Ordinary abelian varieties: Isogeny graphs and polarizations

joint work with Edgar Costa, Taylor Dupuy, David Roe, Christelle Vincent

Stefano Marseglia

Université Côte d'Azur

ANTS XVII

Setup/Goal

Setup/Goal

- Let $\mathscr{I}_h$ be an isogeny class of ordinary abelian varieties over $\mathbb{F}_q$ $(q = p^a)$ with commutative $\mathbb{F}_q$-endomorphism algebra determined by the Weil polynomial $h(X)$, which is then squarefree.

Setup/Goal

- Let $\mathscr{I}_h$ be an isogeny class of ordinary abelian varieties over $\mathbb{F}_q$ ($q = p^a$) with commutative $\mathbb{F}_q$-endomorphism algebra determined by the Weil polynomial $h(X)$, which is then squarefree.
- Let $K = \mathbb{Q}[X]/h(X) = \mathbb{Q}[\pi]$ and $R = \mathbb{Z}[\pi, q/\pi] \subset K$.

Setup/Goal

- Let $\mathscr{I}_h$ be an isogeny class of ordinary abelian varieties over $\mathbb{F}_q$ ($q = p^a$) with commutative $\mathbb{F}_q$-endomorphism algebra determined by the Weil polynomial $h(X)$, which is then squarefree.
- Let $K = \mathbb{Q}[X]/h(X) = \mathbb{Q}[\pi]$ and $R = \mathbb{Z}[\pi, q/\pi] \subset K$.
- For $A \in \mathscr{I}_h$, identify $\mathrm{Frob}_A \mapsto \pi$, $\mathrm{End}_{\mathbb{F}_q}(A) \subset K$.

Setup/Goal

- Let $\mathscr{I}_h$ be an isogeny class of ordinary abelian varieties over $\mathbb{F}_q$ ($q = p^a$) with commutative $\mathbb{F}_q$-endomorphism algebra determined by the Weil polynomial $h(X)$, which is then squarefree.
- Let $K = \mathbb{Q}[X]/h(X) = \mathbb{Q}[\pi]$ and $R = \mathbb{Z}[\pi, q/\pi] \subset K$.
- For $A \in \mathscr{I}_h$, identify $\mathrm{Frob}_A \mapsto \pi$, $\mathrm{End}_{\mathbb{F}_q}(A) \subset K$.
- after Deligne '69: There is an equivalence $\mathscr{F}$ from the category $\mathscr{I}_h$ with $\mathbb{F}_q$-homomorphisms to the category of fractional R-ideals in K with R-linear morphisms.

Setup/Goal

- Let $\mathscr{I}_h$ be an isogeny class of ordinary abelian varieties over $\mathbb{F}_q$ ($q = p^a$) with commutative $\mathbb{F}_q$-endomorphism algebra determined by the Weil polynomial $h(X)$, which is then squarefree.
- Let $K = \mathbb{Q}[X]/h(X) = \mathbb{Q}[\pi]$ and $R = \mathbb{Z}[\pi, q/\pi] \subset K$.
- For $A \in \mathscr{I}_h$, identify $\mathrm{Frob}_A \mapsto \pi$, $\mathrm{End}_{\mathbb{F}_q}(A) \subset K$.
- after Deligne '69: There is an equivalence $\mathscr{F}$ from the category $\mathscr{I}_h$ with $\mathbb{F}_q$-homomorphisms to the category of fractional R-ideals in K with R-linear morphisms.
- $\mathscr{F}$ has been used for: isomorphism classes, principal polarizations, group of points, ...

Setup/Goal

- Let $\mathscr{I}_h$ be an isogeny class of ordinary abelian varieties over $\mathbb{F}_q$ ($q = p^a$) with commutative $\mathbb{F}_q$-endomorphism algebra determined by the Weil polynomial $h(X)$, which is then squarefree.
- Let $K = \mathbb{Q}[X]/h(X) = \mathbb{Q}[\pi]$ and $R = \mathbb{Z}[\pi, q/\pi] \subset K$.
- For $A \in \mathscr{I}_h$, identify $\mathrm{Frob}_A \mapsto \pi$, $\mathrm{End}_{\mathbb{F}_q}(A) \subset K$.
- after Deligne '69: There is an equivalence $\mathscr{F}$ from the category $\mathscr{I}_h$ with $\mathbb{F}_q$-homomorphisms to the category of fractional R-ideals in K with R-linear morphisms.
- $\mathscr{F}$ has been used for: isomorphism classes, principal polarizations, group of points, ...
- In the paper, we focus on isogenies, to efficiently return

Setup/Goal

- Let $\mathscr{I}_h$ be an isogeny class of ordinary abelian varieties over $\mathbb{F}_q$ ($q = p^a$) with commutative $\mathbb{F}_q$-endomorphism algebra determined by the Weil polynomial $h(X)$, which is then squarefree.
- Let $K = \mathbb{Q}[X]/h(X) = \mathbb{Q}[\pi]$ and $R = \mathbb{Z}[\pi, q/\pi] \subset K$.
- For $A \in \mathscr{I}_h$, identify $\mathrm{Frob}_A \mapsto \pi$, $\mathrm{End}_{\mathbb{F}_q}(A) \subset K$.
- after Deligne '69: There is an equivalence $\mathscr{F}$ from the category $\mathscr{I}_h$ with $\mathbb{F}_q$-homomorphisms to the category of fractional R-ideals in K with R-linear morphisms.
- $\mathscr{F}$ has been used for: isomorphism classes, principal polarizations, group of points, ...
- In the paper, we focus on isogenies, to efficiently return
  - non-principal polarizations (not in this talk).

Setup/Goal

- Let $\mathscr{I}_h$ be an isogeny class of ordinary abelian varieties over $\mathbb{F}_q$ ($q = p^a$) with commutative $\mathbb{F}_q$-endomorphism algebra determined by the Weil polynomial $h(X)$, which is then squarefree.
- Let $K = \mathbb{Q}[X]/h(X) = \mathbb{Q}[\pi]$ and $R = \mathbb{Z}[\pi, q/\pi] \subset K$.
- For $A \in \mathscr{I}_h$, identify $\mathrm{Frob}_A \mapsto \pi$, $\mathrm{End}_{\mathbb{F}_q}(A) \subset K$.
- after Deligne '69: There is an equivalence $\mathscr{F}$ from the category $\mathscr{I}_h$ with $\mathbb{F}_q$-homomorphisms to the category of fractional R-ideals in K with R-linear morphisms.
- $\mathscr{F}$ has been used for: isomorphism classes, principal polarizations, group of points, ...
- In the paper, we focus on isogenies, to efficiently return
  - non-principal polarizations (not in this talk).
  - isogeny graphs.

Setup/Goal

- Let $\mathscr{I}_h$ be an isogeny class of ordinary abelian varieties over $\mathbb{F}_q$ ($q = p^a$) with commutative $\mathbb{F}_q$-endomorphism algebra determined by the Weil polynomial $h(X)$, which is then squarefree.
- Let $K = \mathbb{Q}[X]/h(X) = \mathbb{Q}[\pi]$ and $R = \mathbb{Z}[\pi, q/\pi] \subset K$.
- For $A \in \mathscr{I}_h$, identify $\mathrm{Frob}_A \mapsto \pi$, $\mathrm{End}_{\mathbb{F}_q}(A) \subset K$.
- after Deligne '69: There is an equivalence $\mathscr{F}$ from the category $\mathscr{I}_h$ with $\mathbb{F}_q$-homomorphisms to the category of fractional R-ideals in K with R-linear morphisms.
- $\mathscr{F}$ has been used for: isomorphism classes, principal polarizations, group of points, ...
- In the paper, we focus on isogenies, to efficiently return
  - non-principal polarizations (not in this talk).
  - isogeny graphs.
  - pretty pictures.

An example in dimension 1

ℓ-isogeny graphs of ordinary elliptic curves

An example in dimension 1

ℓ-isogeny graphs of ordinary elliptic curves

- are very structured (thanks Kohel);

An example in dimension 1

ℓ-isogeny graphs of ordinary elliptic curves

- are very structured (thanks Kohel);
- have a very cool name ... ℓ-volcanoes (thanks Fouquet-Morain);

An example in dimension 1

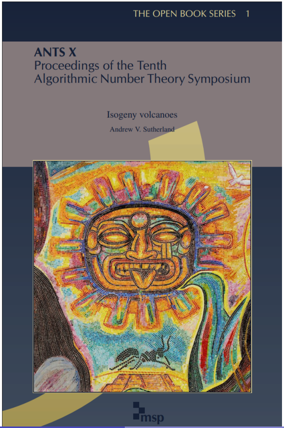
ℓ-isogeny graphs of ordinary elliptic curves

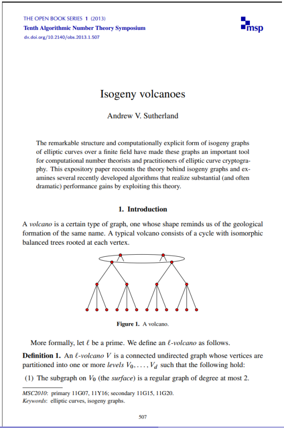
- are very structured (thanks Kohel);
- have a very cool name ... ℓ-volcanoes (thanks Fouquet-Morain);
- they are good friends of ANTS:

An example in dimension 1

ℓ-isogeny graphs of ordinary elliptic curves

- are very structured (thanks Kohel);
- have a very cool name ... ℓ-volcanoes (thanks Fouquet-Morain);
- they are good friends of ANTS:




THE OPEN BOOK SERIES 1 (2013)
Tenth Algorithmic Number Theory Symposium
dx.doi.org/10.2140/obs.2013.1.507

Isogeny volcanoes

Andrew V. Sutherland

The remarkable structure and computationally explicit form of isogeny graphs of elliptic curves over a finite field have made these graphs an important tool for computational number theorists and practitioners of elliptic curve cryptography. This expository paper recounts the theory behind isogeny graphs and examines several recently developed algorithms that realize substantial (and often dramatic) performance gains by exploiting this theory.

1. Introduction

A *volcano* is a certain type of graph, one whose shape reminds us of the geological formation of the same name. A typical volcano consists of a cycle with isomorphic balanced trees rooted at each vertex.

Figure 1. A volcano.

More formally, let ℓ be a prime. We define an ℓ-*volcano* as follows.

Definition 1. An ℓ-*volcano* V is a connected undirected graph whose vertices are partitioned into one or more *levels* $V_0, \dots, V_d$ such that the following hold:

(1) The subgraph on V_0 (the *surface*) is a regular graph of degree at most 2.

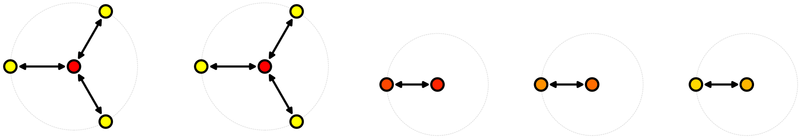
MSC2010: primary 11G07, 11Y16; secondary 11G15, 11G20.
Keywords: elliptic curves, isogeny graphs.

An example in dimension 4

Consider the geometrically simple isogeny class with LMFDB label 4.3.c_ab_af_ai.

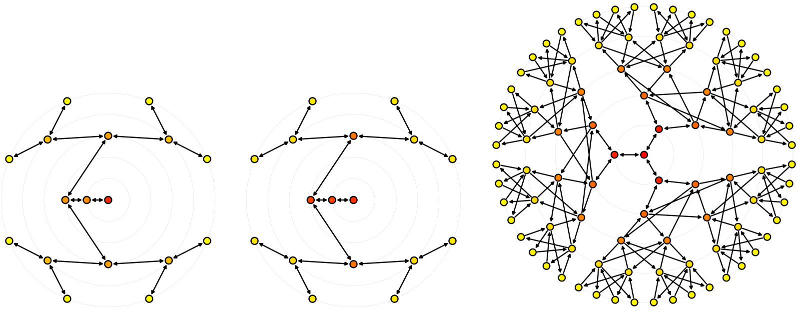
An example in dimension 4

Consider the geometrically simple isogeny class with LMFDB label 4.3.c_ab_af_ai.
The 2-isogeny graph has 14 vertices, in 5 connected components, here colored by endomorphism ring



(within each component a darker color indicates a larger End).

Base change to $\mathbb{F}_9$: 1763 isomorphism classes. Its 2-isogeny graph has 35 components: two with 49 vertices, nine with 17, twelve with 94, and twelve with 32 vertices. Some of them (same convention on colors; no relation with the previous pictures):



Definition

- An isogeny $\varphi\colon A \to B$ of degree larger than 1 is called minimal if, given a decomposition $\varphi = \psi_1 \circ \psi_2$, then either ψ_1 or ψ_2 is an isomorphism.

Definition

- An isogeny $\varphi\colon A \to B$ of degree larger than 1 is called minimal if, given a decomposition $\varphi = \psi_1 \circ \psi_2$, then either ψ_1 or ψ_2 is an isomorphism.
- The length of an isogeny φ is the smallest $r > 0$ such that there exists a decomposition $\varphi = \varphi_1 \circ \cdots \circ \varphi_r$ of φ into minimal isogenies φ_i.

Definition

- An isogeny $\varphi\colon A \to B$ of degree larger than 1 is called minimal if, given a decomposition $\varphi = \psi_1 \circ \psi_2$, then either ψ_1 or ψ_2 is an isomorphism.
- The length of an isogeny φ is the smallest $r > 0$ such that there exists a decomposition $\varphi = \varphi_1 \circ \cdots \circ \varphi_r$ of φ into minimal isogenies φ_i.

For any isogeny $\varphi\colon A \to B$ in $\mathscr{I}_h$, if $I = \mathscr{F}(A)$ and $J = \mathscr{F}(B)$ then there is an element $x \in (J : I) \cap K^\times$ such that $\mathscr{F}(\varphi) = x$.

Definition

- An isogeny $\varphi\colon A \to B$ of degree larger than 1 is called minimal if, given a decomposition $\varphi = \psi_1 \circ \psi_2$, then either ψ_1 or ψ_2 is an isomorphism.
- The length of an isogeny φ is the smallest $r > 0$ such that there exists a decomposition $\varphi = \varphi_1 \circ \cdots \circ \varphi_r$ of φ into minimal isogenies φ_i.

For any isogeny $\varphi\colon A \to B$ in $\mathscr{I}_h$, if $I = \mathscr{F}(A)$ and $J = \mathscr{F}(B)$ then there is an element $x \in (J : I) \cap K^\times$ such that $\mathscr{F}(\varphi) = x$.

From now on, we simply write $\varphi\colon A \to B \in \mathscr{I}_h \overset{\mathscr{F}}{\rightsquigarrow} x \cdot I \subseteq J$.

Definition

- An isogeny $\varphi\colon A \to B$ of degree larger than 1 is called minimal if, given a decomposition $\varphi = \psi_1 \circ \psi_2$, then either ψ_1 or ψ_2 is an isomorphism.
- The length of an isogeny φ is the smallest $r > 0$ such that there exists a decomposition $\varphi = \varphi_1 \circ \cdots \circ \varphi_r$ of φ into minimal isogenies φ_i.

For any isogeny $\varphi\colon A \to B$ in $\mathscr{I}_h$, if $I = \mathscr{F}(A)$ and $J = \mathscr{F}(B)$ then there is an element $x \in (J : I) \cap K^\times$ such that $\mathscr{F}(\varphi) = x$.

From now on, we simply write $\varphi\colon A \to B \in \mathscr{I}_h \overset{\mathscr{F}}{\rightsquigarrow} x \cdot I \subseteq J$.

Proposition

1. $\deg(\varphi) = [J : xI]$.

Definition

- An isogeny $\varphi\colon A \to B$ of degree larger than 1 is called minimal if, given a decomposition $\varphi = \psi_1 \circ \psi_2$, then either ψ_1 or ψ_2 is an isomorphism.
- The length of an isogeny φ is the smallest $r > 0$ such that there exists a decomposition $\varphi = \varphi_1 \circ \cdots \circ \varphi_r$ of φ into minimal isogenies φ_i.

For any isogeny $\varphi\colon A \to B$ in $\mathscr{I}_h$, if $I = \mathscr{F}(A)$ and $J = \mathscr{F}(B)$ then there is an element $x \in (J : I) \cap K^\times$ such that $\mathscr{F}(\varphi) = x$.

From now on, we simply write $\varphi\colon A \to B \in \mathscr{I}_h \overset{\mathscr{F}}{\rightsquigarrow} x \cdot I \subseteq J$.

Proposition

1. $\deg(\varphi) = [J : xI]$. *since ordinary: no problem at p.*

Definition

- An isogeny $\varphi\colon A \to B$ of degree larger than 1 is called minimal if, given a decomposition $\varphi = \psi_1 \circ \psi_2$, then either ψ_1 or ψ_2 is an isomorphism.
- The length of an isogeny φ is the smallest $r > 0$ such that there exists a decomposition $\varphi = \varphi_1 \circ \cdots \circ \varphi_r$ of φ into minimal isogenies φ_i.

For any isogeny $\varphi\colon A \to B$ in $\mathscr{I}_h$, if $I = \mathscr{F}(A)$ and $J = \mathscr{F}(B)$ then there is an element $x \in (J : I) \cap K^\times$ such that $\mathscr{F}(\varphi) = x$.

From now on, we simply write $\varphi\colon A \to B \in \mathscr{I}_h \overset{\mathscr{F}}{\rightsquigarrow} x \cdot I \subseteq J$.

Proposition

1. $\deg(\varphi) = [J : xI]$. *since ordinary: no problem at p.*
2. *The isogeny φ is minimal if and only if the inclusion $xI \subsetneq J$ is maximal, that is, the quotient J/xI is a simple R-module.*

Definition

- An isogeny $\varphi\colon A \to B$ of degree larger than 1 is called minimal if, given a decomposition $\varphi = \psi_1 \circ \psi_2$, then either ψ_1 or ψ_2 is an isomorphism.
- The length of an isogeny φ is the smallest $r > 0$ such that there exists a decomposition $\varphi = \varphi_1 \circ \cdots \circ \varphi_r$ of φ into minimal isogenies φ_i.

For any isogeny $\varphi\colon A \to B$ in $\mathscr{I}_h$, if $I = \mathscr{F}(A)$ and $J = \mathscr{F}(B)$ then there is an element $x \in (J : I) \cap K^\times$ such that $\mathscr{F}(\varphi) = x$.

From now on, we simply write $\varphi\colon A \to B \in \mathscr{I}_h \overset{\mathscr{F}}{\rightsquigarrow} x \cdot I \subseteq J$.

Proposition

1. $\deg(\varphi) = [J : xI]$. *since ordinary: no problem at p.*
2. *The isogeny φ is minimal if and only if the inclusion $xI \subsetneq J$ is maximal, that is, the quotient J/xI is a simple R-module.*
3. *The length of the isogeny φ equals the length of J/xI as an R-module.*

Example : minimal isogenies can make End's jump.

Let $h(X) = X^4 + 6X^2 + 25 = (X^2 - 2X + 5)(X^2 + 2X + 5)$, giving the isogeny class $\mathscr{I}_h$ with LMFDB label 2.5.a_g.

Let $h(X) = X^4 + 6X^2 + 25 = (X^2 - 2X + 5)(X^2 + 2X + 5)$, giving the isogeny class $\mathscr{I}_h$ with LMFDB label 2.5.a_g.

The lattice of inclusions – all of index 2 – of the End's in $\mathscr{I}_h$ is:

$$\begin{tikzcd}
 & & & & \mathcal{O}_K & & & & \\
 & \bullet \arrow[urrr] & & & \bullet \arrow[u] & & & \bullet \arrow[ulll] & \\
\bullet \arrow[ur] & & \bullet \arrow[ul] \arrow[urr] & & & & \bullet \arrow[ulllll] \arrow[ur] & & \bullet \arrow[ullll] \arrow[ul] \\
 & & & & S \arrow[ullll] \arrow[ull] \arrow[urr] \arrow[urrrr] & & & & \\
 & \bullet \arrow[urrr] & & & \bullet \arrow[u] & & & \bullet \arrow[ulll] & \\
 & & & & \bullet \arrow[ulll] \arrow[u] \arrow[urrr] & & & & \\
 & & & & R = \mathbb{Z}\left[\pi, \frac{5}{\pi}\right] \arrow[u] & & & &
\end{tikzcd}$$

Example : minimal isogenies can make End's jump.

Let $h(X) = X^4 + 6X^2 + 25 = (X^2 - 2X + 5)(X^2 + 2X + 5)$, giving the isogeny class $\mathscr{I}_h$ with LMFDB label 2.5.a_g.
The lattice of inclusions – all of index 2 – of the End's in $\mathscr{I}_h$ is:

$$\begin{tikzcd}
 & & & \mathscr{O}_K & & & \\
 & \bullet \arrow[urr] & & \bullet \arrow[u] & & \bullet \arrow[ull] & \\
\bullet \arrow[ur] & & \bullet \arrow[ul] \arrow[ur] & & \bullet \arrow[ulll] \arrow[ur] & & \bullet \arrow[ulll] \arrow[ul] \\
 & & & S \arrow[ulll] \arrow[ul] \arrow[ur] \arrow[urrr] & & & \\
 & \bullet \arrow[urr] & & \bullet \arrow[u] & & \bullet \arrow[ull] & \\
 & & & \bullet \arrow[ull] \arrow[u] \arrow[urr] & & & \\
 & & & R = \mathbb{Z}\left[\pi, \frac{5}{\pi}\right] \arrow[u] & & &
\end{tikzcd}$$

- R has a unique singular maximal ideal $\mathfrak{m}$ with $R/\mathfrak{m} = \mathbb{F}_2$.

Example : minimal isogenies can make End's jump.

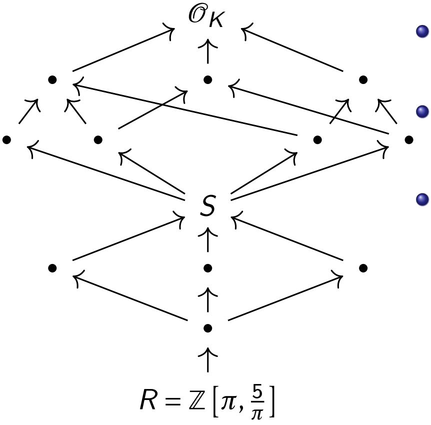
Let $h(X) = X^4 + 6X^2 + 25 = (X^2 - 2X + 5)(X^2 + 2X + 5)$, giving the isogeny class $\mathscr{I}_h$ with LMFDB label 2.5.a_g.
The lattice of inclusions – all of index 2 – of the End's in $\mathscr{I}_h$ is:

$$
\begin{tikzcd}
 & & & \mathscr{O}_K & & & \\
 & \bullet \arrow[urr] & & \bullet \arrow[u] & & \bullet \arrow[ull] & \\
\bullet \arrow[ur] & & \bullet \arrow[ul] \arrow[ur] & & \bullet \arrow[ulll] \arrow[ur] & & \bullet \arrow[ulll] \arrow[ul] \\
 & & & S \arrow[ulll] \arrow[ul] \arrow[ur] \arrow[urrr] & & & \\
 & \bullet \arrow[urr] & & \bullet \arrow[u] & & \bullet \arrow[ull] & \\
 & & & \bullet \arrow[ull] \arrow[u] \arrow[urr] & & & \\
 & & & R = \mathbb{Z}\left[\pi, \frac{5}{\pi}\right] \arrow[u] & & &
\end{tikzcd}
$$

- R has a unique singular maximal ideal $\mathfrak{m}$ with $R/\mathfrak{m} = \mathbb{F}_2$.
- The conductor $\mathfrak{f}_S = (S : \mathscr{O}_K)$ satisfies $S/\mathfrak{f}_S \simeq R/\mathfrak{m}$, and $(\mathfrak{f}_S : \mathfrak{f}_S) = \mathscr{O}_K$.

Example : minimal isogenies can make End's jump.

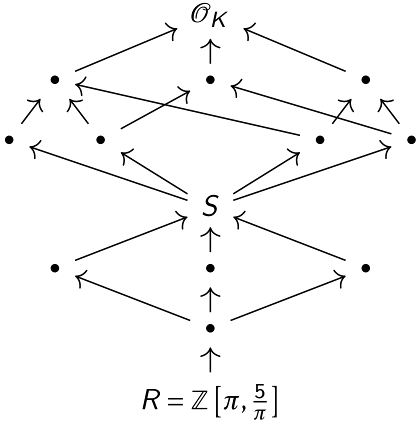
Let $h(X) = X^4 + 6X^2 + 25 = (X^2 - 2X + 5)(X^2 + 2X + 5)$, giving the isogeny class $\mathscr{I}_h$ with LMFDB label 2.5.a_g.
The lattice of inclusions – all of index 2 – of the End's in $\mathscr{I}_h$ is:



- R has a unique singular maximal ideal $\mathfrak{m}$ with $R/\mathfrak{m} = \mathbb{F}_2$.
- The conductor $\mathfrak{f}_S = (S : \mathscr{O}_K)$ satisfies $S/\mathfrak{f}_S \simeq R/\mathfrak{m}$, and $(\mathfrak{f}_S : \mathfrak{f}_S) = \mathscr{O}_K$.
- The isogeny $A \xrightarrow{\varphi} B \overset{\mathscr{F}}{\rightsquigarrow} 1 \cdot \mathfrak{f}_S \subset S$ is minimal, has $\deg \varphi = 2$, is descending
  $\mathrm{End}(A) = \mathscr{O}_K \supsetneq \mathrm{End}(B) = S$ ...

Example : minimal isogenies can make End's jump.

Let $h(X) = X^4 + 6X^2 + 25 = (X^2 - 2X + 5)(X^2 + 2X + 5)$, giving the isogeny class $\mathscr{I}_h$ with LMFDB label 2.5.a_g.
The lattice of inclusions – all of index 2 – of the End's in $\mathscr{I}_h$ is:



- R has a unique singular maximal ideal $\mathfrak{m}$ with $R/\mathfrak{m} = \mathbb{F}_2$.
- The conductor $\mathfrak{f}_S = (S : \mathscr{O}_K)$ satisfies $S/\mathfrak{f}_S \simeq R/\mathfrak{m}$, and $(\mathfrak{f}_S : \mathfrak{f}_S) = \mathscr{O}_K$.
- The isogeny $A \xrightarrow{\varphi} B \overset{\mathscr{F}}{\rightsquigarrow} 1 \cdot \mathfrak{f}_S \subset S$ is minimal, has $\deg \varphi = 2$, is descending $\mathrm{End}(A) = \mathscr{O}_K \supsetneq \mathrm{End}(B) = S$ ...
- ... but the inclusion $S \subsetneq \mathscr{O}_K$ is not minimal!

Endomorphism rings

Theorem

Let $\varphi\colon A \to B \in \mathscr{I}_h \overset{\mathscr{F}}{\rightsquigarrow} x \cdot I \subseteq J$.

Endomorphism rings

Theorem

Let $\varphi\colon A \to B \in \mathscr{I}_h \overset{\mathscr{F}}{\rightsquigarrow} x \cdot I \subseteq J$. Assume φ is minimal and let $\mathfrak{m}$ be the maximal ideal of R such that $J/xI \simeq R/\mathfrak{m}$.

Endomorphism rings

Theorem

Let $\varphi\colon A \to B \in \mathscr{I}_h \overset{\mathscr{F}}{\rightsquigarrow} x \cdot I \subseteq J$. *Assume* φ *is minimal and let* $\mathfrak{m}$ *be the maximal ideal of* R *such that* $J/xI \simeq R/\mathfrak{m}$. *Then:*

1. φ *is horizontal or vertical:* $\mathrm{End}(A) \subseteq \mathrm{End}(B)$ *or* $\mathrm{End}(B) \subseteq \mathrm{End}(A)$.

Endomorphism rings

Theorem

Let $\varphi\colon A \to B \in \mathscr{I}_h \overset{\mathscr{F}}{\rightsquigarrow} x \cdot I \subseteq J$. *Assume* φ *is minimal and let* $\mathfrak{m}$ *be the maximal ideal of* R *such that* $J/xI \simeq R/\mathfrak{m}$. *Then:*

1. φ *is horizontal or vertical:* $\mathrm{End}(A) \subseteq \mathrm{End}(B)$ *or* $\mathrm{End}(B) \subseteq \mathrm{End}(A)$.
2. *If* $\mathfrak{m}$ *is regular then* φ *is horizontal.*

Endomorphism rings

Theorem

Let $\varphi\colon A \to B \in \mathscr{I}_h \overset{\mathscr{F}}{\rightsquigarrow} x \cdot I \subseteq J$*. Assume* φ *is minimal and let* $\mathfrak{m}$ *be the maximal ideal of* R *such that* $J/xI \simeq R/\mathfrak{m}$*. Then:*

1. φ *is horizontal or vertical:* $\mathrm{End}(A) \subseteq \mathrm{End}(B)$ *or* $\mathrm{End}(B) \subseteq \mathrm{End}(A)$.
2. *If* $\mathfrak{m}$ *is regular then* φ *is horizontal.*
3. *If* φ *is vertical then* $\mathfrak{m}$ *is singular.*

Endomorphism rings

Theorem

Let $\varphi : A \to B \in \mathscr{I}_h \overset{\mathscr{F}}{\rightsquigarrow} x \cdot I \subseteq J$. Assume φ is minimal and let $\mathfrak{m}$ be the maximal ideal of R such that $J/xI \simeq R/\mathfrak{m}$. Then:

1. *φ is horizontal or vertical: $\mathrm{End}(A) \subseteq \mathrm{End}(B)$ or $\mathrm{End}(B) \subseteq \mathrm{End}(A)$.*
2. *If $\mathfrak{m}$ is regular then φ is horizontal.*
3. *If φ is vertical then $\mathfrak{m}$ is singular.*
4. *Let $T = \mathrm{End}(A) \cup \mathrm{End}(B)$ and $S = \mathrm{End}(A) \cap \mathrm{End}(B)$. Then $|T/S| = |R/\mathfrak{m}|^{\mathrm{length}_R(T/S)}$. In particular, φ is vertical if and only if $[R : \mathfrak{m}]$ divides the index $[T : S]$.*

Isogeny Graphs

Definition

1. Two isogenies $\varphi_1 \colon A_1 \to B_1$ and $\varphi_2 \colon A_2 \to B_2$ are said to be equivalent, denoted $\varphi_1 \approx \varphi_2$, if and only if there exist isomorphisms $i_1 \colon A_1 \to A_2$ and $i_2 \colon B_1 \to B_2$ such that $i_2 \circ \varphi_1 = \varphi_2 \circ i_1$.

Isogeny Graphs

Definition

1. Two isogenies $\varphi_1 \colon A_1 \to B_1$ and $\varphi_2 \colon A_2 \to B_2$ are said to be equivalent, denoted $\varphi_1 \approx \varphi_2$, if and only if there exist isomorphisms $i_1 \colon A_1 \to A_2$ and $i_2 \colon B_1 \to B_2$ such that $i_2 \circ \varphi_1 = \varphi_2 \circ i_1$.
2. The full isogeny graph $\mathscr{G}$ of an isogeny class $\mathscr{I}_h$ is the directed multigraph whose vertices are isomorphism classes of abelian varieties in $\mathscr{I}_h$ and whose edges are equivalence classes of isogenies of deg. > 1.

Isogeny Graphs

Definition

1. Two isogenies $\varphi_1 \colon A_1 \to B_1$ and $\varphi_2 \colon A_2 \to B_2$ are said to be equivalent, denoted $\varphi_1 \approx \varphi_2$, if and only if there exist isomorphisms $i_1 \colon A_1 \to A_2$ and $i_2 \colon B_1 \to B_2$ such that $i_2 \circ \varphi_1 = \varphi_2 \circ i_1$.
2. The full isogeny graph $\mathscr{G}$ of an isogeny class $\mathscr{I}_h$ is the directed multigraph whose vertices are isomorphism classes of abelian varieties in $\mathscr{I}_h$ and whose edges are equivalence classes of isogenies of deg. > 1.
3. Let D be a positive integer. The D-isogeny graph $\mathscr{G}^D$ is the subgraph of $\mathscr{G}$ with edges $\mathscr{E}^D$ of degree dividing D.

Isogeny Graphs

Definition

1. Two isogenies $\varphi_1 \colon A_1 \to B_1$ and $\varphi_2 \colon A_2 \to B_2$ are said to be equivalent, denoted $\varphi_1 \approx \varphi_2$, if and only if there exist isomorphisms $i_1 \colon A_1 \to A_2$ and $i_2 \colon B_1 \to B_2$ such that $i_2 \circ \varphi_1 = \varphi_2 \circ i_1$.
2. The full isogeny graph $\mathscr{G}$ of an isogeny class $\mathscr{I}_h$ is the directed multigraph whose vertices are isomorphism classes of abelian varieties in $\mathscr{I}_h$ and whose edges are equivalence classes of isogenies of deg. > 1.
3. Let D be a positive integer. The D-isogeny graph $\mathscr{G}^D$ is the subgraph of $\mathscr{G}$ with edges $\mathscr{E}^D$ of degree dividing D.
4. Let D and r be positive integers. The graph $\mathscr{G}^{D,r}$ is the subgraph of $\mathscr{G}$ with edges $\mathscr{E}^{D,r}$ of degree dividing D and length at most r.

Proposition

Given $\varphi_1 : A_1 \to B_1, \varphi_2 : A_2 \to B_2 \in \mathscr{I}_h$

Proposition

Given $\varphi_1 : A_1 \to B_1, \varphi_2 : A_2 \to B_2 \in \mathscr{I}_h \overset{\mathscr{F}}{\rightsquigarrow} x_1 \cdot I_1 \subseteq J_1,\ x_2 \cdot I_2 \subseteq J_2,$ *respectively, then*

$$\varphi_1 \approx \varphi_2 \iff \begin{array}{c} \exists k_A, k_B \in K^\times \text{ such that} \\ k_A I_1 = I_2,\ k_B J_1 = J_2 \text{ and} \\ x_2 k_A = k_B x_1 \end{array}$$

Proposition

Given $\varphi_1 : A_1 \to B_1, \varphi_2 : A_2 \to B_2 \in \mathscr{I}_h \overset{\mathscr{F}}{\rightsquigarrow} x_1 \cdot I_1 \subseteq J_1,\ x_2 \cdot I_2 \subseteq J_2,$ *respectively, then*

$$\varphi_1 \approx \varphi_2 \iff \begin{array}{c} \exists k_A, k_B \in K^\times \text{ such that} \\ k_A I_1 = I_2,\ k_B J_1 = J_2 \text{ and} \\ x_2 k_A = k_B x_1 \end{array}$$

Caution! Composition is not well defined on equivalence classes. Need to take into account automorphisms:

Proposition

Given $\varphi_1 : A_1 \to B_1, \varphi_2 : A_2 \to B_2 \in \mathscr{I}_h \overset{\mathscr{F}}{\rightsquigarrow} x_1 \cdot I_1 \subseteq J_1,\ x_2 \cdot I_2 \subseteq J_2$, *respectively, then*

$$\varphi_1 \approx \varphi_2 \iff \begin{array}{c} \exists k_A, k_B \in K^\times \text{ such that} \\ k_A I_1 = I_2,\ k_B J_1 = J_2 \text{ and} \\ x_2 k_A = k_B x_1 \end{array}$$

Caution! Composition is not well defined on equivalence classes. Need to take into account automorphisms:

Proposition

Given, in $\mathscr{I}_h$

- $\varphi : A \to B \overset{\mathscr{F}}{\rightsquigarrow} x \cdot H \subseteq I$,
- $\psi : B \to C \overset{\mathscr{F}}{\rightsquigarrow} y \cdot I \subseteq J$,
- ρ *an automorphism of* $B \overset{\mathscr{F}}{\rightsquigarrow} z \in (I : I)^\times$,

then

$$\psi \circ \varphi \approx \psi \circ \rho \circ \varphi \iff z \in (H : H)^\times (J : J)^\times .$$

Computing $\mathscr{G}^D$: strategy

Computing $\mathscr{G}^D$: strategy

- Vertices are in bijection with the ideal class monoid $\mathrm{ICM}(R)$ of R.

Computing $\mathscr{G}^D$: strategy

- Vertices are in bijection with the ideal class monoid $\mathrm{ICM}(R)$ of R.
- $\mathrm{Pic}(R)$ acts on the vertices by ideal multiplication: the orbits are called weak equivalence classes.

Computing $\mathscr{G}^D$: strategy

- Vertices are in bijection with the ideal class monoid $\mathrm{ICM}(R)$ of R.
- $\mathrm{Pic}(R)$ acts on the vertices by ideal multiplication: the orbits are called weak equivalence classes.
- Side note: $I = LJ$ for some invertible $L \iff I_{\mathfrak{m}} \simeq J_{\mathfrak{m}}$ as $R_{\mathfrak{m}}$-modules, for every maximal R-ideal $\mathfrak{m}$.

Computing $\mathscr{G}^D$: strategy

- Vertices are in bijection with the ideal class monoid $\mathrm{ICM}(R)$ of R.
- $\mathrm{Pic}(R)$ acts on the vertices by ideal multiplication: the orbits are called weak equivalence classes.
- Side note: $I = LJ$ for some invertible $L \iff I_\mathfrak{m} \simeq J_\mathfrak{m}$ as $R_\mathfrak{m}$-modules, for every maximal R-ideal $\mathfrak{m}$.
- Edges: Compute first minimal edges, i.e. $\mathscr{G}^{D,1}$, then compose.

Computing $\mathscr{G}^D$: strategy

- Vertices are in bijection with the ideal class monoid $\mathrm{ICM}(R)$ of R.
- $\mathrm{Pic}(R)$ acts on the vertices by ideal multiplication: the orbits are called weak equivalence classes.
- Side note: $I = LJ$ for some invertible $L \iff I_{\mathfrak{m}} \simeq J_{\mathfrak{m}}$ as $R_{\mathfrak{m}}$-modules, for every maximal R-ideal $\mathfrak{m}$.
- Edges: Compute first minimal edges, i.e. $\mathscr{G}^{D,1}$, then compose.
- For each target J, need to compute minimal edges to J.

Computing $\mathscr{G}^D$: strategy

- Vertices are in bijection with the ideal class monoid $\mathrm{ICM}(R)$ of R.
- $\mathrm{Pic}(R)$ acts on the vertices by ideal multiplication: the orbits are called weak equivalence classes.
- Side note: $I = LJ$ for some invertible $L \iff I_\mathfrak{m} \simeq J_\mathfrak{m}$ as $R_\mathfrak{m}$-modules, for every maximal R-ideal $\mathfrak{m}$.
- Edges: Compute first minimal edges, i.e. $\mathscr{G}^{D,1}$, then compose.
- For each target J, need to compute minimal edges to J.
- Done by computing maximal $M \subset J$ such that $[J : M]$ divides D.

Computing $\mathscr{G}^D$: strategy

- Vertices are in bijection with the ideal class monoid $\mathrm{ICM}(R)$ of R.
- $\mathrm{Pic}(R)$ acts on the vertices by ideal multiplication: the orbits are called weak equivalence classes.
- Side note: $I = LJ$ for some invertible $L \iff I_{\mathfrak{m}} \simeq J_{\mathfrak{m}}$ as $R_{\mathfrak{m}}$-modules, for every maximal R-ideal $\mathfrak{m}$.
- Edges: Compute first minimal edges, i.e. $\mathscr{G}^{D,1}$, then compose.
- For each target J, need to compute minimal edges to J.
- Done by computing maximal $M \subset J$ such that $[J : M]$ divides D.
- For each M find the source vertex, i.e. I, x such that $x \cdot I = M$.

Computing $\mathscr{G}^D$: strategy

- Vertices are in bijection with the ideal class monoid $\mathrm{ICM}(R)$ of R.
- $\mathrm{Pic}(R)$ acts on the vertices by ideal multiplication: the orbits are called weak equivalence classes.
- Side note: $I = LJ$ for some invertible $L \iff I_\mathfrak{m} \simeq J_\mathfrak{m}$ as $R_\mathfrak{m}$-modules, for every maximal R-ideal $\mathfrak{m}$.
- Edges: Compute first minimal edges, i.e. $\mathscr{G}^{D,1}$, then compose.
- For each target J, need to compute minimal edges to J.
- Done by computing maximal $M \subset J$ such that $[J : M]$ divides D.
- For each M find the source vertex, i.e. I,x such that $x \cdot I = M$. This is annoying! But ...

Computing $\mathscr{G}^D$: strategy

- Vertices are in bijection with the ideal class monoid $\mathrm{ICM}(R)$ of R.
- $\mathrm{Pic}(R)$ acts on the vertices by ideal multiplication: the orbits are called weak equivalence classes.
- Side note: $I = LJ$ for some invertible $L \iff I_\mathfrak{m} \simeq J_\mathfrak{m}$ as $R_\mathfrak{m}$-modules, for every maximal R-ideal $\mathfrak{m}$.
- Edges: Compute first minimal edges, i.e. $\mathscr{G}^{D,1}$, then compose.
- For each target J, need to compute minimal edges to J.
- Done by computing maximal $M \subset J$ such that $[J : M]$ divides D.
- For each M find the source vertex, i.e. I,x such that $x \cdot I = M$. This is annoying! But ...
- ... $\mathrm{Pic}(R)$ acts on edges too:

Computing $\mathscr{G}^D$: strategy

- Vertices are in bijection with the ideal class monoid $\mathrm{ICM}(R)$ of R.
- $\mathrm{Pic}(R)$ acts on the vertices by ideal multiplication: the orbits are called weak equivalence classes.
- Side note: $I = LJ$ for some invertible $L \iff I_{\mathfrak{m}} \simeq J_{\mathfrak{m}}$ as $R_{\mathfrak{m}}$-modules, for every maximal R-ideal $\mathfrak{m}$.
- Edges: Compute first minimal edges, i.e. $\mathscr{G}^{D,1}$, then compose.
- For each target J, need to compute minimal edges to J.
- Done by computing maximal $M \subset J$ such that $[J : M]$ divides D.
- For each M find the source vertex, i.e. I,x such that $x \cdot I = M$. This is annoying! But ...
- ... $\mathrm{Pic}(R)$ acts on edges too: if L is an invertible R-ideal and $x \cdot I \subseteq J$ is a (minimal) isogeny, then $x \cdot IL \subseteq JL$ is a (minimal) isogeny.

Computing $\mathscr{G}^D$: strategy

- Vertices are in bijection with the ideal class monoid $\mathrm{ICM}(R)$ of R.
- $\mathrm{Pic}(R)$ acts on the vertices by ideal multiplication: the orbits are called weak equivalence classes.
- Side note: $I = LJ$ for some invertible $L \iff I_{\mathfrak{m}} \simeq J_{\mathfrak{m}}$ as $R_{\mathfrak{m}}$-modules, for every maximal R-ideal $\mathfrak{m}$.
- Edges: Compute first minimal edges, i.e. $\mathscr{G}^{D,1}$, then compose.
- For each target J, need to compute minimal edges to J.
- Done by computing maximal $M \subset J$ such that $[J : M]$ divides D.
- For each M find the source vertex, i.e. I,x such that $x \cdot I = M$. This is annoying! But ...
- ... $\mathrm{Pic}(R)$ acts on edges too: if L is an invertible R-ideal and $x \cdot I \subseteq J$ is a (minimal) isogeny, then $x \cdot IL \subseteq JL$ is a (minimal) isogeny.
- So: need to enumerate min. isogenies only once per weak eq. class.

Computing $\mathscr{G}^D$: strategy

- We implemented this in the Magma intrinsics `MinimalIsogenyGraphBuilder` and `IsogenyGraphBuilder`.

Computing $\mathscr{G}^D$: strategy

- We implemented this in the Magma intrinsics `MinimalIsogenyGraphBuilder` and `IsogenyGraphBuilder`.
- We included SageMath code to plot the graphs.

Computing $\mathscr{G}^D$: strategy

- We implemented this in the Magma intrinsics `MinimalIsogenyGraphBuilder` and `IsogenyGraphBuilder`.
- We included SageMath code to plot the graphs.
- We have also the Magma intrinsics `IsogenyOrbitBuilder` in which the output is modulo the action of Pic on both source and target (independently). Useful for storing!

Connectedness and diameter

Theorem

Let $D > 1$ and $\mathscr{S}^{\mathrm{sing}}$ be the set of maximal R-ideals above $\mathfrak{f}_R = (R : \mathscr{O}_K)$.

Connectedness and diameter

Theorem

Let $D > 1$ and $\mathscr{S}^{\text{sing}}$ be the set of maximal R-ideals above $\mathfrak{f}_R = (R : \mathscr{O}_K)$.

1. *Suppose that there exists a set $\mathscr{S}$ of (non-necessarily invertible) maximal ideals $\mathfrak{l}$ of R such that $\mathrm{Pic}(\mathscr{O}_K) = \langle \mathfrak{l}\mathscr{O}_K | \mathfrak{l} \in \mathscr{S} \rangle$, and that*

Connectedness and diameter

Theorem

Let $D > 1$ and $\mathscr{S}^{\text{sing}}$ be the set of maximal R-ideals above $\mathfrak{f}_R = (R : \mathcal{O}_K)$.

1. *Suppose that there exists a set $\mathscr{S}$ of (non-necessarily invertible) maximal ideals $\mathfrak{l}$ of R such that $\mathrm{Pic}(\mathcal{O}_K) = \langle \mathfrak{l}\mathcal{O}_K | \mathfrak{l} \in \mathscr{S} \rangle$, and that $N_{\mathscr{S}} = \mathrm{lcm}\left(\{|R/\mathfrak{l}| : \mathfrak{l} \in \mathscr{S}^{\text{sing}} \cup \mathscr{S}\}\right)$ divides D.*

Connectedness and diameter

Theorem

Let $D > 1$ and $\mathscr{S}^{\mathrm{sing}}$ be the set of maximal R-ideals above $\mathfrak{f}_R = (R : \mathcal{O}_K)$.

1. *Suppose that there exists a set $\mathscr{S}$ of (non-necessarily invertible) maximal ideals $\mathfrak{l}$ of R such that $\mathrm{Pic}(\mathcal{O}_K) = \langle \mathfrak{l}\mathcal{O}_K \mid \mathfrak{l} \in \mathscr{S} \rangle$, and that $N_{\mathscr{S}} = \mathrm{lcm}\left(\{|R/\mathfrak{l}| : \mathfrak{l} \in \mathscr{S}^{\mathrm{sing}} \cup \mathscr{S}\}\right)$ divides D.*
   Then the isogeny graph $\mathscr{G}^D$ is connected (as a directed graph).

Connectedness and diameter

Theorem

Let $D > 1$ *and* $\mathscr{S}^{\text{sing}}$ *be the set of maximal* R*-ideals above* $\mathfrak{f}_R = (R : \mathcal{O}_K)$*.*

1. *Suppose that there exists a set* $\mathscr{S}$ *of (non-necessarily invertible) maximal ideals* $\mathfrak{l}$ *of* R *such that* $\mathrm{Pic}(\mathcal{O}_K) = \langle \mathfrak{l}\mathcal{O}_K \mid \mathfrak{l} \in \mathscr{S} \rangle$*, and that* $N_{\mathscr{S}} = \mathrm{lcm}\left(\{|R/\mathfrak{l}| : \mathfrak{l} \in \mathscr{S}^{\text{sing}} \cup \mathscr{S}\}\right)$ *divides* D*.*
   Then the isogeny graph $\mathscr{G}^D$ *is connected (as a directed graph).*
2. *Let* $\mathscr{S}$ *be as in (1) above and set* $S_{\mathscr{S}} = \sum_{\mathfrak{l} \in \mathscr{S}} \left(\mathrm{ord}_{\mathrm{Pic}(\mathcal{O}_K)}([\mathfrak{l}\mathcal{O}_K]) - 1\right)$*.*
   Then the diameter of $\mathscr{G}^{D,1}$ *satisfies:*

$$\mathrm{diam}(\mathscr{G}^{D,1}) \leq \begin{cases} 2\,\mathrm{length}_R(\mathcal{O}_K/R) + S_{\mathscr{S}} & \textit{if } R \textit{ is Bass,} \\ 2\left(\mathrm{length}_R(\mathcal{O}_K/\mathfrak{f}_R) - 1\right) + S_{\mathscr{S}} & \textit{otherwise.} \end{cases}$$

Connectedness and diameter

Theorem

Let $D > 1$ and $\mathscr{S}^{\mathrm{sing}}$ be the set of maximal R-ideals above $\mathfrak{f}_R = (R : \mathcal{O}_K)$.

Connectedness and diameter

Theorem

Let $D > 1$ and $\mathscr{S}^{\mathrm{sing}}$ be the set of maximal R-ideals above $\mathfrak{f}_R = (R : \mathscr{O}_K)$.

3. *If the isogeny graph $\mathscr{G}^D$ is connected (as a directed graph) then D is divisible by the integer*

$$N_{\mathscr{S}^{\mathrm{sing}}} = \mathrm{lcm}\left(\{|R/\mathfrak{l}| : \mathfrak{l} \in \mathscr{S}^{\mathrm{sing}}\}\right).$$

Connectedness and diameter

Theorem

Let $D > 1$ and $\mathscr{S}^{\mathrm{sing}}$ be the set of maximal R-ideals above $\mathfrak{f}_R = (R : \mathcal{O}_K)$.

3. *If the isogeny graph $\mathscr{G}^D$ is connected (as a directed graph) then D is divisible by the integer*

$$N_{\mathscr{S}^{\mathrm{sing}}} = \mathrm{lcm}\left(\left\{|R/\mathfrak{l}| : \mathfrak{l} \in \mathscr{S}^{\mathrm{sing}}\right\}\right).$$

4. *Assume that $\mathscr{G}^D$ is connected. Then*

$$\mathrm{length}_R(R/\mathfrak{f}_R) \leq \mathrm{diam}(\mathscr{G}^{D,1}).$$

Thank you for your attention!