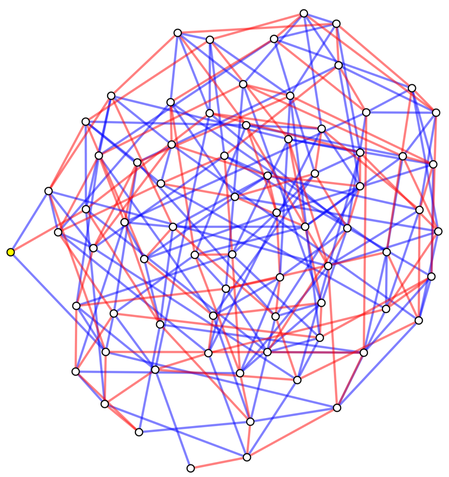
Towards a database of isogeny graphs

Enric Florit - efz1005@gmail.com
Universitat de Barcelona
Gerard Finol - gerardfinol@gmail.com
Universitat Rovira i Virgili

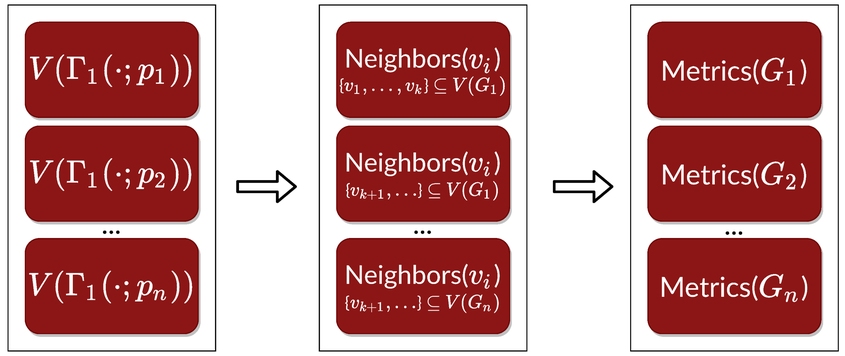
The isogeny graphs $_1(\ell; p)$

- An **elliptic curve** E over a finite field $\mathbb{F}_q$ has equation $E: y^2 = x^3 + Ax + B$. The j-invariant
$$j(E) = 1728\frac{4A^3}{4A^3 + 27B^2}$$
gives the isomorphism class of the curve. The curve is **supersingular** if its **endomorphism** ring is an order in a **quaternion algebra**.
- An **isogeny** of degree ℓ is a finite morphism of elliptic curves
$$\phi' : E \to E'$$
such that $j \ker \phi' j = \ell$.
- The **supersingular isogeny graph** $_1(\ell; p)$ is the graph of supersingular j-invariants over $\mathbb{F}_p$ and degree-ℓ isogenies between them. It is an $(\ell + 1)$-regular **Ramanujan graph**.



$_1(2; 863)$ and $_1(3; 863)$ superimposed.

We are building an open library of **supersingular isogeny graphs** of elliptic curves using **serverless computing**



1. Obtain all supersingular elliptic curves over $\mathbb{F}_{p_i^2}$

2. Find neighbors and construct each graph over ℓ and p

3. Compute properties about the graphs

Each step is computed in parallel

Visit the website:
isogenies.enricflorit.com

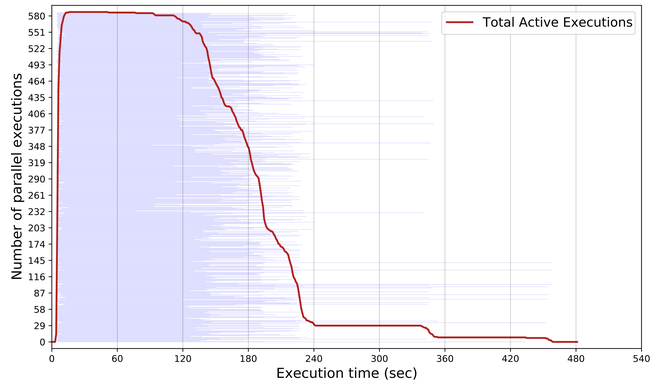
BYMAT
Bringing Young Mathematicians Together

Computing isogenies

For each prime ℓ, the ℓ**th modular polynomial** $_\ell(X; Y) \in \mathbb{Z}[X; Y]$ satisfies $_\ell(j(E); j(E')) = 0$ ( ) there is a degree-ℓ isogeny from E to E'. The roots of $_\ell(j; Y)$ are the **neighbors** of j.

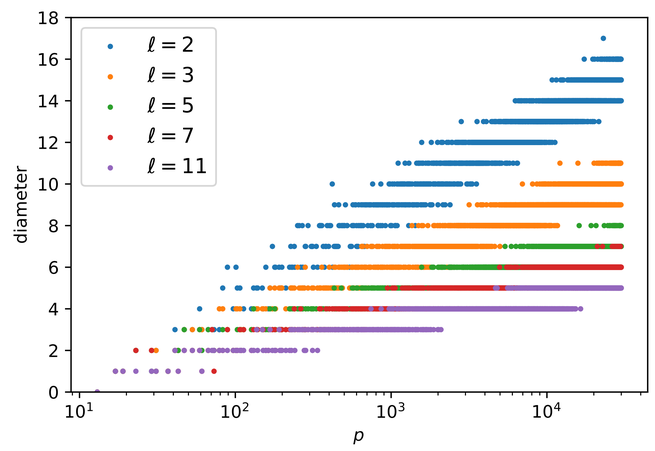
Serverless computing with Lithops

Using `lithops` we can run hundreds of parallel distributed threads to compute graphs.



Histogram of the computation of $_1(11; 4010173)$, overall time of 458 seconds.

Graph diameters



The diameter of $_1(\ell; p)$ grows as $\log p$, as predicted by the Ramanujan property.

Main references

[1] S. Arpin et al., "Adventures in Supersingularland", *arXiv preprint arXiv:1909.07779* **2019**.
[2] J. Sampe et al., "Towards Multicloud Access Transparency in Serverless Computing", *IEEE Software* **2020**, DOI 10.1109/MS.2020.3029994.