Isogeny graphs with real multiplication

Sorina Ionica

Ecole Normale Supérieure de Paris

joint work with Emmanuel Thomé

Isogeny graphs

Kohel 1996: Graph with vertices elliptic curves defined over $\mathbb{F}_q$ and edges all rational isogenies of degree ℓ between curves.

Compute endomorphism rings locally at ℓ by depth first search.

Other applications: class polynomial computations, solving the discrete logarithm problem, hash functions, public key cryptosystems.

The endomorphism ring of an ordinary elliptic curve

- An order $\mathcal{O}$ is a subring and $\mathbb{Z}$-submodule of the ring of integers $\mathcal{O}_K$ of a quadratic imaginary field K.
- Denote by $f = [\mathcal{O}_K : \mathcal{O}]$ the conductor. Then $\mathcal{O} = [1, f\omega_K]$.

$$\begin{array}{ll} \mathcal{O}_K & \leftarrow \omega_K \\ | f & \\ \mathrm{End}(E) & \leftarrow f\omega_K \\ | \frac{g}{f} & \\ \mathbb{Z}[\pi] & \leftarrow g\omega_K \end{array}$$

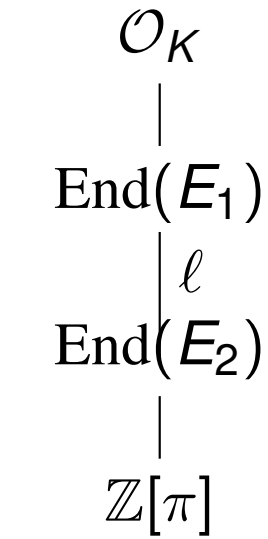
with $g^2 d_K = t^2 - 4q$

Computing the endomorphism ring of an ordinary curve $E/\mathbb{F}_q$ means locating it in the diagram.

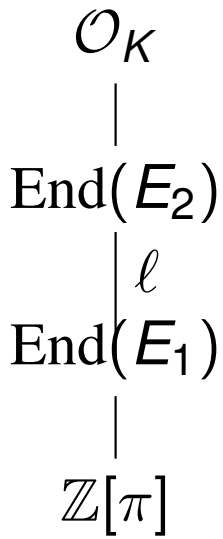
Isogenies and endomorphism rings

The ℓ-isogeny graph has vertices $Ell_t(\mathbb{F}_q)$ and edges ℓ-isogenies defined over $\mathbb{F}_q$.

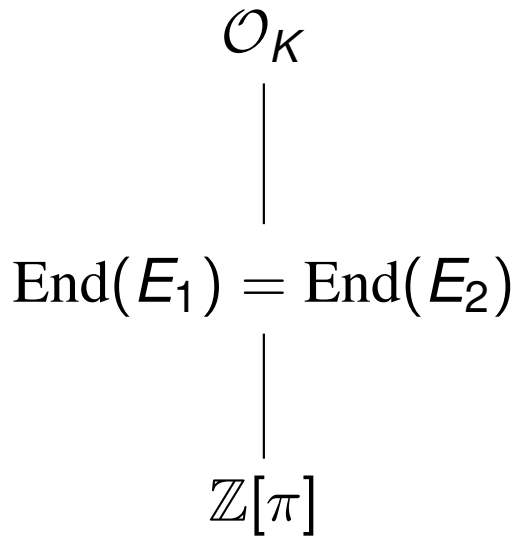
Let $\phi : E_1 \to E_2$ be an isogeny of degree ℓ.



descending



ascending



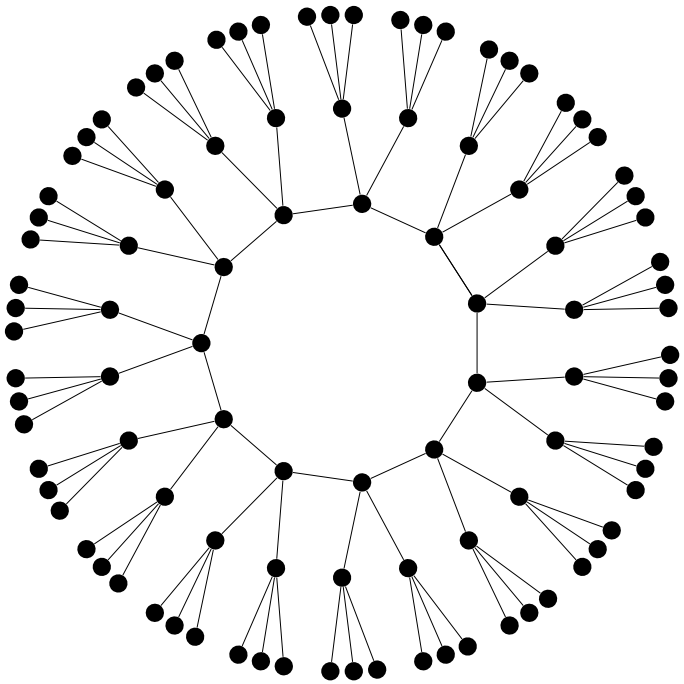
horizontal

Isogenies and ℓ-volcanoes

Let h be the ℓ-adic valuation of the conductor g of $\mathbb{Z}[\pi]$.

Kohel's theorem

Connected components of $Ell_t(\mathbb{F}_q)$ are ℓ-volcanoes of height h.



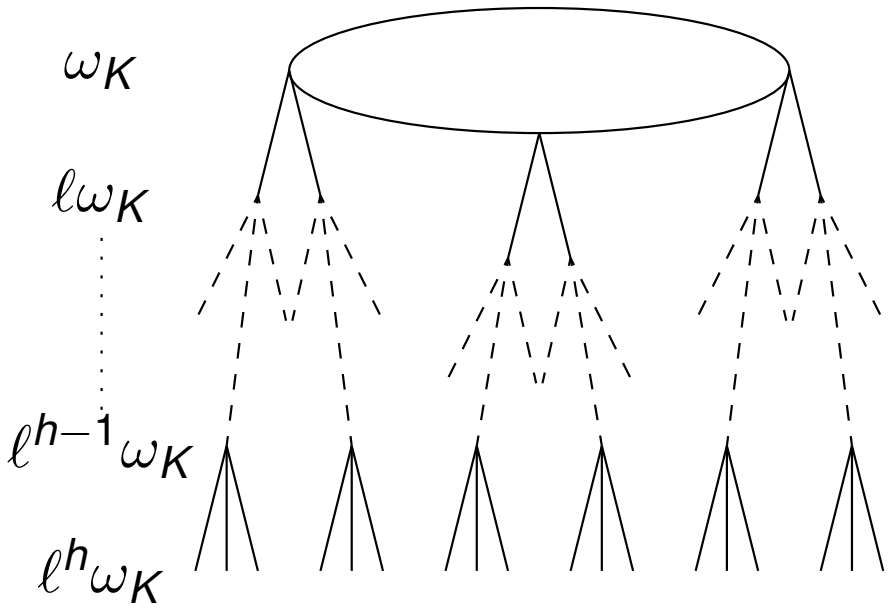
Number of horizontal isogenies starting from given vertex depends on the splitting of ℓ in $\mathcal{O}_K$.

Isogenies and ℓ-volcanoes

Let h be the ℓ-adic valuation of the conductor g of $\mathbb{Z}[\pi]$.

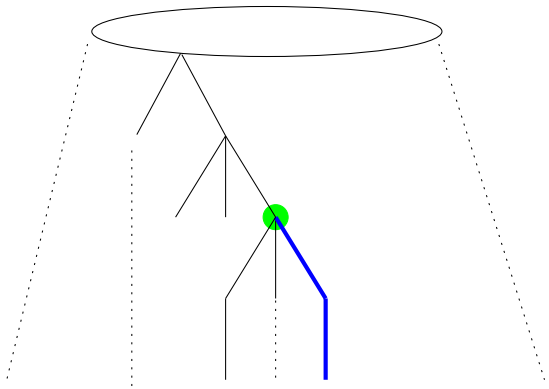
Kohel's theorem

Connected components of $Ell_t(\mathbb{F}_q)$ are ℓ-volcanoes of height h (assuming $j \neq 0, 1728$).



Curves on a fixed level have the same endomorphism ring.

Depth first search



- Find a way to the floor.
- The number of steps in a short path gives the ℓ-adic valuation of the conductor.

The endomorphism ring of an ordinary jacobian

Let K be a primitive quartic CM field and assume that $K = \mathbb{Q}(\gamma)$ with

$$\gamma = i\sqrt{a + b\frac{-1+\sqrt{d}}{2}} \text{ for } d \equiv 1 \bmod 1$$
$$\gamma = i\sqrt{a + b\sqrt{d}} \text{ for } d \equiv 2, 3 \bmod 4$$

Assume real multiplication $\mathcal{O}_{K_0}$ has class number 1.

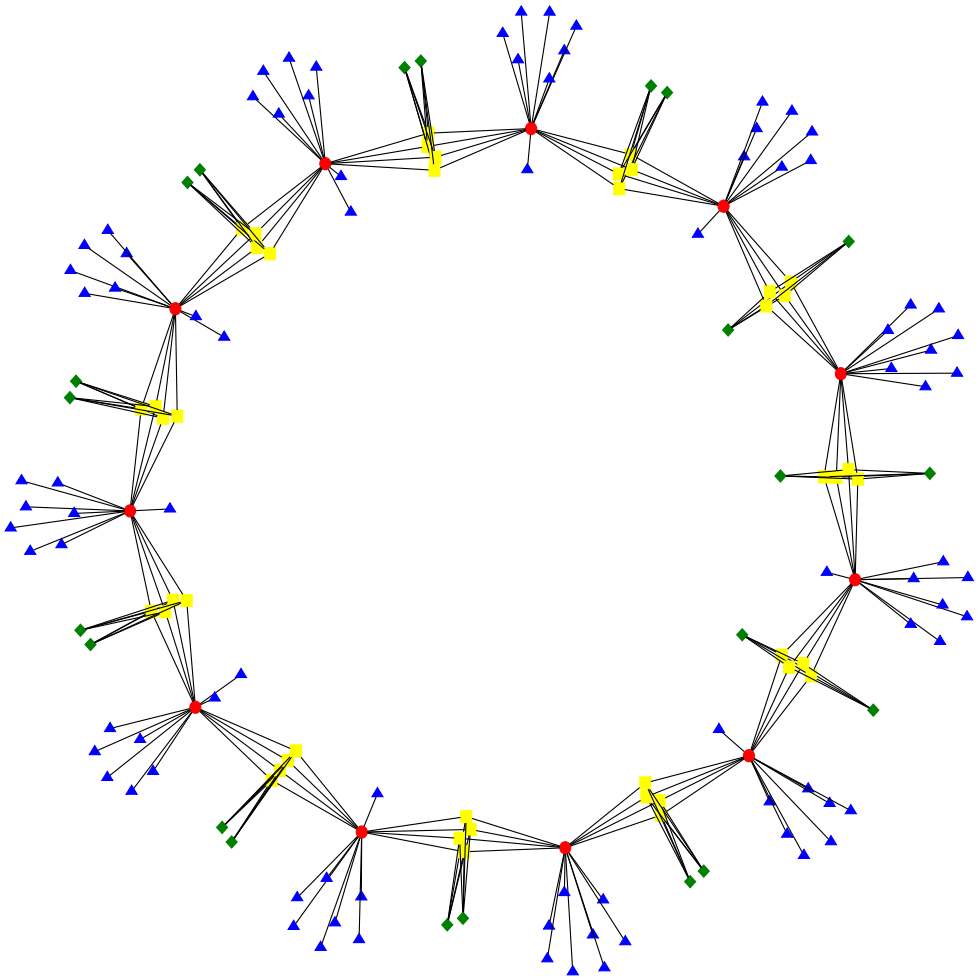
Let J be a jacobian of a genus 2 curve defined over $\mathbb{F}_q$.

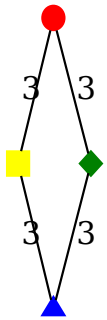
J is simple, ordinary, i.e. $\mathrm{End}(J)$ is an order of K.

$$\mathbb{Z}[\pi, \bar{\pi}] \subset \mathrm{End}(J) \subset \mathcal{O}_K$$

The (ℓ, ℓ)-isogeny graph

Cosset-Robert 2011: algebraic equations for (ℓ, ℓ)-isogenies.

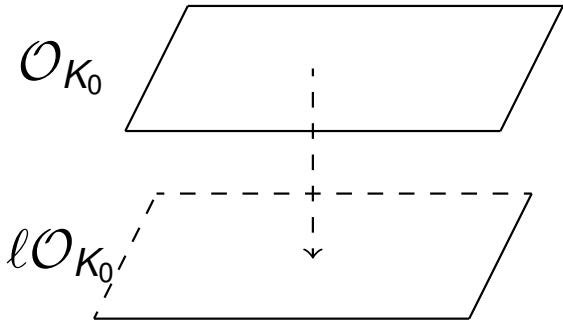




Real multiplication sub-graphs

$$\mathbb{C}^2/\Lambda_1 \oplus \Lambda_2\tau \quad \to \quad \mathbb{C}^2/\frac{\Lambda_1}{\mu} \oplus \Lambda_2\tau,$$

$$\mathbb{C}^2/\Lambda_1 \oplus \Lambda_2\tau \quad \to \quad \mathbb{C}^2/\Lambda_1 \oplus \frac{\Lambda_2}{\mu}(\tau + (\rho, \rho))$$



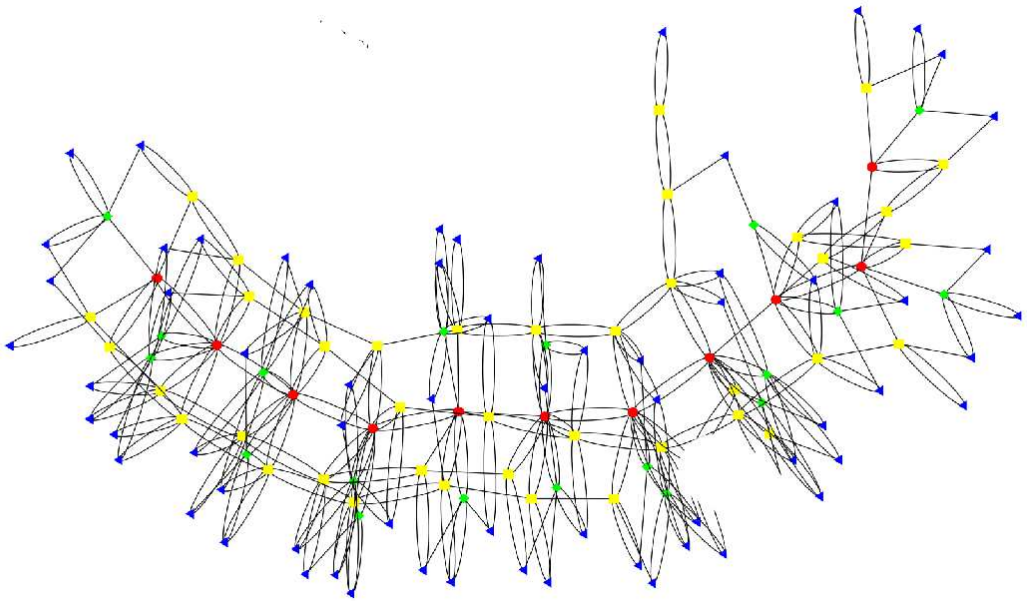
with Λ_1 and Λ_2 are lattices in K_0, $\rho \in \mathcal{O}_{K_0}$, $\tau \in \mathcal{H}_1^2$.

- These isogenies preserve real multiplication $\mathcal{O}_{K_0}$ and one may descend polarization down to principal on the target variety.
- If μ generates is a degree 1 ideal in $\mathcal{O}_{K_0}$, we get ℓ-isogenies!

Thanks to John Boxall.

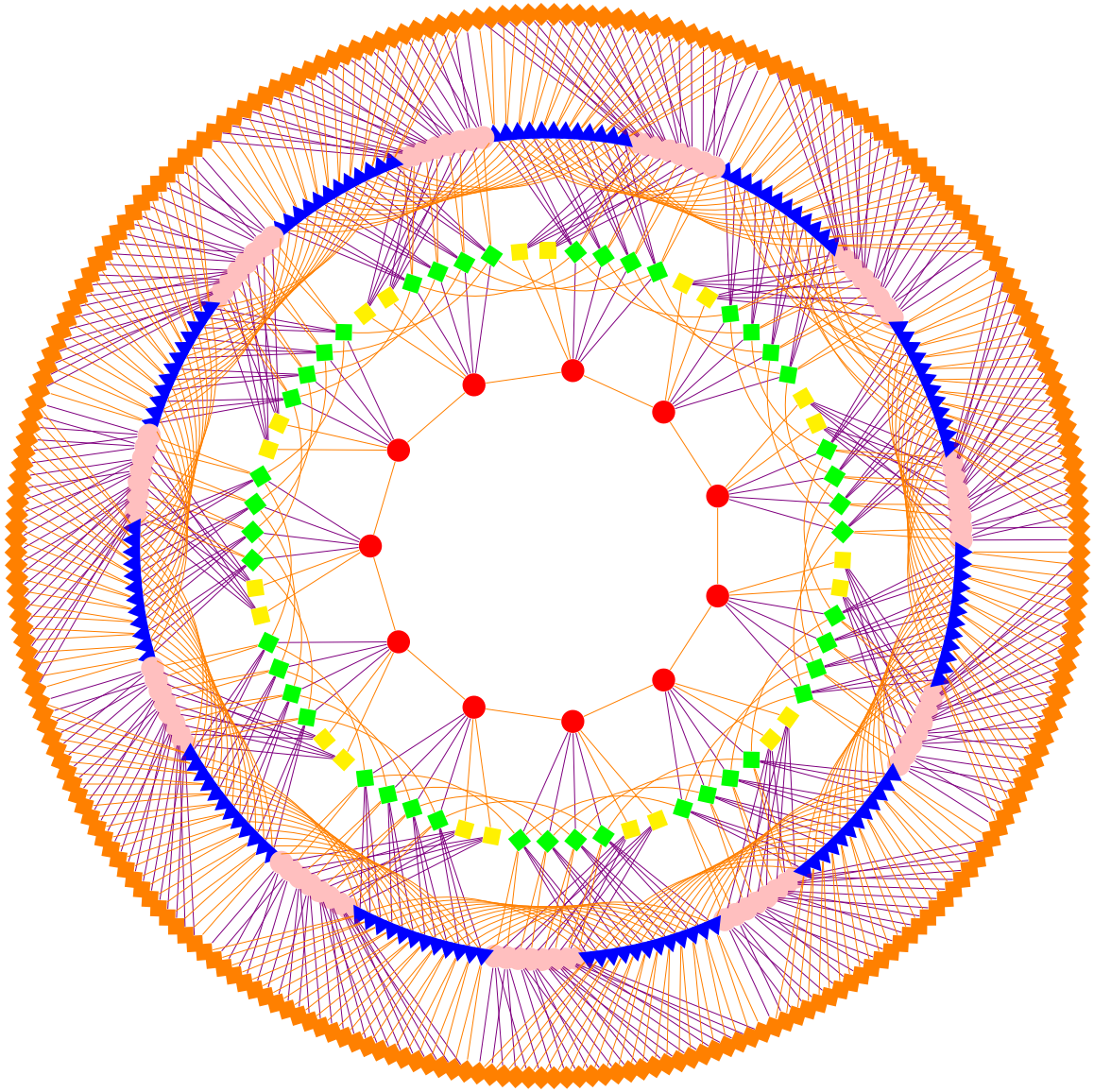
First attempts

Take ℓ such that $\ell\mathcal{O}_{K_0} = \mathfrak{l}_1\mathfrak{l}_2$.
It turns out all isogenies preserving RM are of this type.



Pretty disappointing. To be or not to be bugged...? :(

A graph!



$[A, B] = [81, 1181]$, $p = 85201$, $\ell = 3$

$\mathcal{O}_{K_0}$-orders

$$\mathcal{O}_K = \mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}\eta$$

An order which is a $\mathcal{O}_{K_0}$-module is of the form

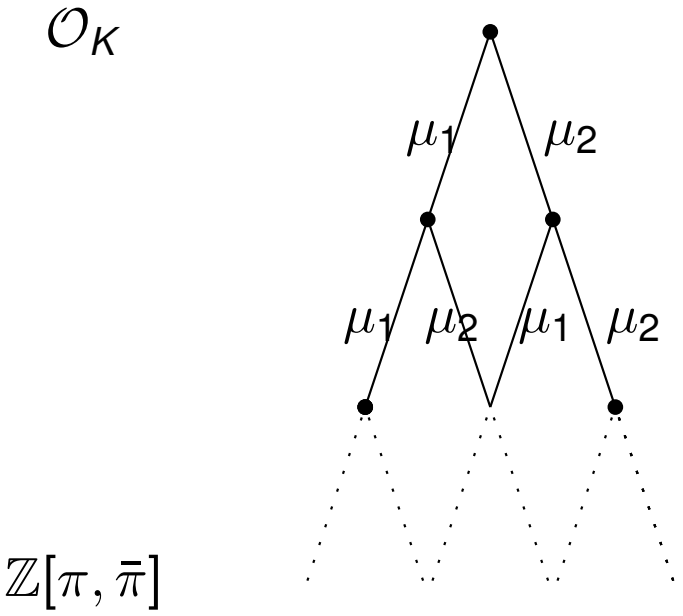
$$\mathcal{O} = \mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}(\alpha\eta).$$

The conductor is $\alpha\mathcal{O}_K$, for $\alpha \in \mathcal{O}_{K_0}$.

$$\begin{aligned} \mathfrak{f}_{\mathcal{O}} &= \{x \in \mathcal{O}_K | x\mathcal{O}_K \subseteq \mathcal{O}\} \\ &= \{x \in \mathcal{O}_K | x\eta \in \mathcal{O}\} = \mathfrak{f}_{\eta,\mathcal{O}}. \end{aligned}$$

The lattice of $\mathcal{O}_{K_0}$-orders

- Computing the endomorphism ring locally means getting $\mathfrak{f} = \ldots \mathfrak{l}_1^{\alpha_1} \mathfrak{l}_2^{\alpha_2} \ldots$.



Rational $\mathfrak{l}$-isogenies

Let $\pi \in \mathcal{O}$. We define

$$v_{\mathfrak{l},\mathcal{O}}(\theta) := max_{a \in \mathcal{O}_{K_0}} \{m | \theta + a \in \mathfrak{l}^m \mathcal{O}\}$$

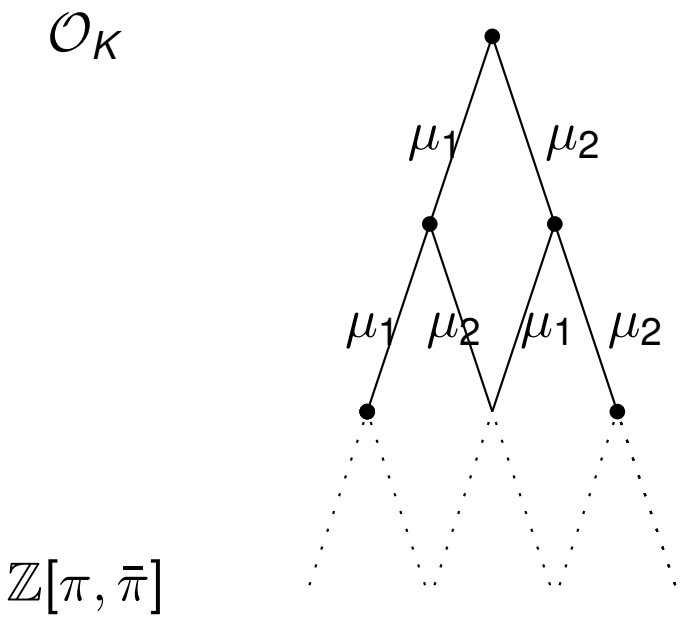
Let π be the Frobenius and write
$\pi = a_1 + a_2\sqrt{d} + (a_3 + a_4\sqrt{d})(\alpha\eta)$.

Hence $v_{\mathfrak{l}}(\mathfrak{f}_{\eta,\mathrm{End}\ J}) = v_{\mathfrak{l},\mathcal{O}_K}(\pi) - v_{\mathfrak{l},\mathrm{End}(J)}(\pi)$.

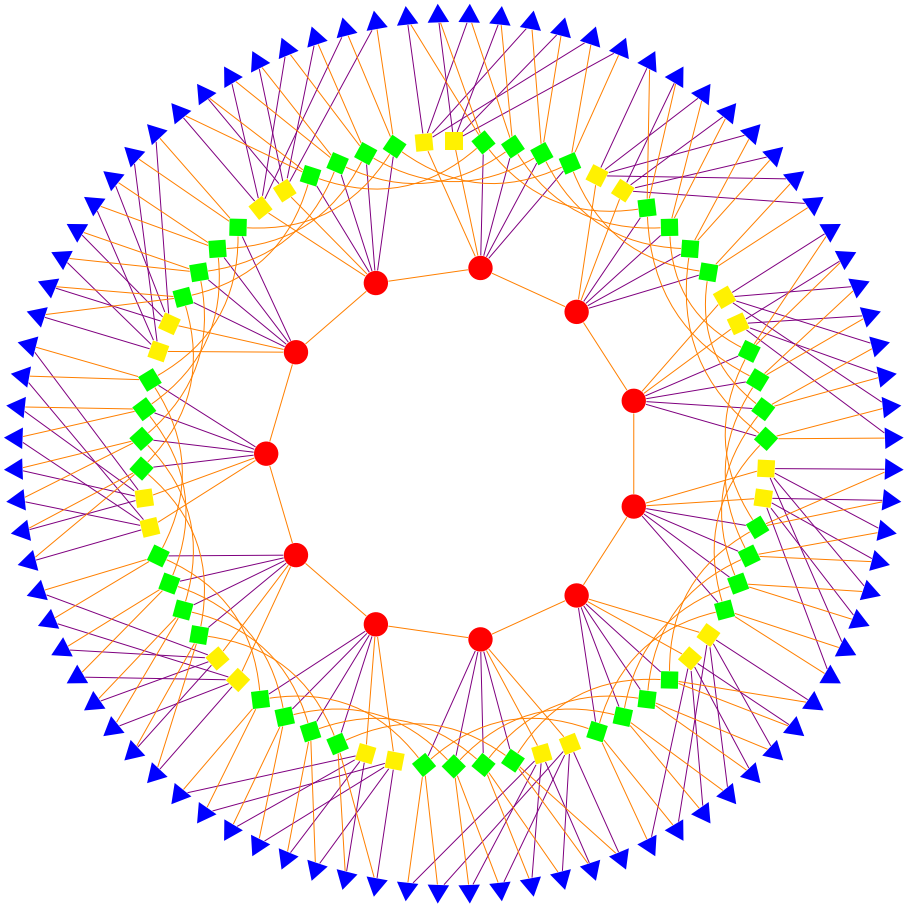
All $\mathfrak{l}$-isogenies are rational iff $v_{\mathfrak{l},\mathrm{End}(J)}(\pi) > 0$.

Classification of isogenies

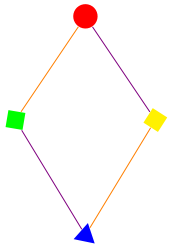
- No ℓ-isogeny between jacobians with distinct endomorphism rings lying on the same level in the lattice.
- Two types of isogenies: ascending/descending and horizontal



Real multiplication isogeny graph



$[A, B] = [81, 1181]$, $p = 211$, $\ell = 3$

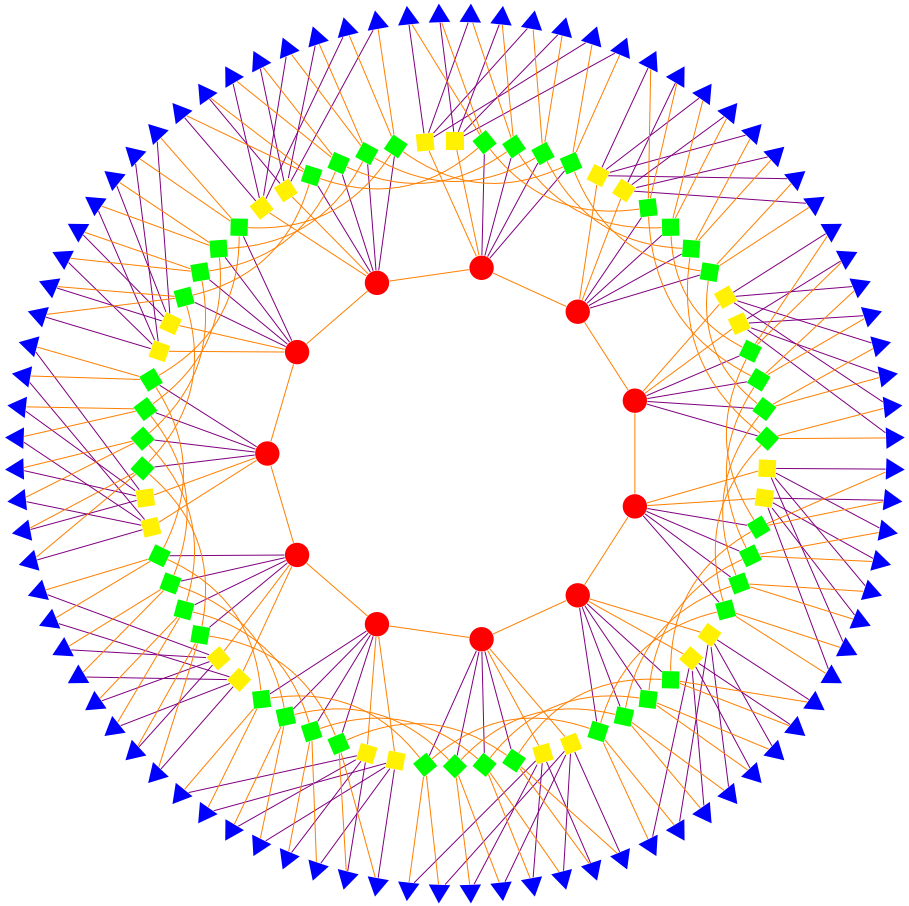


Graph structure

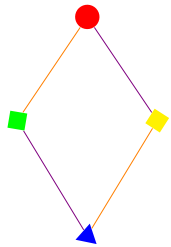
Let $\mathfrak{l}$ be an ideal of norm ℓ in $\mathcal{O}_{K_0}$.

- Assume that $\mathfrak{l}\mathcal{O}_K$ is prime with $\mathfrak{f}_{\mathcal{O}}$.
  - If $\mathfrak{l}$ is split in $\mathcal{O}_K$, there are exactly two horizontal ℓ-isogenies of kernel in $J[\mathfrak{l}]$.
  - If $\mathfrak{l}$ is ramified in $\mathcal{O}_K$, there is exactly one horizontal ℓ-isogeny in $J[\mathfrak{l}]$.
  - If $\mathfrak{l}$ is inert in K, then there are no horizontal isogenies with kernel in $J[\mathfrak{l}]$.
- If $\mathfrak{l}$ is not coprime to $\mathfrak{f}_{\mathcal{O}}$, then there is one ascending ℓ-isogeny with kernel in $J[\mathfrak{l}]$.

Real multiplication isogeny graph



$[A, B] = [81, 1181]$, $p = 211$, $\ell = 3$



$\mathfrak{l}_1$ (yellow) is split into $\mathcal{O}_K$
$\mathfrak{l}_2$ (violet) is inert into $\mathcal{O}_K$

The Tate pairing

$$\begin{aligned} J(\mathbb{F}_q)/mJ(\mathbb{F}_q) \times J[m](\mathbb{F}_q) &\rightarrow \mu_m \\ (P, Q) &\rightarrow (f_{m,P}(Q+R)/f_{m,P}(R))^{\frac{q-1}{m}} \end{aligned}$$

with $f_{m,P}$ s.t. $\mathrm{div}(f_{m,P}) \sim m(P)$.

efficiently computable with Miller's algorithm in $O(\log m)$ operations in $\mathbb{F}_q$.

Pairings on kernels

Assume that $J[\mathfrak{l}^n] \subseteq J(\mathbb{F}_q)$ and $J[\mathfrak{l}^{n+1}] \not\subseteq J(\mathbb{F}_q)$.

$k_{\mathfrak{l},J} := \max_{P \in J[\mathfrak{l}^n]}\{k | T_{\ell^n}(P,P) \in \mu_{\ell^k} \setminus \mu_{\ell^{k-1}}\}$

Let J be a jacobian whose endomorphism ring is locally maximal at ℓ.

Assume that n is the largest integer s.t. $J[\mathfrak{l}^n] \subseteq J(\mathbb{F}_q)$.

The Tate pairing is non-degenerate on $G \times G$ if

$$T_{\ell^n} : G \times G \to \mu_{\ell^{k_{\mathfrak{l},J}}}$$

is surjective. We say it is degenerate otherwise.

Theorem

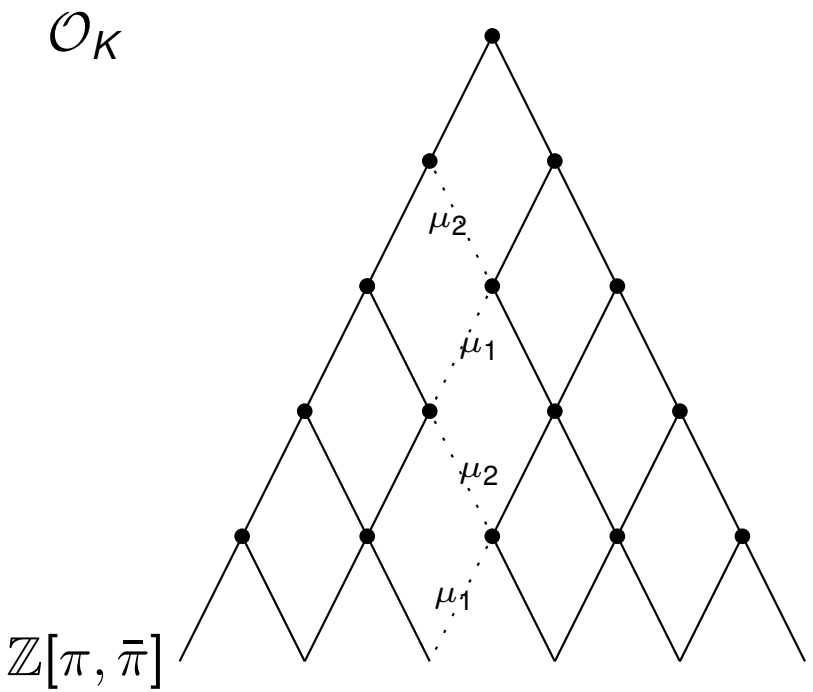
Let I be $\mathfrak{l}$-isogeny of kernel G. Take $\bar{G} \subset J[\mathfrak{l}^n]$ such that $\ell^{n-1}\bar{G} = G$.

- I is descending iff the Tate pairing is non-degenerate on $\bar{G}$.
- I is horizontal or ascending iff the Tate pairing is degenerate on $\bar{G}$.

Walking in the graph

Theorem

A (ℓ, ℓ)-isogeny preserving real multiplication is the composition of a $\mathfrak{l}_1$-isogeny with a $\mathfrak{l}_2$-isogeny.



Algorithm

Idea of the algorithm. Given J such that $[\mathcal{O}_{K_0} : \mathbb{Z}[\pi + \bar{\pi}]] = 1$. We want to compute $\mathrm{End}(J)$. The algorithm computes $v_{\mathfrak{l}_i}(\pi)$, $i = 1, 2$.

1. $\mathrm{Counter}_i \leftarrow 0$, $i := 1, 2$
2. Construct a chain (ℓ, ℓ)-isogenies until the floor is reached.
3. Each time a step I is taken in the graph
   $\mathrm{Counter}_i \leftarrow \mathrm{Counter}_i + 1$, $i = 1, 2$.
4. Return $\mathrm{Counter}_i$, $i = 1, 2$.

Computing degenerate pairings

Let P and Q be s.t. $J[\mathfrak{l}^n] = \langle P, Q \rangle$.

Using bilinearity of the ℓ^n-Tate pairing, we get

$$T_{\ell^n}(aP+bQ, aP+bQ) = T_{\ell^n}(P,P)^{a^2} (T_{\ell^n}(P,Q) T_{\ell^n}(Q,P))^{ab} T_{\ell^n}(Q,Q)^{b^2}$$

$$\begin{aligned} \mathcal{P}(a,b) &= a^2 \log(T_{\ell^n}(P,P)) + 2ab \log(T_{\ell^n}(P,Q) T_{\ell^n}(Q,P)) \\ &\quad + b^2 \log(T_{\ell^n}(Q,Q)) \end{aligned}$$

identically zero modulo $\ell^{n-k_{\mathfrak{l},J}-1}$ and nonzero modulo $\ell^{n-k_{\mathfrak{l},J}}$.

Degenerate self-pairings $\leftrightarrow$ roots of $\mathcal{P}$.

Computing endomorphism rings

Eisenträger and Lauter's algorithm (2005), Freeman-Lauter (2008)

Idea: If $\alpha : J \to J$ is an endomorphism, then $\frac{\alpha}{n}$ is an endomorphism iff $J[n] \subset \mathrm{Ker}\ \alpha$.

Check if an order $\mathcal{O}$ is contained in $\mathrm{End}(J)$:

- Write down a basis for the order $\mathcal{O}$: $\gamma_i = \frac{\alpha_i}{n_i}$, with $\alpha_i \in \mathbb{Z}[\pi]$.
- Check if $\gamma_i \in \mathrm{End}(J)$ by checking if α_i is zero on $J[n_i]$.

Since $n_i | [\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]]$ we end up working over large extension fields!

Complexity analysis

Denote by $\mathbb{F}_{q^r}$ the smallest extension field such that $J[\ell] \subset J[\mathbb{F}_{q^r}]$.

Let $n \geq 1$ be the largest integer such that $J[\ell^n] \subset J(\mathbb{F}_q)$ and $u = v_\ell([\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]])$.

Let $M(r)$ is the cost of a multiplication in F_{q^r}.

Eisenträger-Lauter	This work
$O((r\ell^{u-n} + \ell^{2u})M(r\ell^{u-n}) \log q)$ (worst case)	$O(M(r)(r \log q + \ell^{2n} + n \log \ell))$