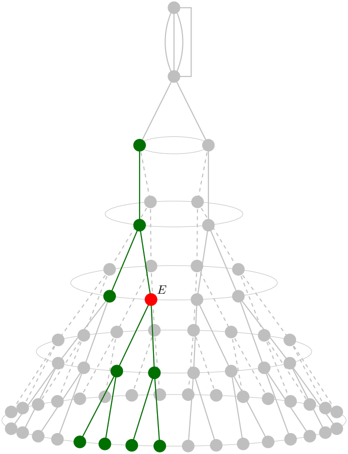
An ℓ-ladder of length n and degree q is a commutative diagram of ℓ-isogeny chains (E_i, ϕ_i), (F_i, ϕ_i') of length n connected by q-isogenies $\psi_i : E_i \to F_i$

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

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.

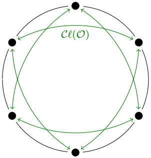
CLOUDS

In order to discuss the local neighborhood of a graph, we introduce the notion of an ℓ-isogeny cloud around E: this is a subgraph of $G_\ell(E)$, whose paths from E extend to length r.

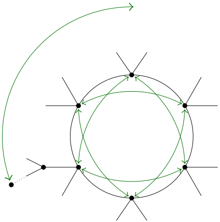


VORTICES & WHIRLPOOLS

We define a vortex to be the ℓ-isogeny subgraph $G_\ell(E,\mathcal{O})$ of $G_\ell(E,K)$ whose vertices are isomorphism classes of $\mathcal{O}$-oriented elliptic curves with ℓ-maximal endomorphism ring, equipped with an action of $\mathcal{C}\ell(\mathcal{O})$.



A *whirlpool* will be a complete isogeny volcano (the union of the subgraphs $G_\ell(E,\mathcal{O}_n)$) acted on by a compatible action of the class group $\mathcal{C}\ell(\mathcal{O}_n)$. We would like to think at isogeny graphs as moving objects.



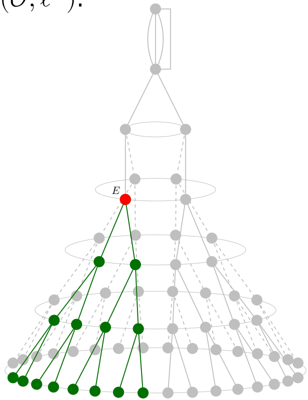
EDDIES

Given an order $\mathcal{O}$, we write $\mathcal{O}(M) = \mathbb{Z} + M\mathcal{O}$ - the order of index M, and $O_n = \mathcal{O}(\ell^n)$. Moreover, we denote the kernel

$$U(\mathcal{O}, M) = \mathsf{ker}(\mathcal{C}\ell(\mathcal{O}(M)) \longrightarrow \mathcal{C}\ell(\mathcal{O}))$$

which is the stabilizer of an isomorphism class of a curve oriented by $\mathcal{O}$.

An Eddy at E is the subgroup of ℓ-isogenies descending from E, equipped with the compatible action of $U(\mathcal{O}, \ell^n)$.



INITIALIZING THE LADDER

L.COLÒ

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:

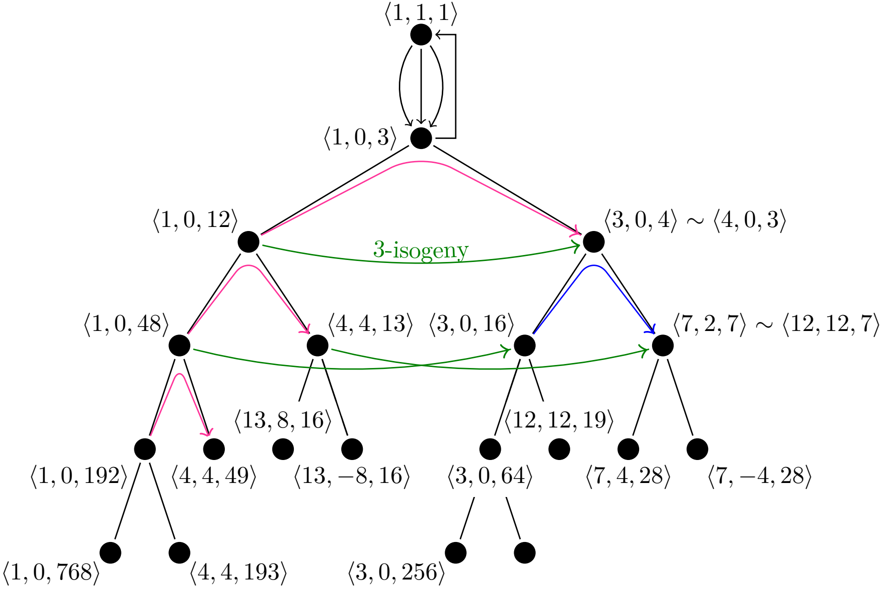
$$\{\langle 1, 0, 48\rangle, \langle 3, 0, 16\rangle, \langle 4, 4, 13\rangle, \langle 7, 2, 7\rangle\}.$$

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.

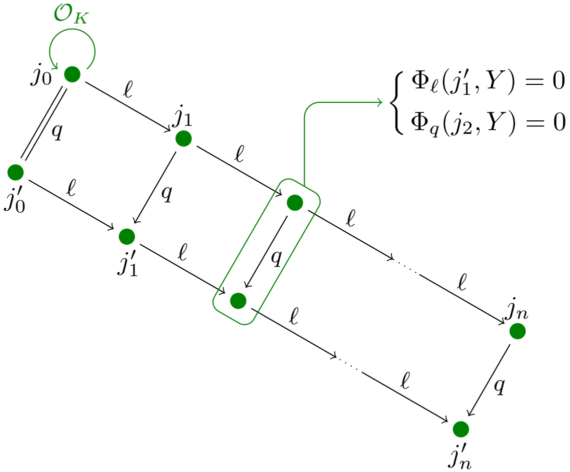
INITIALIZING THE LADDER - A PICTURE



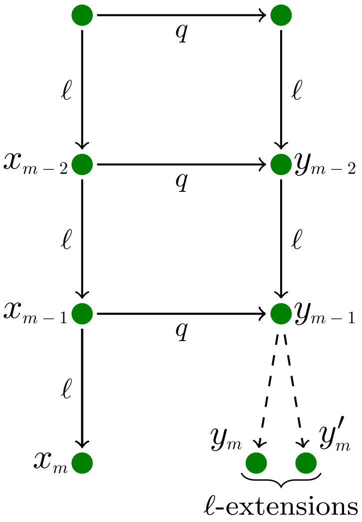
INITIALIZING THE LADDER - A TABLE

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

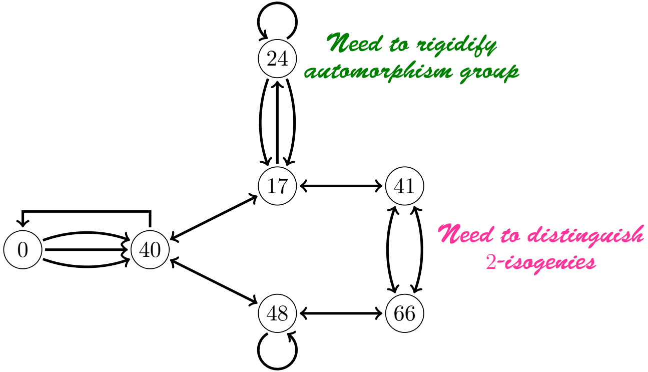
There are multiple reasons to add level structure to our construction:

- 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 $\mathcal{C}\ell(\mathcal{O}, \Gamma)$).

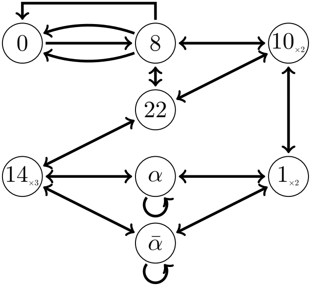
ADDING LEVEL STRUCTURE

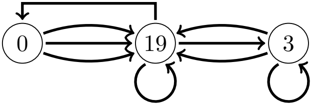
There are multiple reasons to add level structure to our construction:

- 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

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$(E,G) \;=\; \{\alpha \in \text{End}(E) \,|\, \alpha(G) \subseteq G\}$
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 FOR OSIDH

Weber modular function $\mathfrak{f} = f$ such that $j = \frac{(\mathfrak{f}^{24}-16)^3}{\mathfrak{f}^{24}}$

t = Hesse invariant

$2^{12}\left(\frac{\eta_2(\tau)}{\eta_1(\tau)}\right)^{24} = s$

$t_3 = 27 + \left(\frac{\eta_1(\tau)}{\eta_3(\tau)}\right)^{12}$

$$
\begin{tikzcd}
 & W \arrow[d, "u=f^8"', "8"] & & \underset{v}{X} \arrow[dll, "u=\frac{(t^3+8)v}{(v^3-1)}"', "4"] \arrow[dr, "3"', "t=\frac{v^3+2}{v}"] & & \\
 & X\left(\Gamma_0(2)\cap\Gamma_{ns}^{+}(3)\right) = \underset{u}{Y} \arrow[dl, "s=-u^3"', "3"] \arrow[dr, "3"', "r=\frac{u^3-16}{u}"] & & & X(3) \arrow[dll, "4"', "r=\frac{(t^3+216)t}{t^3-27}"] \arrow[dr, "3"', "t_3=t^3"] & \\
X_0(2) \arrow[dr, "j=\frac{(s+16)^3}{s}"', "3"] & & \underset{r}{X_{ns}^{+}(3)} \arrow[dl, "3"', "j=r^3"] & & & X_0(3) \arrow[llll, bend left, "4"', "j=\frac{t_3(t_3+216)^3}{(t_3-27)^3}"] \\
 & \underset{j}{X(1)} & & & &
\end{tikzcd}
$$

j-invariant

WEBER MODULAR FUNCTIONS

Introduced by H. Weber, they are

$$\mathfrak{f}(\tau) = \zeta_{48}^{-1}\frac{\eta\left(\frac{\tau+1}{2}\right)}{\eta(\tau)} = q^{-\frac{1}{48}}\prod_{n=1}^{+\infty}(1+q^{n-\frac{1}{2}})$$

$$\mathfrak{f}_1(\tau) = \frac{\eta\left(\frac{\tau}{2}\right)}{\eta(\tau)} = q^{-\frac{1}{48}}\prod_{n=1}^{+\infty}(1-q^{n-\frac{1}{2}})$$

$$\mathfrak{f}_2(\tau) = \sqrt{2}\frac{\eta\left(2\tau\right)}{\eta(\tau)} = \sqrt{2}q^{\frac{1}{24}}\prod_{n=1}^{+\infty}(1+q^{n})$$

Historically, $\mathfrak{f}_2$ was the first to be studied by Weber, who eventually introduced the others such that

$$(X+\mathfrak{f}^8)(X-\mathfrak{f}_1^8)(X-\mathfrak{f}_2^8) = X^3 - \gamma_2 X + 16$$

WEBER MODULAR FUNCTIONS - PROPERTIES

L.COLÒ I2M

The previous relation $(X+\mathfrak{f}^8)(X-\mathfrak{f}_1^8)(X-\mathfrak{f}_2^8) = X^3 - \gamma_2 X + 16$ yields

- $\mathfrak{f}^8 = \mathfrak{f}_1^8 + \mathfrak{f}_2^8$

Weber modular functions - properties

The previous relation $(X+\mathfrak{f}^8)(X-\mathfrak{f}_1^8)(X-\mathfrak{f}_2^8) = X^3 - \gamma_2 X + 16$ yields

- $\mathfrak{f}^8 = \mathfrak{f}_1^8 + \mathfrak{f}_2^8$
- $\mathfrak{f}_1(2\tau)\mathfrak{f}_2(\tau) = \mathfrak{f}(\tau)\mathfrak{f}_1(\tau)\mathfrak{f}_2(\tau) = \sqrt{2}$

Weber modular functions - properties

The previous relation $(X+\mathfrak{f}^8)(X-\mathfrak{f}_1^8)(X-\mathfrak{f}_2^8) = X^3 - \gamma_2 X + 16$ yields

- $\mathfrak{f}^8 = \mathfrak{f}_1^8 + \mathfrak{f}_2^8$
- $\mathfrak{f}_1(2\tau)\mathfrak{f}_2(\tau) = \mathfrak{f}(\tau)\mathfrak{f}_1(\tau)\mathfrak{f}_2(\tau) = \sqrt{2}$

which gives

- $\zeta_{48}^{-1}\eta\left(\frac{\tau+1}{2}\right)\eta\left(\frac{\tau}{2}\right)\eta(2\tau) = \eta(\tau)^3$

WEBER MODULAR FUNCTIONS - PROPERTIES

L.COLÒ I2M

The previous relation $(X+\mathfrak{f}^8)(X-\mathfrak{f}_1^8)(X-\mathfrak{f}_2^8) = X^3 - \gamma_2 X + 16$ yields

- $\mathfrak{f}^8 = \mathfrak{f}_1^8 + \mathfrak{f}_2^8$
- $\mathfrak{f}_1(2\tau)\mathfrak{f}_2(\tau) = \mathfrak{f}(\tau)\mathfrak{f}_1(\tau)\mathfrak{f}_2(\tau) = \sqrt{2}$

which gives

- $\zeta_{48}^{-1}\eta\left(\frac{\tau+1}{2}\right)\eta\left(\frac{\tau}{2}\right)\eta(2\tau) = \eta(\tau)^3$

They have transformation formulæ

- $(\mathfrak{f}, \mathfrak{f}_1, \mathfrak{f}_2) \circ S = (\mathfrak{f}, \mathfrak{f}_2, \mathfrak{f}_1)$
- $(\mathfrak{f}, \mathfrak{f}_1, \mathfrak{f}_2) \circ T = (\zeta_{48}^{-1}\mathfrak{f}_1, \zeta_{48}^{-1}\mathfrak{f}, \zeta_{24}\mathfrak{f}_2)$

WEBER MODULAR FUNCTIONS - PROPERTIES

The previous relation $(X+\mathfrak{f}^8)(X-\mathfrak{f}_1^8)(X-\mathfrak{f}_2^8) = X^3 - \gamma_2 X + 16$ yields

- $\mathfrak{f}^8 = \mathfrak{f}_1^8 + \mathfrak{f}_2^8$
- $\mathfrak{f}_1(2\tau)\mathfrak{f}_2(\tau) = \mathfrak{f}(\tau)\mathfrak{f}_1(\tau)\mathfrak{f}_2(\tau) = \sqrt{2}$

which gives

- $\zeta_{48}^{-1}\eta\left(\frac{\tau+1}{2}\right)\eta\left(\frac{\tau}{2}\right)\eta(2\tau) = \eta(\tau)^3$

They have transformation formulæ

- $(\mathfrak{f}, \mathfrak{f}_1, \mathfrak{f}_2) \circ S = (\mathfrak{f}, \mathfrak{f}_2, \mathfrak{f}_1)$
- $(\mathfrak{f}, \mathfrak{f}_1, \mathfrak{f}_2) \circ T = (\zeta_{48}^{-1}\mathfrak{f}_1, \zeta_{48}^{-1}\mathfrak{f}, \zeta_{24}\mathfrak{f}_2)$

and relations with the j-invariant

- $j = \frac{(\mathfrak{f}^{24}-16)^3}{\mathfrak{f}^{24}} = \frac{(\mathfrak{f}_1^{24}+16)^3}{\mathfrak{f}_1^{24}} = \frac{(\mathfrak{f}_2^{24}+16)^3}{\mathfrak{f}_2^{24}}$

WEBER MODULAR POLYNOMIALS

$\mathfrak{f}(\tau)$ is a modular function of level 48 giving a degree 72 cover of the j-line.

The modular polynomials with respect to $\mathfrak{f}$ are the new (Weber) integral polynomials $\Phi_q(x, y)$ such that

$$\Phi_q\left(\mathfrak{f}(\tau), \mathfrak{f}(q\tau)\right) = 0$$

Division Polynomials

Asymptotically, modular polynomials have q^2 monomials, but the symmetry $\Phi_q(\zeta_{24}x, \zeta_{24}^q y) = \zeta_{24}^{q+1}(x, y)$ yields a great sparsness:

$$\Phi_5(x, y) = x^6 - x^5y^5 + 4xy + y^6$$
$$\Phi_7(x, y) = x^8 - x^7y^7 + 7x^4y^4 - 8xy + y^8$$
$$\Phi_{11}(x, y) = x^{12} - x^{11}y^{11} + 11x^9y^9 - 44x^7y^7 + 88x^5y^5 - 88x^3y^3 + 32xy + y^{12}$$

WEBER MODULAR POLYNOMIALS - FURTHER REDUCTIONS

L.COLÒ I2M

For $\ell = 2$ or $\ell = 3$, the 48-level structure gives the modular polynomials $\Phi_2(x, y)$ and $\Phi_3(x, y)$ a particular form.

- We descend the 2-level structure by setting $t = -\mathfrak{f}^8$, so that $j = \left(\frac{t^3+16}{t}\right)^3$. We obtain the modular polynomial:

$$\Psi_2(x, y) = (x^2 - y)y + 16x$$

and the Weber modular polynomial $\Phi_2(x, y) = -\Psi_2(-x^8, -y^8)$ remains irreducible

- A similar descent of the 3-level to the function $r = \mathfrak{f}^3$, gives the modular polynomial

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

such that $\Psi_3(r(\tau), r(3\tau)) = 0$, for which $\Phi_3(x, y) = \Psi_3(x^3, y^3)$ is irreducible.

WEBER CURVES

L.COLÒ I2M

We fix the normalization $(\mathfrak{u}_0, \mathfrak{u}_1, \mathfrak{u}_2) = (\mathfrak{f}, \zeta_{16}\mathfrak{f}_1, \zeta_{16}^{-1}\mathfrak{f}_2)$.
Notice that $\{\zeta_{24}^j \mathfrak{u}_i \mid j \in \mathbb{Z}/24\mathbb{Z}\}$ are the 72 roots of

$$(X^{24} - 16)^3 - j(q)X \in \mathbb{Q}(\zeta_{24})[[q^{1/24}]]$$

The map determined by the normalized Weber functions $(\mathfrak{u}_0^m : \mathfrak{u}_1^m : \mathfrak{u}_2^m : 1)$ determines a Weber modular curve $\mathcal{W}_{3n}$ in $\mathbb{P}^3$

$$\mathcal{W}_{3n} : \begin{cases} X_0^n + X_1^n + X_2^n = 0, \\ X_0 X_1 X_2 = \sqrt{2}^m X_3^3 \end{cases}$$

for m and n such that $mn = 8$
The quotient Weber curve $\mathcal{W}_n$ is defined as the image of $(\mathfrak{u}_0^{3m} : \mathfrak{u}_1^{3m} : \mathfrak{u}_2^{3m} : 1)$:

$$\mathcal{W}_n : \begin{cases} X_0^n + X_1^n + X_2^n = 48 X_3^n, \\ X_0 X_1 X_2 = \sqrt{2}^{3m} X_3^3. \end{cases}$$

These curves are equipped with maps $\mathcal{W}_{mn} \to \mathcal{W}_n$ for each product $mn \mid 24$.

WEBER MODULAR CURVES

To each factorization $mn = 24$, the Weber curve $\mathcal{W}_n$ in $\mathbb{P}^3$, defined by the triple of Weber functions $(\mathfrak{u}_0^m, \mathfrak{u}_1^m, \mathfrak{u}_2^m)$, comes equipped with an action of $\mathsf{PSL}_2(\mathbb{Z})$.

Weber Modular Curves

We denote the kernel of the action by Γ_n, identifying the Weber curves with the modular curve $X(\Gamma_n)$.

WEBER MODULAR GROUPS

The $\mathsf{PSL}_2(\mathbb{Z})$ action on Weber functions induces a representation in $\mathsf{GL}_3(\mathbb{Q}(\zeta_n))$

$$S \longmapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & \zeta_8^{-m} \\ 0 & \zeta_8^m & 0 \end{pmatrix} \quad T \longmapsto \begin{pmatrix} 0 & \zeta_{24}^m & 0 \\ \zeta_{24}^{-m} & 0 & 0 \\ 0 & 0 & \zeta_{24}^m \end{pmatrix}$$

Its kernel Γ_n is a normal congruence subgroup of $\mathsf{PSL}_2(\mathbb{Z})$.

Noting that $\Gamma_1 \subset \Gamma_3 \cap \Gamma_8 = \Gamma_{24}$, we reduce to determining Γ_3 and the chain $\Gamma_1 \subset \Gamma_2 \subset \Gamma_4 \subset \Gamma_8$.

Proposition

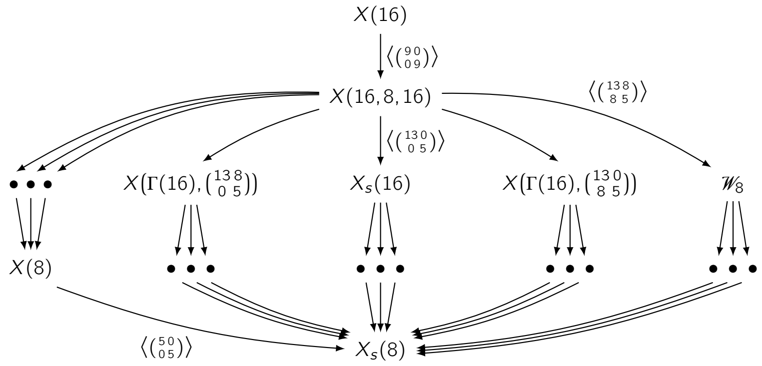
- The Weber kernel group Γ_1 equals $\Gamma(2)$ and $\mathcal{W}_1 \cong X(2)$.
- The Weber kernel group Γ_3 equals $\Gamma(2) \cap \Gamma_{ns}^+(3)$, and for each n dividing 8
$$\Gamma_{3n} = \Gamma_n \cap \Gamma_{ns}^+(3).$$
- The Weber kernel group Γ_2 equals $\Gamma(4)$ and $\mathcal{W}_2 = X(4)$.
- The Weber kernel group Γ_4 equals $\Gamma_s(8)$ and $\mathcal{W}_4 = X_s(8)$.

Weber modular groups - The group Γ_8

$$\Gamma(16) \subset \Gamma_8 \subset \Gamma_s(8) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \ : \ b \equiv c \equiv 0 \bmod 8 \right\}$$

Proposition

The Weber kernel subgroup Γ_8 is generated by $\Gamma(16)$ and $\begin{pmatrix} 13 & 8 \\ 8 & 5 \end{pmatrix}$



SUPERSINGULAR FIELDS OF DEFINITIONS

L.COLÒ I2M

Theorem

For any positive integer N, then the supersingular invariants on the modular curve $X_0(N)$ are defined over $\mathbb{F}_{p^2}$, and if $p \equiv \pm 1 \bmod N$, then the supersingular invariants also split over $\mathbb{F}_{p^2}$ on $X_1(N)$.

As a consequence, the split Cartan modular curve $X_s(N)$, defined by the congruence subgroup $\Gamma_s(N)$ also splits the supersingular moduli for every N. Then, if $p \equiv \pm 1 \bmod N$, then the supersingular invariants on the modular curve $X(N)$ are defined over $\mathbb{F}_{p^2}$.

Theorem

The supersingular Weber invariants on $\mathcal{W}_{24}$ are defined over $\mathbb{F}_{p^2}$.

$$\begin{tikzcd}
X(16,8,16) \arrow[r] \arrow[d, "\left\langle\begin{pmatrix} 13 & 8 \\ 8 & 5 \end{pmatrix}\right\rangle"'] & X(8) \arrow[d, "\left\langle\begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}\right\rangle"] \\
\mathcal{W}_8 \arrow[r] & X_s(8)
\end{tikzcd}$$

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 $\mathcal{W}_8 \to Y \to X_0(2) \to X(1)$.

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

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

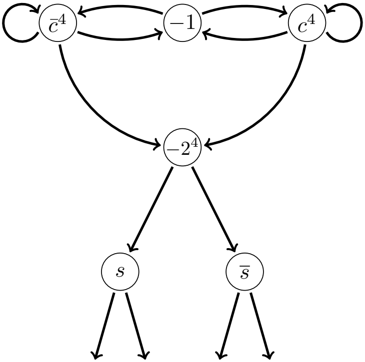
over u on the Weber curve.

The OSIDH protocol is initialized with oriented chains from an effective CM order. 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

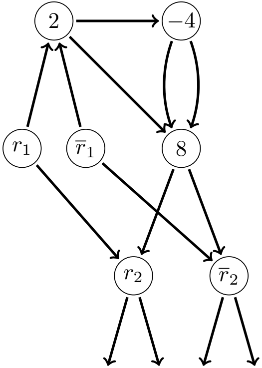
Endomorphism ring is small: generated by an endomorphism of degree 2 We avoiding any pathologies associated with the extra automorphisms.



- $t_0 = -1$ 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

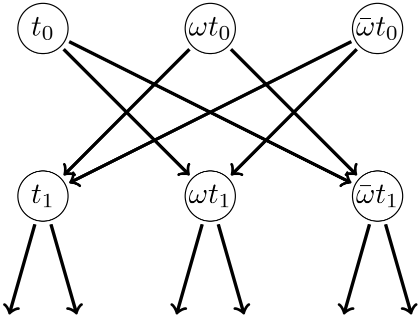


- t-invariants over $j = 12^3$ fall in two orbits of points, $\{2, 2\omega, 2\omega^2\}$ of multiplicity 2, and $\{-4, -4\omega, -4\omega^2\}$ of multiplicity 1.
- These points at the surface are linked by a 2-isogeny and to 2-depth 1, to $t = 8$.
- $\Psi_2(\omega x, \omega^2 y) = \omega \Psi_2(x, y)$: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

THANK YOU FOR YOUR ATTENTION