ORDINARY ABELIAN VARIETIES: ISOGENY GRAPHS AND POLARIZATIONS

EDGAR COSTA, TAYLOR DUPUY, STEFANO MARSEGLIA, DAVID ROE, AND CHRISTELLE VINCENT

Abstract. Given an integer D and an ordinary isogeny class of abelian varieties defined over a finite field $\mathbb{F}_q$ with commutative $\mathbb{F}_q$-endomorphism algebra, we provide algorithms for computing all isogenies of degree dividing D and polarizations of degree dividing D. We discuss phenomena that arise for higher dimension abelian varieties but not elliptic curves, bounds on the diameter of the graph of minimal isogenies, and decompositions of isogeny graphs into orbits for the Picard group of the Frobenius order.

1. Introduction

In his PhD thesis, Kohel [Koh96] pioneered the study of the structure of isogeny graphs of elliptic curves defined over finite fields $\mathbb{F}_q$ of characteristic p. For ordinary elliptic curves, these graphs have a striking form, called "isogeny volcanoes" [FM02]. We refer the interested reader to [Sut13] for details and a more complete history. A natural generalization is to consider the case of higher-dimensional abelian varieties, and the first results in this direction were obtained for the case of absolutely simple ordinary abelian varieties in [BJW17; Mar18; IT20]. More recently, [AMS25] obtain results for unpolarized abelian varieties with commutative $\mathbb{F}_q$-endomorphism ring all containing a fixed order R. The authors define $\mathfrak{l}$-isogenies — special kinds of isogenies of degree coprime with q defined using maximal ideals $\mathfrak{l}$ of R — and provide a structure theorem for the corresponding isogeny graph when the order R is Bass at $\mathfrak{l}$. In this paper, we continue studying the isogeny graphs of abelian varieties with commutative $\mathbb{F}_q$-endomorphism algebra. A goal of this work, along with [CDMRV25], is to add additional information to the L-functions and modular forms database [LMFDB]: isomorphism classes of abelian varieties defined over finite fields together with their isogeny graphs, which we use to efficiently compute non-principal polarizations. In contrast with [AMS25], we assume that the isogeny class is ordinary. This assumption allows us to build upon the algorithm developed in [Mar21] to compute isomorphism classes and polarizations. Also, it allows us to consider isogenies with degree divisible by p and we can avoid further assumptions on the endomorphism rings other than being commutative. One could try to generalize the results contained in this paper to the non-ordinary case by following [BKM23] and [BKM24], where the authors developed algorithms to compute principal polarizations and isomorphism classes (respectively), but that work is not within the scope of the current paper.

From now on, let q be a power of a prime and $h(x)$ be a q-Weil polynomial of degree $2g$. We will always assume that $h(x)$ has no repeated complex roots and its x^g

Date: June 4, 2026.

coefficient is not divisible by p. With these assumptions, Honda-Tate theory [Tat66; Hon68] implies that $h(x)$ determines an $\mathbb{F}_q$-isogeny class $\mathcal{I}_h$ of ordinary, dimension g abelian varieties defined over $\mathbb{F}_q$, each with commutative $\mathbb{F}_q$-endomorphism algebra. In this setting, we study the *D-isogeny graph* of $\mathcal{I}_h$ for $D > 1$, whose vertices are the $\mathbb{F}_q$-isomorphism classes of abelian varieties in $\mathcal{I}_h$ and whose edges are *equivalence classes* of $\mathbb{F}_q$-isogenies of degree dividing D; see Definitions 3.1 and 4.1 for more details. Throughout, all morphisms, isomorphism classes, and isogenies are defined over $\mathbb{F}_q$.

In Section 2, we use Deligne's functor to connect abelian varieties with ideals in the étale algebra $K = \mathbb{Q}[x]/(h(x))$. Denoting by π the class of x in K and by $\overline{\pi}$ its complex conjugate, the order $\mathbb{Z}[\pi, \overline{\pi}] \subset K$ is the *Frobenius order* of the isogeny class $\mathcal{I}_h$. Its set of fractional ideals is a commutative monoid under ideal multiplication, and isomorphism classes of fractional $\mathbb{Z}[\pi, \overline{\pi}]$-ideals form the *ideal class monoid* $\mathrm{ICM}(\mathbb{Z}[\pi, \overline{\pi}])$ [Mar20, Corollary 3.4]. The orbits of the action of $\mathrm{Pic}(\mathbb{Z}[\pi, \overline{\pi}])$ on $\mathrm{ICM}(\mathbb{Z}[\pi, \overline{\pi}])$ by ideal multiplication are called *weak equivalence classes*.

In Section 3 we start studying isogenies in $\mathcal{I}_h$. The main results of this section show that minimal isogenies necessarily have prime-power degree (Proposition 3.4) and that one of the endomorphism ring of the domain or codomain is contained in the endomorphism ring of the other (Theorem 3.6), but there are examples where this inclusion is not maximal (Example 3.7). This contrasts with the case of ℓ-isogenies of elliptic curves for ℓ prime, where the inclusion is always maximal.

We continue in Section 4 by formally defining the D-isogeny graphs $\mathcal{G}^D$. Proposition 4.2 gives a necessary condition for the existence of minimal isogenies of given prime-power degree; Theorem 4.6 provides conditions on D for $\mathcal{G}^D$ to be connected (one sufficient and one necessary) as well as diameter bounds. We then give in Section 5 an algorithm to compute $\mathcal{G}^D$ by leveraging the action of $\mathrm{Pic}(\mathbb{Z}[\pi, \overline{\pi}])$ to compute minimal edges for each equivalence class. Composing these minimal isogenies then yields $\mathcal{G}^D$; see Algorithm 5.2.

In Section 6, we give an algorithm to efficiently store $\mathcal{G}^D$. Lemma 6.3 shows that a quotient of $\mathrm{Pic}(\mathbb{Z}[\pi, \overline{\pi}])$ acts freely on edges between weak equivalence classes; Algorithm 6.7 computes orbit representatives. These results allow storage of only one edge from each orbit, which can both compactify outputs and speed up computations. Finally, in Section 7, we show how to compute polarizations of degree dividing D in $\mathcal{I}_h$ using $\mathcal{G}^D$ as input; see Algorithm 7.5.

All of the code accompanying this paper is available at `https://github.com/stmar89/AbVarFqIsogenies` [CDMRV26], and requires [Magma] to compute and [SageMath] to graphically represent the graphs. For each algorithm in this paper, we provide the name of corresponding intrinsic in our Magma implementation. We conclude with an example produced by Algorithm 5.2.

Example 1.1. Let $D = 2$ and consider the ordinary isogeny class of abelian 4-folds over $\mathbb{F}_3$ with LMFDB label 4.3.c_ab_af_ai and Weil polynomial $h(x) = x^8 + 2x^7 - x^6 - 5x^5 - 8x^4 - 15x^3 - 9x^2 + 54x + 81$. This isogeny class has 14 isomorphism classes; hence its 2-isogeny graph (Figure 1) has 14 vertices, which are here colored by endomorphism ring (darker colors indicating a larger ring). The colors in the figures below are in bijection with the endomorphism ring, consistently across components.

The base change of this isogeny class to $\mathbb{F}_9$ has Weil polynomial

$$h_2(x) = x^8 - 6x^7 + 5x^6 + 33x^5 - 122x^4 + 297x^3 + 405x^2 - 4374x + 6561,$$

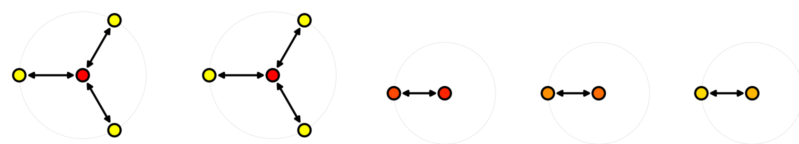

FIGURE 1. The 2-isogeny graph for 4.3.c_ab_af_ai.

which is not in the LMFDB but can be computed as in [DKRV21, §3.4]. This isogeny class has 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.

Interestingly, in both cases all components of the same size are isomorphic as directed graphs, but the vertices need not have identical coloring. This is illustrated by one of the component with 2 vertices in Figure 1, and occurs again over $\mathbb{F}_9$: two examples of components with 17 vertices but different colorings are shown in Figure 2.

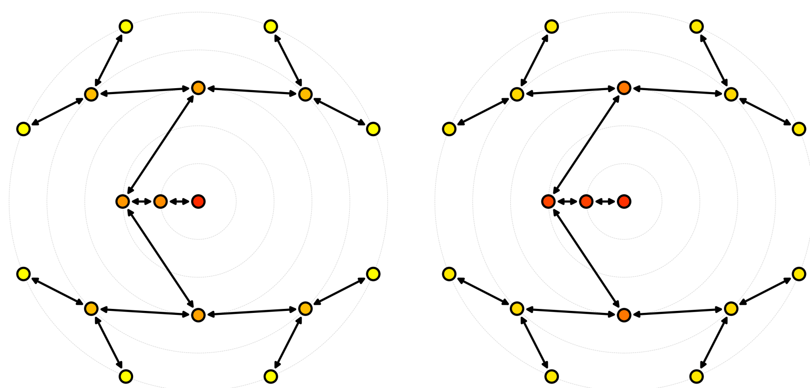

FIGURE 2. Two components of the 2-isogeny graph of the base change of 4.3.c_ab_af_ai to $\mathbb{F}_9$, each with 17 vertices and isomorphic as directed graphs, but whose underlying vertices have different endomorphism rings.

Lest the reader be left with the impression that these isogeny graphs are classical isogeny volcanoes, we show a component with 94 vertices in Figure 3. The vertices of this graph have six different endomorphism rings, which in this case correspond to different levels in the graph. The yellow vertices are abelian varieties whose endomorphism ring is the Frobenius order, which is necessarily the smallest order, and the largest endomorphism ring contains the Frobenius order with index 32 and is contained in the maximal order of K with index $625 = 5^4$. This component does not contain any horizontal isogenies.

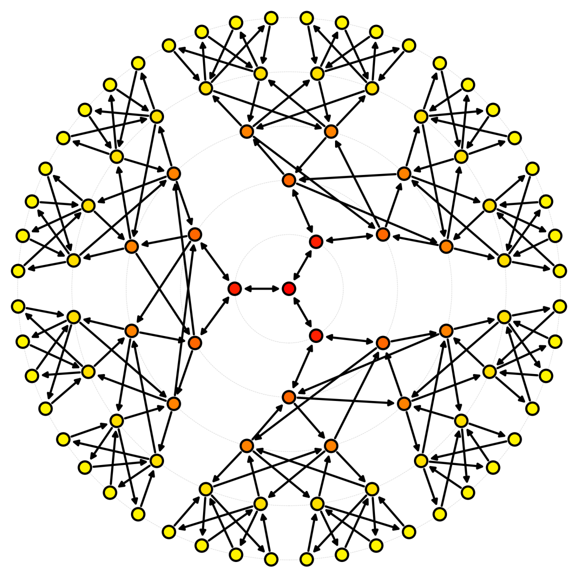

FIGURE 3. A component of the 2-isogeny graph for the base change of 4.3.c_ab_af_ai to $\mathbb{F}_9$ with 94 vertices.

2. The ideal class monoid

In [Del69], Deligne constructed an equivalence between the category of abelian varieties in an $\mathbb{F}_q$-isogeny class $\mathcal{I}_h$, together with their $\mathbb{F}_q$-homomorphisms, and the category of $\mathbb{Z}[\pi,\overline{\pi}]$-modules (up to isomorphism) that are isomorphic to fractional $\mathbb{Z}[\pi,\overline{\pi}]$-ideals, together with $\mathbb{Z}[\pi,\overline{\pi}]$-linear morphisms. We recall the construction, as we need the notation below.

To define the functor, we use that an ordinary abelian variety A defined over a finite field $\mathbb{F}_q$ of characteristic p, together with the action of its Frobenius endomorphism, admits a lifting $\tilde{A}$ to a finite extension of $\mathbb{Q}_p$, called the canonical lift of A. Deligne's functor is then defined by the association $A \mapsto T(A) = H_1(\tilde{A} \otimes_\varepsilon \mathbb{C}, \mathbb{Z})$, where $\varepsilon\colon \overline{\mathbb{Q}}_p \to \mathbb{C}$ is any fixed isomorphism. Since the endomorphism ring of $\tilde{A} \otimes_\varepsilon \mathbb{C}$ is equal to $\mathrm{End}(A)$, $T(A)$ is a $\mathbb{Z}[\pi,\overline{\pi}]$-module which is finitely generated and free of rank $2\dim(A)$, and which can be considered as a global analogue of the Tate module of A. In particular, this module allows us to study isogenies from and to A, including those where p divides the degree. The restriction $\mathcal{F}$ of this functor to $\mathcal{I}_h$ gives a bijection between isomorphism classes of abelian varieties and $\mathrm{ICM}(\mathbb{Z}[\pi,\overline{\pi}])$, which was defined in Section 1, allowing us to represent varieties and isogenies via fractional $\mathbb{Z}[\pi,\overline{\pi}]$-ideals [Mar21]. More specifically, if A and B are in $\mathcal{I}_h$ and $\varphi : A \to B$ is an isogeny, choose fractional $\mathbb{Z}[\pi,\overline{\pi}]$-ideals and identifications $J = \mathcal{F}(A)$ and $I = \mathcal{F}(B)$, and define $x = \mathcal{F}(\varphi) \in K^\times$. Then $xJ \subseteq I$, and we will frequently suppress $\mathcal{F}$ from the notation and identify the isogeny φ with this inclusion.

Let R be an order in an étale algebra K. For each pair of fractional R-ideals I, J, we define $(I : J) = \{x \in K : xJ \subseteq I\}$, the *colon ideal* of I and J. Note that, under the identification in the last paragraph, $\mathcal{F}(\mathrm{Hom}(A,B)) = \mathrm{Hom}_{\mathbb{Z}[\pi,\overline{\pi}]}(J,I)$, which can be canonically identified with $(I : J)$. Each $(I : I)$ is an overorder of R, called the *multiplicator ring* of I. As in the case of the Frobenius order $\mathbb{Z}[\pi,\overline{\pi}]$, ideal multiplication induces the structure of a commutative monoid on the set of fractional R-ideals modulo R-linear isomorphisms, and we again call it the *ideal class monoid* of R and denote it by $\mathrm{ICM}(R)$. For each overorder S of R, the set of invertible fractional S-ideals forms an abelian group, called the *Picard group* $\mathrm{Pic}(S)$ of S, and we have a natural inclusion $\mathrm{Pic}(S) \subseteq \mathrm{ICM}(R)$. This inclusion is an equality if and only if $S = R = \mathcal{O}_K$ is the maximal order of K; in this case $\mathrm{ICM}(\mathcal{O}_K)$ is the direct product of class groups.

If $\mathfrak{m}$ is a maximal R-ideal, we denote by $R_\mathfrak{m}$ the completion of R at $\mathfrak{m}$ and, for a fractional R-ideal I, we write $I_\mathfrak{m} = I \otimes_R R_\mathfrak{m}$. Two fractional R-ideals I, J are *weakly equivalent* if $I_\mathfrak{m} \simeq J_\mathfrak{m}$ for all maximal $\mathfrak{m}$; write $\{I\}$ for the weak equivalence class of I. We have $J \in \{I\}$ precisely when $(I : I) = (J : J)$ and $(I : J)$ is invertible in $(I : I)$ by [Mar20, Corollary 4.5]. Again, as in the case of $\mathbb{Z}[\pi,\overline{\pi}]$, ideal multiplication induces a commutative monoid structure on the set $\mathcal{W}(R)$ of weak equivalence classes of fractional R-ideals. The monoids $\mathrm{ICM}(R)$ and $\mathcal{W}(R)$ can be partitioned by

$$\mathrm{ICM}(R) = \bigsqcup_S \mathrm{ICM}_S(R) \qquad \text{and} \qquad \mathcal{W}(R) = \bigsqcup_S \mathcal{W}_S(R),$$

where S runs over the overorders of R, and $\mathrm{ICM}_S(R)$ (resp. $\mathcal{W}_S(R)$) contains the ideal (resp. weak equivalence) classes with multiplicator ring S.

Proposition 2.1 ([Mar20, Theorem 4.6])**.** *The group* $\mathrm{Pic}(S)$ *acts freely on* $\mathrm{ICM}_S(R)$*, and the quotient space of this action is precisely* $\mathcal{W}_S(R)$*.*

The following statement is probably well known to the expert, but we could not locate it in the literature. We provide a simple direct proof.

Lemma 2.2. *Let S be an overorder of R, and J be an invertible fractional S-ideal. Then there exists an invertible fractional R-ideal I such that $IS = J$. In particular, the extension map $I \mapsto IS$ induces a surjective group homomorphism*

$$e_S\colon \mathrm{Pic}(R) \to \mathrm{Pic}(S).$$

Proof. Let $y \in K^\times$ be such that $J' = yJ \subseteq R$, and let $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ be the support of the finite R-module S/J'. For each maximal ideal $\mathfrak{p}$ of R, the localization $S_\mathfrak{p}$ is a semilocal ring. This implies that for each $\mathfrak{p}_i$ in the support there exists an element $x_i \in J'$ such that $J'_{\mathfrak{p}_i} = (x_i S)_{\mathfrak{p}_i}$, while for every other maximal ideal $\mathfrak{q}$ of R we have that $J'_\mathfrak{q} = S_\mathfrak{q}$. Now, for each i, let k_i be an integer satisfying $\mathfrak{p}_i^{k_i} \subseteq (x_i R)_{\mathfrak{p}_i}$. Define

$$I' = \sum_{i=1}^n \left(x_i R + \mathfrak{p}_i^{k_i}\right) \prod_{j \neq i} \mathfrak{p}_j^{k_j}.$$

A direct verification shows that $I'_{\mathfrak{p}_i} = (x_i R)_{\mathfrak{p}_i}$ for all i and $I'_\mathfrak{q} = R_\mathfrak{q}$ for the other maximal ideals $\mathfrak{q}$ of R. In particular, I' is invertible, since it is locally principal, and furthermore $I'S = J'$. Therefore for $I = y^{-1} I'$ we have $IS = J$ as required. $\square$

Finally, for a fractional R-ideal I, we denote by $I^\dagger$ its *trace dual ideal*

$$I^\dagger = \{x \in K : \mathrm{Tr}_{K/\mathbb{Q}}(xI) \subseteq \mathbb{Z}\}.$$

Lemma 2.3. *Let $x \in K^\times$, L be an invertible R-ideal, and I be a fractional R-ideal.*

(1) We have $(xI)^\dagger = \frac{1}{x}I^\dagger$ *and* $(IL)^\dagger = I^\dagger L^{-1}$.
(2) The map $I \mapsto I^\dagger$ *induces well defined maps* $\mathrm{ICM}(R) \to \mathrm{ICM}(R)$ *and* $\mathcal{W}(R) \to \mathcal{W}(R)$.

Proof. The first statement follows by direct computation and localization, and the second statement from the first. □

3. Isogenies

We now discuss isogenies between isomorphism classes and set $R = \mathbb{Z}[\pi, \overline{\pi}]$ for the remainder of the paper. Because we work up to isomorphism, we impose the following equivalence relation:

Definition 3.1. 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 $i_2 \circ \varphi_1 = \varphi_2 \circ i_1$.

For the purposes of computing the isogeny graphs we seek, we will need the following two notions:

Definition 3.2. An isogeny $\varphi \colon A \to B$ of degree larger than 1 is called *minimal* if, given a decomposition $\varphi = \psi_1 \circ \psi_2$, we have that either ψ_1 or ψ_2 is an isomorphism.

As well as:

Definition 3.3. The *length* of an isogeny φ is the smallest positive integer r such that there exists a decomposition $\varphi = \varphi_1 \circ \cdots \circ \varphi_r$ of φ into minimal isogenies φ_i.

Both the length and degree are constant in an equivalence class of isogenies.

In Proposition 3.4, we obtain some properties of the Deligne functor $\mathcal{F}$ which we will need to study isogenies between abelian varieties in $\mathcal{I}_h$.

Proposition 3.4. *Let* $A, B \in \mathcal{I}_h$*, and choose fractional* $\mathbb{Z}[\pi, \overline{\pi}]$*-ideals* I *and* J *as well as isomorphisms identifying* $I = \mathcal{F}(A)$ *and* $J = \mathcal{F}(B)$*. Then for any isogeny* $\varphi \colon A \to B$*, there is an element* $x_\varphi \in (J : I) \cap K^\times$ *such that* $\mathcal{F}(\varphi)$ *can be identified with* x_φ*. Moreover, we have:*
(i) $\deg(\varphi) = [J : x_\varphi I]$.
(ii) Given a positive integer D*, if* $\deg \varphi$ *divides* D *then* $DJ \subseteq x_\varphi I$*.*
(iii) The isogeny φ *is minimal if and only if the inclusion* $x_\varphi I \subsetneq J$ *is maximal, that is, the quotient* $J/x_\varphi I$ *is a simple* R*-module.*
(iv) The length of the isogeny φ *equals the length of* $J/x_\varphi I$ *as an* R*-module.*

Proof. We use the notation introduced in Section 2 recalling the construction of Deligne's functor. Let $\tilde{\varphi} \colon \tilde{A} \to \tilde{B}$ be the canonical lift of φ, then $\deg(\varphi) = \deg(\tilde{\varphi}) = \deg(\tilde{\varphi} \otimes_\varepsilon \mathbb{C})$. Since $\tilde{\varphi} \otimes \mathbb{C}$ is separable and taking integral homology, we get

$$\deg(\varphi) = \left| \frac{T(B)}{T(\tilde{\varphi})T(A)} \right| = [J : x_\varphi I].$$

This concludes the proof of (i). Part (ii) is then an immediate consequence of (i), since a finite abelian group is annihilated by its order.

We now prove (iii). Suppose that $J/x_\varphi I$ is not simple, so there exists an R-module M such that $x_\varphi I \subsetneq M \subsetneq J$. Using Deligne's functor, this is equivalent to the existence of two isogenies $\psi_1 \colon A \to C$ and $\psi_2 \colon C \to B$ such that $\varphi = \psi_2 \circ \psi_1$, representing the inclusions $x_\varphi I \subsetneq M$ and $1 \cdot M \subsetneq J$. Since the inclusions are strict, neither ψ_1 nor ψ_2 is an isomorphism by (i).

We finally consider (iv). The length of $J/x_\varphi I$ as an R-module is the length of a chain of inclusions of R-modules

$$x_\varphi I = M_n \subsetneq M_{n-1} \subsetneq \ldots \subsetneq M_1 = J$$

in which every quotient M_i/M_{i+1} is a simple R-module. The conclusion then follows by functoriality and (iii). $\square$

Before we state our next result we need the following:

Definition 3.5. Let $\varphi\colon A \to B$ be an isogeny in $\mathcal{I}_h$. We say that φ is *horizontal* if $\mathrm{End}(A) = \mathrm{End}(B)$; φ is *ascending* if $\mathrm{End}(A) \subsetneq \mathrm{End}(B)$ and *descending* if $\mathrm{End}(B) \subsetneq \mathrm{End}(A)$; and finally φ is *vertical* if it is ascending or descending.

Theorem 3.6. *Let $\varphi\colon A \to B$ be a minimal isogeny in $\mathcal{I}_h$, and choose fractional $\mathbb{Z}[\pi,\overline{\pi}]$-ideals I and J and isomorphisms identifying $I = \mathcal{F}(A)$ and $J = \mathcal{F}(B)$ as well as an element $x \in (J : I) \cap K^\times$ and an identification $x = \mathcal{F}(\varphi)$. Then there is a unique maximal ideal $\mathfrak{m}$ of R such that $J/xI \simeq R/\mathfrak{m}$, and we have:*

- *(i) φ is horizontal or vertical, that is, $\mathrm{End}(A) \subseteq \mathrm{End}(B)$ or $\mathrm{End}(B) \subseteq \mathrm{End}(A)$.*
- *(ii) If $\mathfrak{m}$ is regular then I and J are weakly equivalent. In particular, φ is horizontal.*
- *(iii) If φ is vertical then $\mathfrak{m}$ is singular.*
- *(iv) 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 $[T : S]$.*

Proof. Using Deligne's functor we have $\mathrm{End}(A) = (I : I)$ and $\mathrm{End}(B) = (J : J)$, and since $(xI : xI) = (I : I)$ in what follows we replace xI with I for simplicity. Furthermore, since φ is minimal the finite R-module J/I is simple by Proposition 3.4.(iii), and there is a unique maximal R-ideal $\mathfrak{m}$ such that $J/I \simeq R/\mathfrak{m}$.

Now suppose that $\mathrm{End}(B) \not\subseteq \mathrm{End}(A)$, so there is an element $\beta \in (J : J) \setminus (I : I)$. Therefore we have $\beta J \subseteq J$ but $\beta I \not\subseteq I$, giving the inclusions $I \subsetneq I + \beta I \subseteq J$. Since J/I is a simple R-module, we get $I + \beta I = J$. Hence, for every $\alpha \in (I : I)$ we have

$$\alpha J = \alpha I + \beta\alpha I \subseteq I + \beta I = J.$$

This shows that $(I : I) \subseteq (J : J)$, thus proving part (i).

Since $J/I \simeq R/\mathfrak{m}$, we get that I and J are locally equal at every maximal ideal other than $\mathfrak{m}$. If $\mathfrak{m}$ is regular, then $R_\mathfrak{m} = \mathcal{O}_{K,\mathfrak{m}}$, which is a product of discrete valuation rings. It follows that $I_\mathfrak{m}$ and $J_\mathfrak{m}$ are isomorphic, so I and J are weakly equivalent. In particular, $(I : I) = (J : J)$, that is, φ is a horizontal isogeny. This completes the proof of part (ii), and part (iii) is immediate.

We finally prove part (iv). As observed above I and J are locally equal at every maximal ideal other than $\mathfrak{m}$. Since taking colon ideals commutes with localization, the same is true for their multiplicator rings. Hence, T/S is either trivial or a finite R-module whose support contains only $\mathfrak{m}$. In both cases, we have the equality $|T/S| = |R/\mathfrak{m}|^{\mathrm{length}_R(T/S)}$. The former case happens precisely when φ is horizontal, thus completing the proof. $\square$

In the ℓ-isogeny graph of ordinary elliptic curves, if the isogeny $\varphi\colon A \to B$ is vertical then the index of one of the endomorphism rings in the other is at most

ℓ. This implies that there is no order strictly between $\mathrm{End}(A)$ and $\mathrm{End}(B)$ if ℓ is prime. The following shows that this results fails in general for minimal isogenies.

Example 3.7. Let $\mathcal{I}_h$ be the isogeny class of abelian surfaces defined over $\mathbb{F}_5$ with LMFDB label 2.5.a_g given by the Weil polynomial $h(x) = x^4 + 6x^2 + 25 = (x^2 - 2x + 5)(x^2 + 2x + 5)$. Let R be the Frobenius order of $\mathcal{I}_h$, which has index $[\mathcal{O}_K : R] = 64$ in the maximal order $\mathcal{O}_K$ of the endomorphism algebra K. Then R has a unique singular maximal ideal $\mathfrak{m}$ with residue field $\mathbb{F}_2$, as well as a unique overorder S satisfying $[\mathcal{O}_K : S] = 8$. Furthermore, the conductor $\mathfrak{f}_S = (S : \mathcal{O}_K)$ of S in $\mathcal{O}_K$ is the unique singular maximal ideal of S, we have an isomorphism $S/\mathfrak{f}_S \simeq R/\mathfrak{m}$, and $(\mathfrak{f}_S : \mathfrak{f}_S) = \mathcal{O}_K$.

Let $\varphi\colon A \to B$ be the descending isogeny that is sent to the inclusion $1 \cdot \mathfrak{f}_S \subset S$ by Deligne's functor; this isogeny is minimal of degree 2 by Proposition 3.4 parts (i) and (iii) since $S/\mathfrak{f}_S$ is simple of size 2. Relating this to Theorem 3.6.(iv), we observe that $\mathrm{length}_R(\mathcal{O}_K/S) = 3 = 2\dim(A) - 1$, and indeed $[\mathrm{End}(A) : \mathrm{End}(B)] = [\mathcal{O}_K : S] = \deg(\varphi)^3$. This agrees with [Bis15, Lemma 2.1] where isogenies with kernel $(\mathbb{Z}/\ell\mathbb{Z})^g$ are considered instead.

Strikingly, there are several orders T such that $S \subsetneq T \subsetneq \mathcal{O}_K$, despite the fact that φ is minimal. Indeed, S has 4 overorders with index 4 in $\mathcal{O}_K$ and 3 overorders with index 2 in $\mathcal{O}_K$.

Proposition 3.8. *Let $\varphi_1\colon A_1 \to B_1$ and $\varphi_2\colon A_2 \to B_2$ be two isogenies in $\mathcal{I}_h$, and for $i = 1, 2$, choose fractional $\mathbb{Z}[\pi, \overline{\pi}]$-ideals I_i and J_i and isomorphisms identifying $I_i = \mathcal{F}(A_i)$ and $J_i = \mathcal{F}(B_i)$, as well as elements $x_i \in (J_i : I_i) \cap K^\times$ and identifications $x_i = \mathcal{F}(\varphi_i)$. Furthermore, let $M_i = x_i I_i \subseteq J_i$. The following are equivalent:*

- *(i) $\varphi_1 \approx \varphi_2$, that is, the isogenies are equivalent.*
- *(ii) There are elements $k_A, k_B \in K^\times$ such that $k_A I_1 = I_2$, $k_B J_1 = J_2$ and $x_2 k_A = k_B x_1$.*
- *(iii) There are elements $k_A, k_B \in K^\times$ such that $k_A I_1 = I_2$, $k_B J_1 = J_2$ and $k_B M_1 = M_2$.*

Proof. The equivalence of (i) and (ii) follows from the fact that $\mathcal{F}$ is an equivalence of categories. The fact that (ii) implies (iii) is clear. So, assume (iii). We get

$$k_B x_1 I_1 = k_B M_1 = M_2 = x_2 I_2 = x_2 k_A I_1.$$

Let $u = \frac{x_2 k_A}{k_B x_1}$. Then u is a unit of the order $(I_1 : I_1)$. If we let $k_0 = k_A u^{-1}$ we then obtain $k_0 I_1 = I_2$, $k_B J_1 = J_2$ and $x_2 k_0 = k_B x_1$, by which (ii) holds. □

Corollary 3.9. *Let $\varphi_1\colon A_1 \to B$ and $\varphi_2\colon A_2 \to B$ be isogenies with the same codomain, and choose fractional $\mathbb{Z}[\pi, \overline{\pi}]$-ideals J and I_i and isomorphisms identifying $J = \mathcal{F}(B)$ and $I_i = \mathcal{F}(A_i)$ for $i = 1, 2$, as well as elements $x_i \in (J : I_i) \cap K^\times$ and identifications $x_i = \mathcal{F}(\varphi_i)$. As before let $M_i = x_i I_i \subseteq J$. The following are equivalent:*

- *(i) $\varphi_1 \approx \varphi_2$, that is, the isogenies are equivalent.*
- *(ii) There exists an element $k_A \in K^\times$ such that $k_A I_1 = I_2$ and a unit $u \in (J : J)^\times$ such that $x_2 k_A = x_1 u$.*
- *(iii) There exists a unit $u \in (J : J)^\times$ such that $u M_1 = M_2$.*

Moreover, if $A_1 = A_2$ and we let $\mathcal{F}(A_1) = \mathcal{F}(A_2) = I$ then (i)-(iii) above are also equivalent to *(iv) there are units $v \in (I : I)^\times$ and $u \in (J : J)^\times$ such that $x_2 v = u x_1$.*

Proof. The equivalence of (i) and (ii) follows by Proposition 3.8. Assume (i). By Proposition 3.8, there is an element $u \in K^\times$ such that $uJ = J$ and $uM_1 = M_2$. In particular, $u \in (J : J)^\times$, and (iii) holds. Assume now (iii), so that $ux_1 I_1 = x_2 I_2$. By setting $k_A = ux_1/x_2$ and $k_B = u$, we see that Proposition 3.8.(iii) holds, which is equivalent to (i). Finally if $A_1 = A_2$ the equivalence of (ii) and (iv) is clear. □

For ordinary elliptic curves with non-maximal endomorphism ring, prime degree isogenies are always vertical [Sut13, §2.7]; this is another fact that fails in general:

Example 3.10. Consider the isogeny class with label 2.11.a_ac given by the Weil polynomial $h(x) = x^4 - 2x^2 + 121$, and as usual denote its Frobenius order by R. Then R has a unique singular maximal ideal $\mathfrak{m}$ of index $[R : \mathfrak{m}] = 2$. The 4 overorders of R form a chain of inclusions $R \subset S_4 \subset S_2 \subset \mathcal{O}_K$ all of index 2.

A computation shows there are two weak equivalence classes of fractional R-ideals with multiplicator ring $S_4 : \mathcal{W}_{S_4}(R) = \{[S_4], [S_4^\dagger]\}$. Set $J = S_4^\dagger$, which is not invertible as a fractional S_4-ideal. A further computation shows that J contains exactly 3 fractional R-ideals $I_1, I_2, I_3 \subset J$ with $[J : I_i] = 2$. For each such I_i, the inclusion $1 \cdot I_i \subset J$ represents a minimal isogeny of degree 2. One of these fractional ideals is the trace dual ideal, say $I_1 = S_2^\dagger$; since $S_4 \subsetneq S_2$ this implies the isogeny corresponding to $1 \cdot I_1 \subset J$ is a minimal descending isogeny.

The other two ideals I_2, I_3 are non-isomorphic invertible fractional S_4-ideals. In particular, the isogenies induced by $1 \cdot I_2 \subset J$ and $1 \cdot I_3 \subset J$ are horizontal. For both of these isogenies the source and target are not weakly equivalent as ideals. Moreover, using Proposition 3.8, one sees that these isogenies are not equivalent.

With these results, we are ready to compute isogeny equivalences.

Algorithm 3.11 (`AreIsogeniesEquivalent`)**.**
Input: For R the Frobenius order of an isogeny class $\mathcal{I}_h$, inclusions $x_1 I_1 \subset J_1$ and $x_2 I_2 \subset J_2$ of R-ideals representing two isogenies.
Output: Whether the two isogenies are equivalent.

(1) Compute the multiplicator rings S of I_1 and T of J_1.
(2) Compute the unit groups $S^\times, T^\times$ as subgroups of $\mathcal{O}_K^\times$.
(3) Compute elements $y, z \in K^\times$ such that $I_1 = yI_2$ and $J_1 = zJ_2$ (if not possible, return *false*).
(4) If $\frac{x_1 y}{x_2 z} \in S^\times T^\times$ then return *true*; else return *false*.

Proof. The algorithm is correct by Corollary 3.9.(iv). □

We caution that composition is not well defined on equivalence classes:

Proposition 3.12. *Let $\varphi\colon A \to B$ and $\psi\colon B \to C$ be isogenies and ρ an automorphism of B; then φ and $\rho \circ \varphi$ are equivalent isogenies. Choose fractional $\mathbb{Z}[\pi, \overline{\pi}]$-ideals H, I and J and identifications $H = \mathcal{F}(A)$, $I = \mathcal{F}(B)$ and $J = \mathcal{F}(C)$, as well as elements $x \in (I : H) \cap K^\times$, $y \in (J : I) \cap K^\times$ and $z \in (I : I)^\times$ and identifications $x = \mathcal{F}(\varphi)$, $y = \mathcal{F}(\psi)$ and $z = \mathcal{F}(\rho)$. Then the compositions $\psi \circ \varphi$ and $\psi \circ \rho \circ \varphi$ are equivalent if and only if $z \in (H : H)^\times (J : J)^\times$.*

Proof. The compositions $\psi \circ \varphi$ and $\psi \circ \rho \circ \varphi$ correspond to the inclusions $yxH \subset J$ and $yzxH \subset J$, respectively. By Corollary 3.9.(iv), the compositions are equivalent if and only if there are units $u \in (H:H)^\times$ and $v \in (J:J)^\times$ such that $uyx = vyzx$. This happens precisely when $z = uv^{-1}$, thus completing the proof. □

Finally we end this section with a result which will be useful below:

Lemma 3.13. *Let R be the Frobenius order of an isogeny class and I and J be fractional R-ideals. Assume that I and J are weakly equivalent, so that $(I:J)$ is an invertible fractional $(I:I)$-ideal. Let L be an invertible fractional R-ideal such that $L(I:I) = (I:J)$, which exists by Lemma 2.2. Then the following maps are inverses of each other:*

$$\{\textit{fractional } R\textit{-ideals } M \subseteq J\} \longrightarrow \{\textit{fractional } R\textit{-ideals } N \subseteq I\}$$
$$M \longmapsto ML$$
$$NL^{-1} \longleftarrow N.$$

This bijection preserves inclusions and indices: $[J:M] = [I:ML]$.

Proof. Since L is invertible, clearly the map is injective and inclusion preserving. Let p be a rational prime dividing $[W:M]$ and let x be a generator of L_p over R_p. Then $I_p = x_p W_p$ and $(ML)_p = x_p M_p$ which shows that the map preserves indices. To prove that the map is surjective, choose $N \subseteq I$ and denote by S the multiplicator ring of I. Since $L^{-1} = (R:L)$, we have $L^{-1}S \cdot LS = RS = S$; because the inverse is unique, we get that $L^{-1}S = (LS)^{-1}$, which implies that $L^{-1}S = (W:I)$. Now consider the fractional R-ideal $M = L^{-1}N$; we have $ML = N$. To show that M is a preimage of N, we need to show that $M \subseteq J$, but this is the case since

$$M \subseteq MS = L^{-1}NS = L^{-1}SNS = (J:I)N \subseteq (J:I)I = J.$$

□

4. Isogeny graphs

We finally define the main object of study of this article, the isogeny graph associated to an isogeny class $\mathcal{I}_h$. Let h be a q-Weil polynomial, R the corresponding Frobenius order and $\mathcal{I}_h$ the corresponding isogeny class of $\mathbb{F}_q$-abelian varieties. For each weak equivalence class w of fractional R-ideals, we fix a representative ideal W_w and write $\mathfrak{w}_w$ for the class of W_w in $\mathrm{ICM}(R)$. We may represent each ideal class $[M] \in \mathrm{ICM}(R)$ by the pair $(w_M, \mathfrak{a}_M)$, where $w_M = \{M\}$ is the weak equivalence class of M and $\mathfrak{a}_M = [(M : W_{\{M\}})] \in \mathrm{Pic}((M:M))$.

Moreover, we choose an ideal M within each ideal class $[M] \in \mathrm{ICM}(R)$; we may then represent any isogeny $\varphi : A \to B$ by an element x_φ as in Corollary 3.4 so that $x_\varphi I \subset J$, where I is the chosen ideal in the ideal class corresponding to A and J is the chosen ideal in the ideal class corresponding to B.

Definition 4.1.

(1) The *full isogeny graph* $\mathcal{G}$ of an isogeny class $\mathcal{I}_h$ is the labeled directed multigraph whose vertices are isomorphism classes of abelian varieties in $\mathcal{I}_h$ and whose edges are equivalence classes of isogenies of degree > 1. The set $\mathcal{V}$ of vertices is labeled by pairs $(w_M, \mathfrak{a}_M)$, and the set $\mathcal{E}$ of edges by the multiplication-by-x map from the source I to the target J (which we will simply write as $xI \subset J$). Here I and J are the chosen representatives, and x is as described above.

(2) Let D be a positive integer. The *D-isogeny graph* $\mathcal{G}^D$ is the subgraph of $\mathcal{G}$ with edges $\mathcal{E}^D$ of degree dividing D.
(3) Let D and r be positive integers. The graph $\mathcal{G}^{D,r}$ is the subgraph of $\mathcal{G}$ with edges $\mathcal{E}^{D,r}$ of degree dividing D and length at most r.

Proposition 4.2. *Let R be the Frobenius order of an isogeny class $\mathcal{I}_h$. A minimal isogeny of degree ℓ^n exists in $\mathcal{I}_h$ if and only if R has a maximal ideal of index ℓ^n.*

In particular, if there is no maximal ideal of R of index dividing D then the set $\mathcal{E}^D$ of edges of $\mathcal{G}^D$ is empty.

Proof. Let $\varphi\colon A \to B$ be a minimal isogeny of degree ℓ^n in $\mathcal{I}_h$. Then the existence of a maximal R-ideal $\mathfrak{l}$ with index ℓ^n follows from Proposition 3.4 parts (i) and (iii) since any finite simple R-module is isomorphic to $R/\mathfrak{l}$ for some maximal ideal $\mathfrak{l}$.

Conversely, given a maximal R-ideal $\mathfrak{l}$ of index ℓ^n, consider the inclusion $1\cdot\mathfrak{l} \subset R$. Let $\varphi\colon A \to B$ be an isogeny in $\mathcal{I}_h$ such that we can make the identifications $\mathfrak{l} = \mathcal{F}(A)$, $R = \mathcal{F}(B)$ and $1 = \mathcal{F}(\varphi)$. Then φ has degree ℓ^n by Proposition 3.4.(i). □

Remark 4.3. Deligne's functor $\mathcal{F}$ is particularly well suited for studying base field extensions; see [Mar22] for a comprehensive treatment. We collect here a few facts which will be used in the next examples. As usual let $\mathcal{I}_h$ be an ordinary isogeny class defined over $\mathbb{F}_q$ with squarefree Weil polynomial $h(x)$, and $R_1 = \mathbb{Z}[\pi,\overline{\pi}]$ be its Frobenius order. For i a positive integer, denote by $h_i(x)$ the Weil polynomial of the isogeny class $\mathcal{I}_h \otimes \mathbb{F}_{q^i}$, and we assume further that $h_i(x)$ is also squarefree. The Frobenius order R_i of $\mathcal{I}_{h_i}$ can be identified with the order $\mathbb{Z}[\pi^i,\overline{\pi}^i]$ in K. In particular, if A is in $\mathcal{I}_{h_i}$ and I is a fractional R_i-ideal corresponding to A, then A can be defined over $\mathbb{F}_q$ if and only if $R_1 \subseteq (I : I)$.

More generally, the natural inclusion $\mathrm{ICM}(R_1) \subseteq \mathrm{ICM}(R_i)$ implies that $\mathcal{G}$ is a subgraph of $\mathcal{G}_i$, where $\mathcal{G}$ and $\mathcal{G}_i$ are the full isogeny graphs of $\mathcal{I}_h$ and $\mathcal{I}_{h_i}$ (respectively). This gives us an injection from the vertices of $\mathcal{G}$ to the vertices of $\mathcal{G}_i$. Furthermore, for any $A, B \in \mathcal{I}_h$ defined over $\mathbb{F}_q$, we have identifications $\mathrm{Hom}_{\mathbb{F}_q}(A,B) = (\mathcal{F}(A) : \mathcal{F}(B)) = \mathrm{Hom}_{\mathbb{F}_{q^i}}(A,B)$. This shows that if we fix two vertices in $\mathcal{G}$, they are connected by an edge in $\mathcal{G}$ if and only if they are in $\mathcal{G}_i$. Analogous statements hold for the D-isogeny graph $\mathcal{G}^D$.

Finally, if $\mathcal{I}_h$ is geometrically simple and ordinary then $h_i(x)$ is an irreducible polynomial for every $i > 1$ and automatically squarefree. Therefore, by taking the limit we get an embedding of the isogeny graph over $\mathbb{F}_q$ into the associated isogeny graph over $\overline{\mathbb{F}}_q$. This limit is a regular graph, and as i increases the edges going out of a fixed vertex will appear at the same time as their target does.

Corollary 4.4. *Let ℓ be a prime number and $\mathcal{G}$ be the ℓ-isogeny graph of an isogeny class defined over $\mathbb{F}_q$ with Frobenius order R_1. Let $\mathcal{G}'$ be the ℓ-isogeny graph for the same isogeny class base changed $\mathbb{F}_{q^i}$ for $i > 1$, and with Frobenius order R_i.*

In this situation, if $\mathcal{G}$ has no edges and $\mathcal{G}'$ has edges then ℓ divides $[R_1 : R_i]$.

Proof. Proposition 4.2 implies that R_i has a maximal ideal $\mathfrak{m}$ of index ℓ while R_1 does not. Note that $R_1/\mathfrak{m}R_1$ is an $R_i/\mathfrak{m}$-vector space of dimension $n > 1$, since R_1 does not have a maximal ideal of index ℓ. Consider the map of finite abelian groups $\sigma\colon R_1/R_i \to (R_1/\mathfrak{m}R_1)/(R_i/\mathfrak{m})$. We have that $[R_1 : R_i] = \ell^{n-1}\cdot|\ker(\sigma)|$ which implies that ℓ divides $[R_1 : R_i]$. □

To illustrate Remark 4.3, we present an example of a 2-isogeny graph of abelian surfaces over $\mathbb{F}_3$ with no edges. We explain how 2-isogenies appear after base change to $\mathbb{F}_{3^i}$ for appropriate $i > 1$. Note that there exist arbitrarily large i where the 2-isogeny graph over $\mathbb{F}_{3^i}$ has no edge.

Example 4.5. Consider the isogeny class $\mathcal{I}_h$ of geometrically simple abelian surfaces over $\mathbb{F}_3$ with LMFDB label 2.3.ad_f and Weil polynomial $h(x) = x^4 - 3x^3 + 5x^2 - 9x + 9$. Over the fields $\mathbb{F}_3, \mathbb{F}_9, \mathbb{F}_{81}$, and $\mathbb{F}_{6561}$ the 2-isogeny graph has 1, 5, 145 and 672945 vertices respectively, all with no edges.

The Frobenius order R_1 of $\mathcal{I}_h$ is the maximal order $\mathcal{O}_K$; it has a unique maximal ideal $\mathfrak{m}$ above 2 which is of index 16. By Proposition 4.2, the 2-isogeny graph of $\mathcal{I}_h$ therefore has no edges.

Now for i a positive integer and $\mathcal{I}_{h_i}$ the base change of $\mathcal{I}_h$ to $\mathbb{F}_{3^i}$, let R_i be the Frobenius order of $\mathcal{I}_{h_i}$. Corollary 4.4 implies that if $[R_1 : R_i]$ is coprime to 2, there will be no edges in the 2-isogeny graph over $\mathbb{F}_{3^i}$. Table 1 records first the cardinality of $\mathrm{ICM}(R_i)$ – which we observe grows very quickly – and the indices of the maximal primes above 2. Then, to track the development of 2-isogenies we define $[R_1 : R_i]_{\mathrm{new}}$ to be the index $[R_1 : R_i]$ divided by the least common multiple of $[R_1 : R_j]$ for proper divisors j of i.

i	$\#\mathrm{ICM}(R_i)$	$[[R_i : \mathfrak{m}] : 2 \in \mathfrak{m}]$	$[R_1 : R_i]_{\mathrm{new}}$	$[R_1 : R_i]/[R_1 : R_i]_{\mathrm{new}}$
1	1	[16]	1	1
2	5	[16]	3^2	1
3	25	[16]	23	1
4	145	[16]	29	3^2
5	5246	[2]	$2^6 \cdot 61$	1
6	8075	[16]	$3^2 \cdot 17$	$3^2 \cdot 23$
7	201707	[16]	$29^2 \cdot 1667$	1
8	672945	[16]	$23^2 \cdot 103$	$3^2 \cdot 29$
9	234025	[16]	$17^2 \cdot 251$	23
10	10677440	[2]	2^8	$2^6 \cdot 3^2 \cdot 61$
11	10716555	[16]	$419^2 \cdot 25453$	1
12	3464756875	[16]	$23 \cdot 61^2$	$3^4 \cdot 17 \cdot 23 \cdot 29$
13	–	[16]	$5^2 \cdot 13^6 \cdot 131$	1
14	–	[16]	2731	$3^2 \cdot 29^2 \cdot 1667$
15	–	[2]	$569^2 \cdot 719$	$2^6 \cdot 23 \cdot 61$
16	–	[16]	15473	$3^2 \cdot 23^2 \cdot 29 \cdot 103$
17	–	[16]	$9283^2 \cdot 10449287$	1
18	–	[16]	$3^2 \cdot 17^4 \cdot 179$	$3^4 \cdot 17^2 \cdot 23 \cdot 251$
19	–	[16]	$191 \cdot 1901^2 \cdot 276337$	1
20	–	[2]	$2^6 \cdot 199^2 \cdot 1301$	$2^{14} \cdot 3^2 \cdot 29 \cdot 61$

Table 1. Information about the isogeny class 2.3.ad_f. See Example 4.5 for a description.

Theorem 4.6. *Let $D > 1$, R be the Frobenius order of the isogeny class $\mathcal{I}_h$, and $\mathcal{S}^{\mathrm{sing}}$ be the set of maximal R-ideals containing the conductor $\mathfrak{f}_R = (R : \mathcal{O}_K)$ of R.*

(i) Suppose that there exists a set $\mathcal{S}$ of (non-necessarily invertible) maximal ideals $\mathfrak{l}$ of R such that their extensions $\mathfrak{l}\mathcal{O}_K$ form a generating set of $\mathrm{Pic}(\mathcal{O}_K)$

and that the integer

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

divides D. Then the isogeny graph $\mathcal{G}^D$ is connected (as a directed graph).

(ii) *Let $\mathcal{S}$ be a set of maximal R-ideals satisfying the conditions in (i). Then the diameter of $\mathcal{G}^{D,1}$ satisfies:*

$$\operatorname{diam}(\mathcal{G}^{D,1}) \leq \begin{cases} 2\operatorname{length}_R(\mathcal{O}_K/R) + \sum_{\mathfrak{l}\in\mathcal{S}}\left(\operatorname{ord}_{\operatorname{Pic}(\mathcal{O}_K)}([\mathfrak{l}\mathcal{O}_K]) - 1\right) & \text{if } R \text{ is Bass,} \\ 2\left(\operatorname{length}_R(\mathcal{O}_K/\mathfrak{f}_R) - 1\right) + \sum_{\mathfrak{l}\in\mathcal{S}}\left(\operatorname{ord}_{\operatorname{Pic}(\mathcal{O}_K)}([\mathfrak{l}\mathcal{O}_K]) - 1\right) & \text{otherwise,} \end{cases}$$

where $\operatorname{ord}_G(h)$ for an element h of a group G denotes the order of h in G.

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

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

(iv) *Assume that $\mathcal{G}^D$ is connected. Then*

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

Proof. Let $\mathcal{S} = \{\mathfrak{l}_1, \ldots, \mathfrak{l}_n\}$ and $N_{\mathcal{S}}$ be as in (i). Consider any two fractional R-ideals I and J. By [Mar20, Remark 5.4], there are invertible R-ideals L_I and L_J such that $\mathfrak{f}_R L_I \subseteq I \subseteq \mathcal{O}_K L_I$ and $\mathfrak{f}_R L_J \subseteq J \subseteq \mathcal{O}_K L_J$. We construct a path $[I] \to [\mathcal{O}_K L_I] \to [\mathfrak{f}_R L_J] \to [J]$ which is a composition of minimal isogenies in $\mathcal{G}^D$.

We have isomorphisms of finite R-modules $\mathcal{O}_K/\mathfrak{f}_R \simeq \mathcal{O}_K L_I/\mathfrak{f}_R L_I \simeq \mathcal{O}_K L_J/\mathfrak{f}_R L_J$. The simple factors of $\mathcal{O}_K/\mathfrak{f}_R$ are $R/\mathfrak{m}$ for $\mathfrak{m} \in \mathcal{S}^{\mathrm{sing}}$. By Proposition 3.4, each such simple factor is equivalent to an edge of degree $|R/\mathfrak{m}|$ which belongs to $\mathcal{E}^D$ by the assumption on $N_{\mathcal{S}}$. Hence, the paths $[I] \to [\mathcal{O}_K L_I]$ and $[\mathfrak{f}_R L_J] \to [J]$ are in $\mathcal{G}^D$, each one with length bounded by $\operatorname{length}_R(\mathcal{O}_K/\mathfrak{f}_R) - 1$, where the -1 comes from the fact that $\mathfrak{f}_R$ and $\mathcal{O}_K$ are in the same weak equivalence class.

Since $\mathcal{O}_K L_I$ and $\mathfrak{f}_R L_J$ are both invertible fractional $\mathcal{O}_K$-ideals, and $\mathcal{S}$ generates $\operatorname{Pic}(\mathcal{O}_K)$, there are $a \in K^\times$ and integers $0 \leq e_i < \operatorname{ord}_{\operatorname{Pic}(\mathcal{O}_K)}([\mathfrak{l}_i\mathcal{O}_K])$ such that

$$a\mathcal{O}_K L_I = (\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}\mathcal{O}_K)\mathfrak{f}_R L_J.$$

Therefore an edge $[\mathcal{O}_K L_I] \to [\mathfrak{f}_R L_J]$ can be obtained as the composition of at most $\sum_{i=1}^n \left(\operatorname{ord}_{\operatorname{Pic}(\mathcal{O}_K)}([\mathfrak{l}_i\mathcal{O}_K]) - 1\right)$ minimal edges in $\mathcal{G}^D$. This proves (i) and gives the generic bound of (ii).

Suppose now that R is Bass; we prove the refined bound of (ii) by modifying the argument above. Let I and J be fractional R-ideals, which are invertible in their respective multiplicator rings S_I and S_J since R is Bass by [BL94, Prop. 2.7]. By Lemma 2.2, there is an invertible fractional R-ideal L_I such that

$$L_I \subseteq L_I S_I = I \subseteq L_I\mathcal{O}_K = I\mathcal{O}_K.$$

The isomorphism of R-modules $L_I\mathcal{O}_K/L_I \simeq \mathcal{O}_K/R$ then yiels a path $[I] \to [I\mathcal{O}_K]$ in $\mathcal{G}^D$ of length bounded by $\operatorname{length}_R(\mathcal{O}_K/R)$. Now, consider the $\mathcal{O}_K$-ideal $\mathfrak{f}_J = (S_J : \mathcal{O}_K)$; as argued above the path $[I\mathcal{O}_K] \to [\mathfrak{f}_J J]$ is in $\mathcal{G}^D$ with length bounded by $\sum_{i=1}^n \left(\operatorname{ord}_{\operatorname{Pic}(\mathcal{O}_K)}([\mathfrak{l}_i\mathcal{O}_K]) - 1\right)$. Finally consider the finite R-module $M = J/\mathfrak{f}_J J$. Since J is invertible in S_J, we have an R-linear isomorphism $M \simeq S_J/\mathfrak{f}_J$. Moreover, since R is Bass then S_J is Gorenstein. Hence $\operatorname{length}_R(S_J/\mathfrak{f}_J) = \operatorname{length}_R(\mathcal{O}_K/S_J)$ by [Bas63, Cor. 6.5]. This implies that $\operatorname{length}_R(M)$ is bounded by $\operatorname{length}_R(\mathcal{O}_K/R)$, and therefore the inclusion $\mathfrak{f}_J J \subseteq J$ induces a path $[\mathfrak{f}_J J] \to [J]$ in $\mathcal{G}^D$ of length bounded by $\operatorname{length}_R(\mathcal{O}_K/R)$. These three paths give the refined bound in (ii).

We now prove (iii). Let $\mathfrak{l}$ be in $\mathcal{S}^{\mathrm{sing}}$. By assumption there is a path $E\colon [\mathfrak{l}] \to [R]$ which is a composition of minimal isogenies of degree dividing D. Let $a \in K^\times$ be an element such that E is represented by the inclusion $a\mathfrak{l} \subseteq R$. Since $\mathfrak{l}$ is singular, we have $(R : \mathfrak{l}) = (\mathfrak{l} : \mathfrak{l})$, see for example [Mar24, Lemma 2.8]. It follows that $a\mathfrak{l} \subseteq \mathfrak{l} \subset R$. Therefore in any composition series of $R/a\mathfrak{l}$ there is a simple factor isomorphic to $R/\mathfrak{l}$, and in any decomposition of E into minimal isogenies, there is one with kernel isomorphic to $R/\mathfrak{l}$ by Proposition 3.4.(iii). Thus $|R/\mathfrak{l}|$ divides D.

Finally to prove (iv), assume that $\mathcal{G}^D$ is connected and take any path $E\colon [\mathcal{O}_K] \to [R]$ in $\mathcal{G}^D$. If E is represented by the inclusion $a\mathcal{O}_K \subset R$ for $a \in K^\times$, then $a \in \mathfrak{f}_R$ and we have inclusions $a\mathcal{O}_K \subseteq \mathfrak{f}_R \subseteq R$. The length of E equals $\mathrm{length}_R(R/a\mathcal{O}_K)$ by Proposition 3.4.(iv); this is bounded from below by $\mathrm{length}_R(R/\mathfrak{f}_R)$. Since the choice of the path E between $[\mathcal{O}_K]$ and $[R]$ was arbitrary, we deduce that $\mathrm{length}_R(R/\mathfrak{f}_R)$ is a lower bound for $\mathrm{diam}(\mathcal{G}^{D,1})$, that is, the inequality in (iv) holds. □

Remark 4.7. The bounds of Theorem 4.6 are in general not sharp, but they are frequently attained. We ran the following experiment:[1] we consider a large number of ordinary squarefree isogeny classes such that $\mathbb{Z}[\pi, \overline{\pi}]$ has exactly one singular maximal ideal $\mathfrak{m}$ and such that $\mathcal{O}_K$ has trivial Picard group. We compute $\mathcal{G}^D$ for $D = |R/\mathfrak{m}|$ and its diameter d.

We observe that in many cases the lower bound on d from in (iv) is attained. There are many cases in which the two upper bounds in (ii) are equal to 2 and attained; in all these cases $\mathbb{Z}[\pi, \overline{\pi}]$ is Bass. We note that there are several examples in which the refined upper bound in the Bass case is attained and is strictly smaller than the generic bound; for almost all of these example $\mathbb{Z}[\pi, \overline{\pi}]$ is Bass. We did not find any non-Bass example whose diameter exceeded the smaller bound, so it is possible that the Bass bound holds for all R.

5. Computing the isogeny graph

We now give an algorithm to compute the D-isogeny graph $\mathcal{G}^D$ of the isogeny class $\mathcal{I}_h$ with Frobenius order R. The computation of $\mathcal{G}^D$ is divided in two steps: First we compute the subgraph $\mathcal{G}^{D,1}$ containing only minimal edges in Algorithm 5.1, and then we recover $\mathcal{G}^D$ by taking all possible compositions in Algorithm 5.2. For each overorder S of R let e_S be the natural map $\mathrm{Pic}(R) \to \mathrm{Pic}(S)$ (c.f. Lemma 2.2), and for each class in $\mathrm{Pic}(S)$, fix a preimage $\mathfrak{a} \in \mathrm{Pic}(R)$ via e_S and an invertible fractional R-ideal $I_{\mathfrak{a}}$ representing $\mathfrak{a}$. We denote the set of chosen preimages in $\mathrm{Pic}(R)$ by $\mathcal{P}_S$, and recall the definition of W_w and the labeling of $\mathcal{G}^D$ from Definition 4.1. We have previously written w for a weak equivalence class; going forward we will use s for the weak equivalence class of the source of an isogeny and t for the target.

Algorithm 5.1 (`MinimalIsogenyGraphBuilder`).

Input: A q-Weil polynomial h and an integer $D > 1$.

Output: The subgraph $\mathcal{G}^{D,1}$ of the D-isogeny graph $\mathcal{G}^D$ of the isogeny class $\mathcal{I}_h$.

(1) Compute the set $\mathcal{V}$ of vertices $(t, e_T(\mathfrak{b}))$ by computing all weak equivalence classes t of R and ideal classes $\mathfrak{b} \in \mathcal{P}_T$, for T the multiplicator ring of t.

(2) For each weak equivalence class t:

  (a) Compute the fractional R-ideals M contained in W_t such that the inclusion $M \subset W_t$ is maximal and the index $[W_t : M]$ divides D.

---

[1] See `bounds_diameter_GD.m` in [CDMRV26] for details and raw output.

Algorithmic Number Theory Symposium XVII, Groningen, July 6-10, 2026

(b) Compute the orbits of these submodules under the action of $T^\times$, and choose a representative M for each orbit.
(c) For each orbit representative M do:
  (i) Compute the vertex $(s, e_S(\mathfrak{a})) \in \mathcal{V}$ that represents the ideal class of M, where $S = (M : M)$ and $\mathfrak{a} \in \mathcal{P}_S$, together with $x \in K^\times$ such that $xW_sI_\mathfrak{a} = M$.
  (ii) For every $\mathfrak{b} \in \mathcal{P}_T$ do:
    (A) Compute an element $y \in K^\times$ such that $yI_{\mathfrak{a}'}S = I_\mathfrak{a}I_\mathfrak{b}S$ where $\mathfrak{a}'$ is the unique element in $\mathcal{P}_S$ satisfying $e_S(\mathfrak{a}\mathfrak{b}) = e_S(\mathfrak{a}')$.
    (B) Yield the (minimal) edge $(s, e_S(\mathfrak{a}')) \to (t, e_T(\mathfrak{b}))$ with label $xyW_sI_{\mathfrak{a}'} \subset W_tI_\mathfrak{b}$.

Proof. The set of vertices $\mathcal{V}$ is complete by Proposition 2.1.

Let I and J be fractional R-ideals and $a \in K^\times$ be such that $aI \subset J$ is maximal with index dividing D. To show that the set $\mathcal{E}^{D,1}$ of minimal edges returned by the algorithm is complete, we prove that there is an edge in $\mathcal{E}^{D,1}$ representing the equivalence class of the corresponding minimal isogeny. Let t be the weak equivalence class of J and $\mathfrak{b} \in \mathcal{P}_T$ be such that $(J : W_t) \in e_T(\mathfrak{b})$. Thus there exists $b \in K^\times$ such that $bI_\mathfrak{b}T = (J : W_t)$, where $I_\mathfrak{b}$ is the chosen representative of $\mathfrak{b}$. Consider the invertible fractional R-ideal $L = bI_\mathfrak{b}$. By construction, we have $LW_t = J$. Set $M = L^{-1}(aI)$. By Lemma 3.13, $M \subset W_t$ is a maximal inclusion of index dividing D, that is, M is one of the fractional R-ideals computed in step 2a. If u is a unit of $T = (W_t : W_t) = (J : J)$ then the isogenies $aI \subset J$ and $uaI \subset J$ are equivalent by Corollary 3.9.(iv). Hence, we can assume that M is the orbit representative picked in step 2c. We have $MI_\mathfrak{b} = (1/b)aI$ and $W_tI_\mathfrak{b} = (1/b)J$. By Proposition 3.8.(i), the isogeny $aI \subset J$ is equivalent to $MI_\mathfrak{b} \subset W_tI_\mathfrak{b}$. Finally, the isogeny $MI_\mathfrak{b} \subset W_tI_\mathfrak{b}$ is equivalent to $xyW_sI_{\mathfrak{a}'} \subset W_tI_\mathfrak{b}$ constructed in step 2(c)ii by Corollary 3.9.(iii). Hence every minimal isogeny with index dividing D is represented in $\mathcal{E}^{D,1}$, and $\mathcal{E}^{D,1}$ represents all minimal isogenies of degree dividing D by Proposition 3.4.(ii).

We now prove that distinct elements of $\mathcal{E}^{D,1}$ represent inequivalent isogenies. If the source or target vertices of two edges are not the same, the edges represent inequivalent isogenies. Therefore we consider two edges produced in step 2(c)ii with the same source and with target $(t, e_T(\mathfrak{b}))$, where T is the multiplicator ring of t and $\mathfrak{b} \in \mathcal{P}_T$. A priori, we know that the sources of the two edges are of the form $(s_i, e_S(\mathfrak{a}_i\mathfrak{b}))$ for $i = 1, 2$. Since we are assuming that they are equal, we get $s_1 = s_2$ and $\mathfrak{a}_1 = \mathfrak{a}_2$, which we then denote simply by s and $\mathfrak{a}$, respectively. Because the edges are distinct, they come from fractional R-ideals M_1, and M_2 contained in W_t which do not belong to the same orbit under $T^\times$. Write $M_1 = x_1W_sI_\mathfrak{a}$ and $M_2 = x_2W_sI_\mathfrak{a}$ for elements $x_1, x_2 \in K^\times$ so that the edges represent the inclusions $M_1I_\mathfrak{b} \subseteq W_tI_\mathfrak{b}$ and $M_2I_\mathfrak{b} \subseteq W_tI_\mathfrak{b}$. Corollary 3.9.(iii) then implies that these edges represent inequivalent isogenies. □

Algorithm 5.2 (`IsogenyGraphBuilder`)**.**

Input: A q-Weil polynomial h and an integer $D > 1$.

Output: The D-isogeny graph $\mathcal{G}^D$ of the isogeny class $\mathcal{I}_h$.

(1) Run Algorithm 5.1 to compute the vertices $\mathcal{V}$ and minimal edges $\mathcal{E}^{D,1}$ of $\mathcal{G}^D$. Write $\mathcal{E}^{=n}$ for the edges of degree exactly n, $\mathcal{E}^{=n,1}$ for the minimal edges of degree n, and initialize $\mathcal{E}^{=n} = \mathcal{E}^{=n,1}$ for $1 < n \mid D$.
(2) Loop over the divisors $n \neq 1$ of D in increasing order, and for each divisor $d_2 > 1$ of n, loop over pairs $(E_2, E_1) \in \mathcal{E}^{=d_2,1} \times \mathcal{E}^{=n/d_2}$ such that the source of the minimal edge $E_2 \colon (w_2, \mathfrak{a}_2) \to (w_3, \mathfrak{a}_3)$ equals the target of the edge $E_1 \colon (w_1, \mathfrak{a}_1) \to (w_2, \mathfrak{a}_2)$.
   (a) Compute a complete set $\mathcal{U}$ of representatives for the cosets of the quotient $\mathcal{O}_2^\times/(\mathcal{O}_1^\times\mathcal{O}_3^\times \cap \mathcal{O}_2^\times)$, where $\mathcal{O}_i$ is the multiplicator ring of w_i.
   (b) For each $u \in \mathcal{U}$ do:
      (i) Compute the degree-n composition $E\colon (w_1, \mathfrak{a}_1) \to (w_2, \mathfrak{a}_2) \to (w_3, \mathfrak{a}_3)$ labelled by $x_1 u x_2 W_{w_1} I_{\mathfrak{a}_1} \subset W_{w_3} I_{\mathfrak{a}_3}$.
      (ii) If Algorithm 3.11 returns that there is no already computed edge equivalent to E in $\mathcal{E}^{=n}$, add E to $\mathcal{E}^{=n}$.
(3) Construct $\mathcal{G}^D$ from $\mathcal{V}$ and the edges $\mathcal{E}^{=n}$ for $1 < n \mid D$ and return it.

Proof. The labels of the minimal edges in $\mathcal{E}^{D,1}$, and consequently of all of $\mathcal{E}^D$, are chosen so that the ideals representing source and target are equal whenever source and target coincide. In other words, we do not need to consider isomorphism between different representatives when computing the compositions. Let $n > 1$ be a divisor of D. Every edge of degree n can be written as a minimal edge E_2 of degree $d_2|n$ following, if $d_2 < n$, an edge E_1 of degree $n/d_2 < n$. Since we are looping over the divisors n of D in increasing order, all such edges E_1 have already been computed. In step 2b, we loop over the set $\mathcal{U}$ to consider all the contributions coming from the automorphisms of the source of E_2 given by Proposition 3.12, and therefore the set $\mathcal{E}^{=n}$ contains representatives of all equivalence classes of the edges of degree n. The use of Algorithm 3.11 and the fact that the edges produced for each $u \in \mathcal{U}$ are all pairwise not equivalent by Corollary 3.9.(iv) guarantee that $\mathcal{E}^{=n}$ contains at most one representative for each equivalence class. □

6. The Picard group action

Algorithms 5.1 and 5.2 will struggle when $\mathrm{Pic}(R) = \mathrm{Pic}(\mathbb{Z}[\pi, \overline{\pi}])$ is large. In this situation, we can try to take advantage of additional structure to both improve the runtime and reduce the size of the output. Indeed, the group $\mathrm{Pic}(R)$ acts on both the vertices and edges of $\mathcal{G}$ via ideal multiplication. While this action is not free in general, we can use it to define free actions of specific quotient groups on subsets of the edges in $\mathcal{G}$.

Definition 6.1. Suppose that s and t are weak equivalence classes of R with multiplicator rings S and T, $e_S \colon \mathrm{Pic}(R) \to \mathrm{Pic}(S)$ and $e_T \colon \mathrm{Pic}(R) \to \mathrm{Pic}(T)$.

(1) Write $\mathrm{dom}\colon \mathcal{E} \to \mathcal{V}$ for the map that sends each isogeny to its domain, and $\mathrm{cod}\colon \mathcal{E} \to \mathcal{V}$ for the map that sends each isogeny to its codomain.
(2) Set $\mathcal{E}_{s,t} = \{\varphi \in \mathcal{E} : \mathrm{dom}(\varphi) \in s, \mathrm{cod}(\varphi) \in t\}$, and write $\mathcal{E}_{s,t}^D$ for the set of elements of $\mathcal{E}_{s,t}$ of degree dividing D and $\mathcal{E}_{s,t}^{D,r}$ for the set of elements of $\mathcal{E}_{s,t}^D$ of length r.
(3) Finally, define the quotient group $G_{S,T} = \mathrm{Pic}(R)/(\ker(e_S) \cap \ker(e_T))$.

We now extend [Mar20, Theorem 4.6] from vertices to edges:

Proposition 6.2. *Let A and B belong to an isogeny class with isogeny graph $\mathcal{G}$ and Frobenius order R and $\varphi\colon A \to B$ be an isogeny, and choose fractional $\mathbb{Z}[\pi, \overline{\pi}]$-ideals I and J and isomorphisms identifying $I = \mathcal{F}(A)$ and $J = \mathcal{F}(B)$, as well as $x \in (J : I) \cap K^\times$ and an identification $x = \mathcal{F}(\varphi)$ Furthermore, let M be an invertible fractional R-ideal with class $[M] \in \operatorname{Pic}(R)$.*

1. *Ideal multiplication induces an action of $\operatorname{Pic}(R)$ on $\mathcal{G}$: we denote by $[M] \cdot \varphi$ the isogeny represented by the inclusion $xMI \subseteq MJ$.*
2. *The action of $\operatorname{Pic}(R)$ on $\mathcal{G}$ preserves degree and length, and thus induces actions on $\mathcal{G}^D$ and $\mathcal{G}^{D,r}$.*
3. *This action induces an action of $G_{S,T}$ on $\mathcal{E}_{s,t}$, $\mathcal{E}_{s,t}^D$ and $\mathcal{E}_{s,t}^{D,r}$.*

Proof. The first two parts follow from Proposition 3.4 and Lemma 3.13.

To see that the action on $\mathcal{E}_{s,t}$ factors through $G_{S,T}$, we show that $\ker(e_S) \cap \ker(e_T)$ acts trivially. Let $[H] \in \ker(e_S) \cap \ker(e_T)$, $I \in s$, $J \in t$, and $xI \subseteq J$ represent an edge in $\mathcal{E}_{s,t}$. Acting by $[H]$ yields $xHI \subseteq HJ$. Since $HS = y_1 S$ and $HT = y_2 T$ for $y_1, y_2 \in K$, the two inclusions represent equivalent isogenies by Proposition 3.8. □

Lemma 6.3. *Let R be the Frobenius order of an isogeny class, and s and t be weak equivalence classes of fractional R-ideals with multiplicator rings S and T.*

1. *The group $G_{S,T}$ acts freely on $\mathcal{E}_{s,t}$.*
2. *For each orbit O of this action, we have $\operatorname{dom}(O) = s$ and $\operatorname{cod}(O) = t$.*
3. *If O is an orbit and $\mathfrak{j} \in t$, the set $\{\varphi \in O : \operatorname{cod}(\varphi) = \mathfrak{j}\}$ is a torsor for $\ker(e_T)/(\ker(e_S) \cap \ker(e_T))$. Similarly, if $\mathfrak{i} \in s$, the set $\{\varphi \in O : \operatorname{dom}(\varphi) = \mathfrak{i}\}$ is a torsor for $\ker(e_S)/(\ker(e_S) \cap \ker(e_T))$.*

Proof. We may assume that $\mathcal{E}_{s,t}$ is nonempty since otherwise the action is vacuously free and there are no orbits. Suppose that $\mathfrak{a} \in \operatorname{Pic}(R)$ fixes some $\varphi \in \mathcal{E}_{s,t}$. Then it certainly fixes $\operatorname{dom}(\varphi)$, and thus $e_S(\mathfrak{a}) = 1$ by Proposition 2.1. Similarly, it fixes $\operatorname{cod}(\varphi)$ so $e_T(\mathfrak{a}) = 1$. Thus the action of $G_{S,T}$ is free.

Since e_S is surjective, $\operatorname{Pic}(R)$ acts transitively on s and thus $\operatorname{dom}(O) = s$ for any orbit O of the action of $G_{S,T}$ on $\mathcal{E}_{s,t}$. Similarly, e_T is surjective so $\operatorname{cod}(O) = t$.

Since $G_{S,T}$ acts on codomains through its projection onto $\operatorname{Pic}(T)$, the subgroup $\ker(e_T)/(\ker(e_S) \cap \ker(e_T))$ is precisely the set of group elements fixing the codomain. It thus acts on the set $\{\varphi \in O : \operatorname{cod}(\varphi) = \mathfrak{j}\}$, which is a torsor for the subgroup since $G_{S,T}$ acts freely. The statement about $\{\varphi \in O : \operatorname{dom}(\varphi) = \mathfrak{i}\}$ follows similarly. □

In light of Lemma 6.3 , we modify Algorithms 5.1 and 5.2 to return sets of representatives $\mathcal{R}_{s,t}$ for the orbits of $G_{S,T}$ on $\mathcal{E}_{s,t}$. This has the benefit of both dramatically shrinking the output size and reducing the amount of compositions computed when $\operatorname{Pic}(R)$ is large. However, composing orbit representatives requires additional work. We consider the subsets $\mathcal{R}_{s,t}^{=n}$ and $\mathcal{R}_{s,t}^{=n,1}$ consisting of edges with degree n and minimal edges of degree n (respectively).

In this section, s, t, and u are weak equivalence classes of fractional R-ideals, with corresponding multiplicator rings S, T, and U. Furthermore, for isogenies φ and φ', we write $\varphi' \sim \varphi$ if $\varphi' \approx \mathfrak{a} \cdot \varphi$ for some $\mathfrak{a} \in \operatorname{Pic}(R)$. We define a multivalued composition map $\underline{\circ}\colon \mathcal{R}_{t,u} \times \mathcal{R}_{s,t} \to \mathcal{R}_{s,u}$ by setting

$$\psi \underline{\circ} \varphi = \{\theta \in \mathcal{R}_{s,u} : \exists \varphi', \psi', \theta' \text{ with } \varphi' \sim \varphi, \psi' \sim \psi, \theta' \sim \theta, \theta' = \psi' \circ \varphi'\}.$$

Proposition 6.4. *Suppose that* $\mathfrak{a}_0 \in \mathrm{Pic}(R)$ *satisfies* $\mathrm{cod}(\mathfrak{a}_0 \cdot \varphi) = \mathrm{dom}(\psi)$. *Let* X *be a set of coset representatives for* $\ker(e_T)/(\ker(e_T) \cap (\ker(e_S) \cdot \ker(e_U)))$ *and* Y *be a set of coset representatives for* $T^\times/(T^\times \cap (S^\times U^\times))$. *Define*

$$\psi \underline{\bullet} \varphi = \{\psi \circ \rho \circ (\mathfrak{a}_1 \mathfrak{a}_0 \cdot \varphi) : \mathfrak{a}_1 \in X, \mathcal{F}(\rho) \in Y\} \subseteq \psi \underline{\circ} \varphi.$$

(1) The $G_{S,U}$*-orbits represented by* $\psi \underline{\circ} \varphi$ *and by* $\psi \underline{\bullet} \varphi$ *are the same.*
(2) If $\chi = \psi \circ \rho \circ (\mathfrak{a}_1 \mathfrak{a}_0 \cdot \varphi)$ *and* $\chi' = \psi \circ \rho' \circ (\mathfrak{a}_1' \mathfrak{a}_0 \cdot \varphi)$ *are two elements of* $\psi \underline{\bullet} \varphi$ *then* $\chi \sim \chi'$ *if and only if* $\chi \approx \chi'$.

Proof. By the definition of $\sim$, the orbits represented by $\psi \underline{\bullet} \varphi$ are contained within those represented by $\psi \underline{\circ} \varphi$, so it suffices to check the opposite containment. Suppose that $\varphi' \sim \varphi$ and $\psi' \sim \psi$ can be composed as $\theta' = \psi' \circ \varphi'$. Then $\varphi' = \beta \circ (\mathfrak{b}_1 \cdot \varphi) \circ \alpha$ with $\mathcal{F}(\alpha) \in S^\times, \mathcal{F}(\beta) \in T^\times, \mathfrak{b}_1 \in \mathrm{Pic}(R)$ and $\psi' = \delta \circ (\mathfrak{b}_2 \cdot \psi) \circ \gamma$ with $\mathcal{F}(\gamma) \in T^\times, \mathcal{F}(\delta) \in U^\times, \mathfrak{b}_2 \in \mathrm{Pic}(R)$. Since we are working with θ' up to $G_{S,U}$-equivalence, we may omit α and δ, set $\rho = \gamma \circ \beta$, and check that each composition $(\mathfrak{b}_2 \cdot \psi) \circ \rho \circ (\mathfrak{b}_1 \cdot \varphi)$ is in the same orbit as one of the form $\psi \circ \rho \circ (\mathfrak{a}_1 \mathfrak{a}_0 \cdot \varphi)$.

Let $\mathfrak{a}_2 \in \ker(e_T) \cap \ker(e_U)$. Then $\mathfrak{b}_2 \mathfrak{a}_2 \cdot (\psi \circ \rho \circ (\mathfrak{a}_1 \mathfrak{a}_0 \cdot \varphi)) \approx (\mathfrak{b}_2 \mathfrak{a}_2 \cdot \psi) \circ \rho \circ (\mathfrak{b}_2 \mathfrak{a}_2 \mathfrak{a}_1 \mathfrak{a}_0 \cdot \varphi) = (\mathfrak{b}_2 \cdot \psi) \circ \rho \circ (\mathfrak{b}_2 \mathfrak{a}_2 \mathfrak{a}_1 \mathfrak{a}_0 \cdot \varphi)$, so it suffices to check that $\mathfrak{b}_2^{-1} \mathfrak{b}_1 \cdot \varphi \approx \mathfrak{a}_2 \mathfrak{a}_1 \mathfrak{a}_0 \cdot \varphi$ for some $\mathfrak{a}_2 \in \ker(e_T) \cap \ker(e_U)$ and $\mathfrak{a}_1 \in X$. Since the composition $(\mathfrak{b}_2 \cdot \psi) \circ \rho \circ (\mathfrak{b}_1 \cdot \varphi)$ is well defined, we must have $\mathrm{cod}(\mathfrak{b}_1 \cdot \varphi) = \mathrm{dom}(\mathfrak{b}_2 \cdot \psi)$ and thus $\mathrm{cod}(\mathfrak{b}_2^{-1} \mathfrak{b}_1 \cdot \varphi) = \mathrm{dom}(\psi) = \mathrm{cod}(\mathfrak{a}_0 \cdot \varphi)$. But as $\mathfrak{a}_2$ and $\mathfrak{a}_1$ vary, $\mathfrak{a}_2 \mathfrak{a}_1 \mathfrak{a}_0 \cdot \varphi$ ranges over all equivalence classes of isogenies with the same codomain as $\mathfrak{a}_0 \cdot \varphi$. This completes the proof of part 1

Now suppose that $\chi \sim \chi'$. To prove that $\chi \approx \chi'$, it suffices to show that $\mathrm{dom}(\chi) = \mathrm{dom}(\chi')$ and $\mathrm{cod}(\chi) = \mathrm{cod}(\chi')$ since any element of $\mathrm{Pic}(R)$ that acts nontrivially must change either the domain or codomain. All elements of $\psi \underline{\bullet} \varphi$ have the same codomain, so suppose that $\mathfrak{a}_1, \mathfrak{a}_1' \in X$. Since $\chi \sim \chi'$, by Lemma 6.3 the domains of $\mathfrak{a}_1 \mathfrak{a}_0 \cdot \varphi$ and $\mathfrak{a}_1' \mathfrak{a}_0 \cdot \varphi$ differ by an element of $\ker(e_U)$. By the definition of X, both lie in $\ker(e_T)$ as well, and thus their difference is in $\ker(e_U) \cap \ker(e_T) \subseteq (\ker(e_T) \cap (\ker(e_S) \cdot \ker(e_U)))$. Since X is a set of coset representatives, we have $\mathfrak{a}_1 = \mathfrak{a}_1'$, and thus $\mathrm{dom}(\chi) = \mathrm{dom}(\chi')$. $\square$

Next, we augment Algorithm 3.11 to give a test for when two isogenies are in the same orbit, and prove that our algorithm is correct.

Algorithm 6.5 (`AreIsogeniesGSTEquivalent`).

Input: For R the Frobenius order of an isogeny class $\mathcal{I}_h$, inclusions $x_1 I_1 \subset J_1$ and $x_2 I_2 \subset J_2$ of R-ideals representing two isogenies φ and ψ with weakly equivalent domains and weakly equivalent codomains.

Output: Whether the two isogenies are in the same $\mathrm{Pic}(R)$-orbit.

(1) Represent the ideal classes $[I_1] = (s, \mathfrak{a}_1'), [I_2] = (s, \mathfrak{a}_2'), [J_1] = (t, \mathfrak{b}_1'), [J_2] = (t, \mathfrak{b}_2')$, let S be the multiplicator ring of the domains and T the multiplicator ring of the codomains and choose lifts $\mathfrak{a}_i, \mathfrak{b}_i \in \mathrm{Pic}(R)$ of $\mathfrak{a}_i'$ and $\mathfrak{b}_i'$.
(2) Express $\mathfrak{a}_2 \mathfrak{b}_1 \mathfrak{a}_1^{-1} \mathfrak{b}_2^{-1} = \mathfrak{k}_S \mathfrak{k}_T$ for some $\mathfrak{k}_S \in \ker(e_S)$ and $\mathfrak{k}_T \in \ker(e_T)$. If this is not possible, return *false*.
(3) Compare $(\mathfrak{b}_2 \mathfrak{b}_1^{-1} \mathfrak{k}_T) \cdot \varphi$ to ψ using Algorithm 3.11.

Proof. Step 2 can be done by finding the preimage of $\mathfrak{a}_2 \mathfrak{b}_1 \mathfrak{a}_1^{-1} \mathfrak{b}_2^{-1}$ under the natural homomorphism $\ker(e_S) \oplus \ker(e_T) \to \mathrm{Pic}(R)$, and yields an element $\mathfrak{b}_2 \mathfrak{b}_1^{-1} \mathfrak{k}_T = \mathfrak{a}_2 \mathfrak{a}_1^{-1} \mathfrak{k}_S^{-1}$ whose image under e_S is $\mathfrak{a}_2' \mathfrak{a}_1'^{-1}$ (which maps the domain of φ to the domain of ψ) and whose image under e_T is $\mathfrak{b}'_2\mathfrak{b}'^{-1}_1$ (which maps the codomain of φ to the codomain of ψ). If no such $\mathfrak{k}_S$ and $\mathfrak{k}_T$ exist, φ and ψ cannot be in the same orbit since it is not possible to get their domains and codomains to match. If they do exist, then $\varphi \sim \psi$ if and only if $(\mathfrak{b}_2\mathfrak{b}_1^{-1}\mathfrak{k}_T) \cdot \varphi \approx \psi$. □

We now adapt Algorithm 5.1 to compute orbit representatives for the set of minimal isogenies. In contrast to Algorithm 5.1, we do not need to loop over $\mathrm{Pic}(T)$.

Algorithm 6.6 (`MinimalIsogenyOrbitBuilder`)**.**
Input: A q-Weil polynomial h and an integer $D > 1$.
Output: For weak equivalence classes s, t and $1 < n \mid D$, the finite set $\mathcal{R}^{=n,1}_{s,t}$.

(1) For each weak equivalence class t and T the multiplicator ring of t, do
  (a) Compute the fractional R-ideals M contained in W_t such that the inclusion $M \subset W_t$ is maximal and the index $[W_t : M]$ divides D.
  (b) Among the M in the same weak equivalence class s, choose one representative for each $\ker(e_T)/(\ker(e_S) \cap \ker(e_T))$-orbit. Determine the action of $T^\times$ on this quotient and pick one representative from each of these $T^\times$ orbits.
  (c) For each representative M, compute the vertex $(s, e_S(\mathfrak{a})) \in \mathcal{V}$ that represents it with $\mathfrak{a} \in \mathcal{P}_S$, together with $x \in K^\times$ such that $xW_sI_\mathfrak{a} = M$. Yield the minimal edge $(s, e_S(\mathfrak{a})) \to (t, 1)$ with label $xW_sI_\mathfrak{a} \subset W_t$.

Proof. By Lemma 6.3 every orbit contains a representative with codomain W_t, and the subset of such isogenies is a torsor for $\ker(e_T)/(\ker(e_S) \cap \ker(e_T))$. Correctness now follows from the correctness of Algorithm 5.1. □

We use Algorithm 6.6 to compute orbit representatives for isogenies of degree n.

Algorithm 6.7 (`IsogenyOrbitBuilder`)**.**
Input: A q-Weil polynomial h and an integer $D > 1$.
Output: For weak equivalence classes s, t and $1 < n \mid D$, the finite set $\mathcal{R}^{=n}_{s,t}$.

(1) Run Algorithm 6.6 to compute $\mathcal{R}^{=n,1}_{s,t}$ for $1 < n \mid D$. Initialize $\mathcal{R}^{=n}_{s,t} = \mathcal{R}^{=n,1}_{s,t}$.
(2) Loop over the divisors n of D in increasing order, and for each divisor $1 < d_2 < n$ of n, loop over triples of weak equivalence classes s, t, u and $(E_2, E_1) \in \mathcal{R}^{=d_2,1}_{t,u} \times \mathcal{R}^{=n/d_2}_{s,t}$:
  (a) For each E in the composition $E_2 \underline{\bullet} E_1$, use Algorithm 6.5 to determine if its orbit has already been added to $\mathcal{R}^{=n}_{s,u}$, and add it if not.
(3) Return the $\mathcal{R}^{=n}_{s,t}$.

Proof. The correctness of Algorithm 6.5 guarantees that no two returned isogenies lie in the same orbit, and Proposition 6.4 implies that any composition of minimal isogenies will be in the same orbit as one constructed in $E_2 \underline{\bullet} E_1$. Finally, every isogeny can be expressed as a composition of minimal isogenies as constructed in Algorithm 6.6 by Proposition 3.4 . □

7. Polarizations

In this section, we compute the polarizations of elements belonging to a given isogeny class. Throughout, for an isogeny class $\mathcal{I}_h$, let g be the dimension of the abelian varieties it contains; then the étale algebra $K = \mathbb{Q}(\pi)$ satisfies $[K : \mathbb{Q}] = 2g$. Recall that K is equipped with an involution $x \mapsto \overline{x}$. We say that an element $x \in K$ is *totally imaginary* if $x = -\overline{x}$ and *totally real* if $x = \overline{x}$. A totally real element $x \in K^\times$ is called *totally positive* if $\phi(x) > 0$ for every homomorphism $\phi\colon K \to \mathbb{C}$. Let Φ be a CM-type of K, that is, a choice of g homomorphisms $K \to \mathbb{C}$, one per conjugate pair. We say that $x \in K$ is *Φ-positive* if $\Im(\phi(x)) > 0$ for every $\phi \in \Phi$. For each abelian variety A we denote by $A^\vee$ its dual. Given a weak equivalence class s, we denote by $s^\vee$ the weak equivalence class containing the dual of each element of s (well defined by Lemma 2.3 and Proposition 7.1).

Recall from Section 2 that we have fixed an isomorphism $\varepsilon\colon \overline{\mathbb{Q}}_p \to \mathbb{C}$. Given a homomorphism $\phi\colon K \to \mathbb{C}$, post-composing by ε^{-1} gives a homomorphism $\phi_\varepsilon\colon K \to \overline{\mathbb{Q}}_p$ which induces a p-adic place v_{ϕ_ϵ} on K by taking the usual p-adic valuation of the image of an element under ϕ_ϵ. We say that a CM-type Φ **satisfies the Shimura–Taniyama formula** for a Frobenius order $\mathbb{Z}[\pi, \overline{\pi}]$ ([CCO14, p. 2.1.4.1]) if for each p-adic place v induced on K by Φ in this manner, we have

$$\frac{\mathrm{ord}_v(\pi)}{\mathrm{ord}_v(q)} = \frac{\#\{\phi \in \Phi : \phi \text{ induces } v \text{ on } K\}}{[K_v : \mathbb{Q}_p]}. \tag{7.1}$$

Such a CM-type always exists for ordinary isogeny classes of abelian varieties defined over $\mathbb{F}_q$ (see [How95, Notation 4.6], for example, for how to construct a CM-type satisfying the Shimura–Taniyama formula for a given Frobenius order $\mathbb{Z}[\pi, \overline{\pi}]$ in the ordinary case), and in particular for every polynomial $h(x)$ considered in this article. In what follows we suppose that Φ satisfies the Shimura–Taniyama formula; this condition ensures that Φ is a CM-type for the complex abelian variety $\tilde{A} \otimes_\varepsilon \mathbb{C}$, where $\tilde{A}$ is the canonical lift of A.

Proposition 7.1 ([Mar21, Theorem 5.4])**.** *Let $A, A_1, A_2 \in \mathcal{I}_h$, and identify $I = \mathcal{F}(A)$, $I_1 = \mathcal{F}(A_1)$ and $I_2 = \mathcal{F}(A_2)$. Further, let $\varphi\colon A \to A^\vee$ be an isogeny and (A_1, ψ_1) and (A_2, ψ_2) be polarized abelian varieties, and choose identifications $\mu = \mathcal{F}(\varphi)$, $\lambda_1 = \mathcal{F}(\psi_1)$ and $\lambda_2 = \mathcal{F}(\psi_2)$. Then the following statements hold:*

- *(i) We can make the identification $\overline{I}^\dagger = \mathcal{F}(A^\vee)$.*
- *(ii) φ is a polarization if and only if μ is totally imaginary and Φ-positive.*
- *(iii) (A_1, ψ_1) and (A_2, ψ_2) are isomorphic if and only if there is an element $y \in K^\times$ satisfying $yI_1 = I_2$ and $\lambda_1 = \overline{y}\lambda_2 y$.*

We break the search for polarized abelian varieties up into two steps. First, we give two different algorithms for producing isogenies of the form $A \to A^\vee$, one based on Algorithm 5.2 and one on Algorithm 6.7. Second, we give an algorithm that produces the list of all polarized abelian varieties with polarization of degree dividing D within an isogeny class given the set of such $A \to A^\vee$ as input.

Algorithm 7.2 (`DualIsogenies_FromIter`)**.**
Input: A q-Weil polynomial h and an integer $D > 1$.
Output: Isogenies $\varphi\colon A \to A^\vee$ in $\mathcal{G}^D$, one per equivalence class.

1. Use Algorithm 5.2 to compute the isogeny graph $\mathcal{G}^D$.
2. For each vertex V do:
   - (a) Identify the vertex $V^\vee$ corresponding to the ideal class of $\overline{I_V}^\dagger$.
   - (b) Compute $\iota \in K^\times$ such that $\iota I_{V^\vee} = \overline{I_V}^\dagger$.

(c) For each edge in $\mathcal{G}^D$ represented by $x_0 I_V \subseteq I_{V^\vee}$, yield the isogeny represented by $\iota x_0 I_V \subseteq \overline{I_V}^\dagger$.

Proof. The correctness follows from Proposition 7.1.(i) and the definition of $\mathcal{G}^D$. $\square$

Remark 7.3. In step 2a, one needs to solve a discrete logarithm problem in $\mathrm{ICM}(R)$. This expensive step can be avoided by tracking the action of duality when constructing the set of vertices of $\mathcal{G}$ as orbits of Picard groups; see Proposition 2.1. By Lemma 2.3, this action is encoded by the formula $\overline{(IL)}^\dagger = \overline{I}^\dagger \overline{L}^{-1}$.

Alternatively, we can iterate over representatives from Algorithm 6.7, which saves time when $\mathrm{Pic}(\mathbb{Z}[\pi, \overline{\pi}])$ is large.

Algorithm 7.4 (`DualIsogenies_FromOrbit`).
Input: A q-Weil polynomial h and an integer $D > 1$.
Output: Isogenies $\varphi\colon A \to A^\vee$ in $\mathcal{G}^D$, one per equivalence class.

(1) Use Algorithm 6.7 to compute $\mathcal{R}^n_{s,s^\vee}$ for $1 < n \mid D$.
(2) For each weak equivalence class s, compute $J_s = (\overline{W}^\dagger_{s^\vee} : W_s)$; set $\mathfrak{j}_s = [J_s]$.
(3) For each endomorphism ring S, compute the endomorphism β of the finite abelian group $G_{S,\overline{S}}$ defined by $\beta(\mathfrak{b}) = \mathfrak{b}\overline{\mathfrak{b}}$.
(4) For each weak equivalence class s and each $\varphi \in \mathcal{R}^D_{s,s^\vee}$ do:
  (a) Let S be the multiplicator ring of s, $\mathfrak{w}_s\mathfrak{a}$ be the domain of φ and $\mathfrak{w}_{s^\vee}$ be the codomain. Choose an element $\mathfrak{a}' \in \mathrm{image}(\beta)$ mapping to $\mathfrak{a}^{-1}\mathfrak{j}_s$ in $\mathrm{Pic}(S)$ and $\overline{\mathfrak{a}}^{-1}\bar{\mathfrak{j}}_s$ in $\mathrm{Pic}(\overline{S})$; if no $\mathfrak{a}'$ exists then continue to the next φ. Otherwise, choose $\mathfrak{b}_0 \in G_{S,\overline{S}}$ with $\beta(\mathfrak{b}_0) = \mathfrak{a}'$.
  (b) For each $\mathfrak{c} \in \ker(\beta)$, let $\mathfrak{b}_0\mathfrak{c} \cdot \varphi$ be represented by $x_0 I \subseteq J$ and:
    (i) Compute $\iota \in K^\times$ such that $\iota J = \overline{I}^\dagger$, and yield $\iota x_0 I \subseteq \overline{I}^\dagger$.

Proof. The $G_{S,\overline{S}}$-orbit of φ consists of isogenies with domain $\mathfrak{w}_s\mathfrak{a}\mathfrak{b}$ and codomain $\mathfrak{w}_{s^\vee}\mathfrak{b}$ for $\mathfrak{b} \in G_{S,\overline{S}}$. By Proposition 7.1.(i) and Lemma 2.3, we seek $\mathfrak{b}$ so that

$$\begin{aligned}
\mathfrak{w}_s\mathfrak{a}\mathfrak{b} &= \overline{(\mathfrak{w}_{s^\vee}\mathfrak{b})}^\dagger = \overline{\mathfrak{w}_{s^\vee}}^\dagger\overline{\mathfrak{b}}^{-1} = \mathfrak{w}_s\mathfrak{j}_s\overline{\mathfrak{b}}^{-1}\\
\mathfrak{w}_{s^\vee}\mathfrak{b} &= \overline{(\mathfrak{w}_s\mathfrak{a}\mathfrak{b})}^\dagger = \overline{\mathfrak{w}_s}^\dagger\overline{\mathfrak{a}}^{-1}\overline{\mathfrak{b}}^{-1} = \mathfrak{w}_{s^\vee}\bar{\mathfrak{j}}_s\overline{\mathfrak{a}}^{-1}\overline{\mathfrak{b}}^{-1}
\end{aligned}$$

which will occur when $\mathfrak{b}\overline{\mathfrak{b}} = \mathfrak{a}'$ in $\mathrm{Pic}(S)$ (by the first line) and in $\mathrm{Pic}(\overline{S})$ (by the second line). The elements $\mathfrak{b}_0\mathfrak{c}$ are precisely the solutions to this equation. So far we have worked up to isomorphism; to get an isogeny of the form $\varphi\colon A \to A^\vee$ we need to compose with ι so that the codomain is precisely the dual of the domain, not merely isomorphic to it. $\square$

Algorithm 7.5 (`NonPrincipalPolarizationsOfDegreeDividing`).
Input: A q-Weil polynomial h, an integer $D > 1$, and a CM-type Φ of $K = \mathbb{Q}[x]/(h(x))$ satisfying the Shimura–Taniyama formula.
Output: Pairs (I, μ) representing the isomorphism classes of polarized abelian varieties in $\mathcal{I}_h$ with polarizations of degree > 1 dividing D.

(1) Use either Algorithm 7.2 or 7.4 to compute a list $\mathcal{L}$ of isogenies $\varphi\colon A \to A^\vee$ of degree dividing D.
(2) For each overorder S of R do:

Algorithmic Number Theory Symposium XVII, Groningen, July 6-10, 2026

(a) Compute a complete set $\mathcal{S}$ of representatives for the cosets of the quotient $S^\times/S^\times_+$, where $S^\times_+$ is the subgroup of $S^\times$ consisting of totally real and totally positive units.

(b) Compute representatives $v_1, \dots, v_n$ in $S^\times$ of $\dfrac{S^\times_+}{S^\times_+ \cap \langle w\overline{w} : w \in S^\times\rangle}$.

(3) For each isogeny $xI_A \subseteq \overline{I_A}^\dagger$ in $\mathcal{L}$ do:

(a) Set $S = (I_A : I_A)$ and assign $\mathcal{S}$ and $v_1, \dots, v_n$ as above.

(b) If there exists $v \in \mathcal{S}$ with $\mu = xv$ totally imaginary and Φ-positive then yield the non-isomorphic polarizations $(I_A, \mu v_1), \dots, (I_A, \mu v_n)$.

Proof. By Proposition 7.1.(ii), each element μv_i represents a polarization of I_A. Each μv_i is an isogeny from I_A to $\overline{I}^\dagger_A$ of degree dividing D, since it is a composition of automorphisms v and v_i of I_A and an isogeny x of degree dividing D.

We now prove that the output consists of non-isomorphic polarized abelian varieties. Pick $(I_{A_1}, \mu_1), (I_{A_2}, \mu_2)$ in $\mathcal{L}$. Since the ideal I_A representing the vertex of A is deterministically chosen, we can assume that $A_1 = A_2$. Then Proposition 7.1.(iii) says that (I_{A_1}, μ_1) and (I_{A_1}, μ_2) are isomorphic if and only if there is a unit $u \in S^\times$ such that $\mu_1 = \overline{u}\mu_2 u$. A necessary condition is that μ_1 and μ_2 come from the same edge x_0 by Corollary 3.9.(iv) (composed with an isomorphism ι as in Algorithm 7.2 or 7.4). There exists at most one element v of $\mathcal{S}$ such that the element $\mu = vx$ is totally imaginary and Φ-positive. By writing $\mu_1 = \mu v_i$ and $\mu_2 = \mu v_j$, we see that μ_1 and μ_2 give rise to isomorphic polarized abelian varieties if and only if $\mu_1 = \mu_2$.

It remains to show that any (I, λ) with $\deg(\lambda) \mid D$ is isomorphic to some $(I_A, \mu v_i)$ in the output. Proposition 7.1.(iii) states that this happens precisely if there exists $x \in K^\times$ such that $xI_A = I$ and $\mu v_i = \overline{x}\lambda x$. Now, since λ is an isogeny of degree dividing D, there exists a unique edge $x_0 I_A \subseteq I_{A^\vee}$ together with elements $y, z \in K^\times$ such that $yI_A = I$, $z\overline{I}^\dagger = I_{A^\vee}$ and $x_0 = z\lambda y$ by Proposition 3.8.(ii). Take $\iota \in K^\times$ satisfying $\iota I_{A^\vee} = \overline{I_A}^\dagger$. Let $\overline{u} = \overline{y}/z\iota$. Since $\overline{y}\overline{I}^\dagger = z\iota\overline{I}^\dagger$, then $u \in S^\times$. We summarize the situation in the following diagram:

$$\begin{tikzcd}
I \arrow[d, "\lambda"] & I_A \arrow[l, "y"'] \arrow[d, "x_0"] & \\
\overline{I}^\dagger \arrow[r, "z"] \arrow[dr, "\overline{y}"'] & I_{A^\vee} \arrow[r, "\iota"] & \overline{I_A}^\dagger \arrow[dl, "\overline{u}"] \\
& \overline{I_A}^\dagger &
\end{tikzcd}$$

We have $\overline{u}^{-1}\overline{y}\lambda y = \iota x_0$. By multiplying by u^{-1}, we see that $\iota x_0 u^{-1}$ is totally imaginary and Φ-positive, since λ is so. Let v be the representative in $\mathcal{S}$ of u^{-1}, so that $vu \in S^\times_+$. Let v_i be the representative of $(vu)^{-1}$ in $S^\times_+/(S^\times \cap \langle w\overline{w} : w \in S^\times\rangle)$. Hence there exists $w \in S^\times$ such that $vuv_i = w\overline{w}$. By setting $x = wu^{-1}y$, we get $\overline{x}\lambda x = \mu v_i$, that is, an isomorphism between $(I_A, \mu v_i)$ and (I, λ). □

8. Implementation and timings

In Table 2, we give some timings for the Magma [Magma] implementation [CDMRV26] of Algorithms 5.2, 6.7, and 7.5. There are many factors influence the runtime, and we did not explore which were most impactful or provide an asymptotic complexity analysis.

(a) `IsogenyGraphBuilder` (5.2)

isogeny class	g	q	$\lvert\mathrm{Pic}(R)\rvert$	D=4	D=9	D=12	D=36	D=100
1.101.n	1	101	2	< 0.1	< 0.1	< 0.1	< 0.1	< 0.1
3.5.a_ab_l	3	5	5	< 0.1	< 0.1	< 0.1	< 0.1	0.3
4.3.c_ab_af_ai	4	3	6	0.9	1.1	0.9	1.6	4.0
2.101.ax_mo	2	101	30	0.2	0.1	0.2	0.3	0.2
2.101.ak_bk	2	101	100	0.4	< 0.1	0.4	0.4	0.7
2.101.k_dy	2	101	300	21.9	0.3	24.3	21.4	215
4.9.ag_f_bh_aes*	4	9	576	236	401	287	735	1344
3.16.ac_c_abb	3	16	1000	1764	0.1	1696	1700	1937

(b) `IsogenyOrbitBuilder` (6.7)

isogeny class	g	q	$\lvert\mathrm{Pic}(R)\rvert$	D=4	D=9	D=12	D=36	D=100
1.101.n	1	101	2	< 0.1	< 0.1	< 0.1	< 0.1	< 0.1
3.5.a_ab_l	3	5	5	< 0.1	< 0.1	< 0.1	< 0.1	0.3
4.3.c_ab_af_ai	4	3	6	1.4	1.1	1.5	8.3	108
2.101.ax_mo	2	101	30	< 0.1	< 0.1	< 0.1	0.1	< 0.1
2.101.ak_bk	2	101	100	< 0.1	< 0.1	< 0.1	< 0.1	0.1
2.101.k_dy	2	101	300	1.4	0.3	1.4	1.5	111
4.9.ag_f_bh_aes*	4	9	576	32.0	14.3	34.0	235	2361
3.16.ac_c_abb	3	16	1000	7.3	0.1	7.3	7.3	22.4

(c) Polarization filter overhead, i.e. (7.5) − (5.2)

isogeny class	g	q	$\lvert\mathrm{Pic}(R)\rvert$	D=4	D=9	D=12	D=36	D=100
1.101.n	1	101	2	< 0.1	< 0.1	< 0.1	< 0.1	< 0.1
3.5.a_ab_l	3	5	5	0.1	< 0.1	0.1	0.1	0.2
4.3.c_ab_af_ai	4	3	6	0.6	0.6	0.6	0.5	0.5
2.101.ax_mo	2	101	30	0.2	0.2	0.2	0.2	0.2
2.101.ak_bk	2	101	100	0.6	0.6	0.6	0.6	0.7
2.101.k_dy	2	101	300	54.4	31.6	41.1	32.3	157
4.9.ag_f_bh_aes*	4	9	576	613	288	560	442	1377
3.16.ac_c_abb	3	16	1000	554	560	559	552	607

TABLE 2. Wall-clock seconds per cell, single-threaded on an Intel i9-13900KS (Ubuntu 24.04 LTS, 192 GB RAM), Magma 2.29-7. < 0.1 is below the noise floor. Rows ordered by $\lvert\mathrm{Pic}(R)\rvert$; * marks the base change to $\mathbb{F}_9$ of 4.3.c_ab_af_ai.

Acknowledgements. We thank the referees for their extensive comments which helped improve the exposition. Costa was supported by Simons Foundation grant SFI-MPS-Infrastructure-00008651, Roe by SFI-MPS-SSRFA-00005427, and both by 550033. Dupuy was supported by National Science Foundation grant DMS-2401570. Dupuy and Vincent are grateful for the hospitality of the GAATI laboratory at the Université de Polynésie française, where they completed this work. Marseglia was supported by NWO grant VI.Veni.202.107, and by Marie Skłodowska-Curie Actions - Postdoctoral Fellowships 2023 (project 101149209 - AbVarFq). Vincent was supported by a Simons Foundation Travel Support for Mathematicians grant.

LLMs. After referee feedback, some revisions to the Github repository and the timing tables were aided by Claude Sonnet 4.6, Opus 4.7, GPT 5.5 and Gemini 3.1 Pro Review. However, the algorithms and arguments are human generated.

References

[AMS25] Sarah Arpin, Stefano Marseglia, and Caleb Springer. "Isogeny graphs of abelian varieties and singular ideals in orders". Available at `https://arxiv.org/abs/2508.03570`. 2025 (↑ 1).

[Bas63] Hyman Bass. "On the ubiquity of Gorenstein rings". In: *Math. Z.* 82 (1963), pp. 8–28 (↑ 13).

[BKM23] Jonas Bergström, Valentijn Karemaker, and Stefano Marseglia. "Polarizations of abelian varieties over finite fields via canonical liftings". In: *Int. Math. Res. Not. IMRN* 4 (2023), pp. 3194–3248 (↑ 1).

[BKM24] Jonas Bergström, Valentijn Karemaker, and Stefano Marseglia. "Abelian varieties over finite fields with commutative endomorphism algebra: theory and algorithms". In: *arXiv e-prints*, arXiv:2409.08865 (Sept. 2024), arXiv:2409.08865. eprint: `2409.08865` (math.NT) (↑ 1).

[Bis15] Gaetan Bisson. "Computing endomorphism rings of abelian varieties of dimension two". In: *Math. Comp.* 84.294 (2015), pp. 1977–1989 (↑ 8).

[Magma] Wieb Bosma, John Cannon, and Catherine Playoust. "The Magma algebra system. I. The user language". In: *J. Symbolic Comput.* 24.3-4 (1997). Computational algebra and number theory (London, 1993), pp. 235–265 (↑ 2, 22).

[BJW17] Ernest Hunter Brooks, Dimitar Jetchev, and Benjamin Wesolowski. "Isogeny graphs of ordinary abelian varieties". In: *Res. Number Theory* 3 (2017), Paper No. 28, 38 pp. (↑ 1).

[BL94] J. Buchmann and H. W. Lenstra Jr. "Approximating rings of integers in number fields". In: *J. Théor. Nombres Bordeaux* 6.2 (1994), pp. 221–260 (↑ 13).

[CCO14] Ching-Li Chai, Brian Conrad, and Frans Oort. "Complex multiplication and lifting problems". Vol. 195. Mathematical Surveys and Monographs. American Mathematical Society, Providence, RI, 2014 (↑ 20).

[CDMRV25] Edgar Costa, Taylor Dupuy, Stefano Marseglia, David Roe, and Christelle Vincent. "Labeling abelian varieties over finite fields". To appear in *Contemporary Mathematics*, available at `https://arxiv.org/abs/2501.17012`. 2025 (↑ 1).

[CDMRV26] Edgar Costa, Taylor Dupuy, Stefano Marseglia, David Roe, and Christelle Vincent. "AbVarFqIsogenies". stmar89/AbVarFqIsogenies. 2026 (↑ 2, 14, 22).

[Del69] Pierre Deligne. "Variétés abéliennes ordinaires sur un corps fini". In: *Invent. Math.* 8 (1969), pp. 238–243 (↑ 4).

[DKRV21] Taylor Dupuy, Kiran Kedlaya, David Roe, and Christelle Vincent. "Isogeny classes of abelian varieties over finite fields in the LMFDB". In: *Arithmetic geometry, number theory, and computation.* Simons Symposia. Springer, Cham, 2021, pp. 375–448 (↑ 3).

[FM02] Mireille Fouquet and François Morain. "Isogeny volcanoes and the SEA algorithm". In: *Algorithmic number theory (Sydney, 2002).* Vol. 2369. Lecture Notes in Comput. Sci. Springer, Berlin, 2002, pp. 276–291 (↑ 1).

[Hon68] Taira Honda. "Isogeny classes of abelian varieties over finite fields". In: *J. Math. Soc. Japan* 20 (1968), pp. 83–95 (↑ 2).

[How95] Everett W. Howe. "Principally polarized ordinary abelian varieties over finite fields". In: *Trans. Amer. Math. Soc.* 347.7 (1995), pp. 2361–2401 (↑ 20).

[IT20] Sorina Ionica and Emmanuel Thomé. "Isogeny graphs with maximal real multiplication". In: *J. Number Theory* 207 (2020), pp. 385–422 (↑ 1).

[Koh96] David Kohel. "Endomorphism rings of elliptic curves over finite fields". PhD thesis. University of California, Berkeley, 1996 (↑ 1).

[LMFDB] The LMFDB Collaboration. "The L-functions and Modular Forms Database". `http://www.lmfdb.org`. [Online; accessed 1 September 2023]. 2022 (↑ 1).

[Mar20] Stefano Marseglia. "Computing the ideal class monoid of an order". In: *Journal of the London Mathematical Society* 101.3 (2020), pp. 984–1007 (↑ 2, 5, 13, 16).

[Mar21] Stefano Marseglia. "Computing square-free polarized abelian varieties over finite fields". In: *Math. Comp.* 90.328 (2021), pp. 953–971 (↑ 1, 4, 20).

[Mar22] Stefano Marseglia. "Computing base extensions of ordinary abelian varieties over finite fields". In: *Int. J. Number Theory* 18.9 (2022), pp. 1957–1974 (↑ 11).

[Mar24] Stefano Marseglia. "Cohen-Macaulay type of orders, generators and ideal classes". In: *Journal of Algebra* 658 (2024), pp. 247–276 (↑ 14).

[Mar18] Chloe Martindale. "Isogeny Graphs, Modular Polynomials, and Applications". PhD thesis. Université de Bordeaux and Leiden University, 2018 (↑ 1).

[SageMath] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 10.9).* `https://www.sagemath.org`. 2026 (↑ 2).

[Sut13] Andrew V. Sutherland. "Isogeny volcanoes". In: *ANTS X. Proceedings of the tenth algorithmic number theory symposium, San Diego, CA, USA, July 9–13, 2012.* Berkeley, CA: Mathematical Sciences Publishers (MSP), 2013, pp. 507–530 (↑ 1, 9).

[Tat66] John Tate. "Endomorphisms of abelian varieties over finite fields". In: *Invent. Math.* 2 (1966), pp. 134–144 (↑ 2).

Edgar Costa, Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA
Email address: edgarc@mit.edu
URL: https://edgarcosta.org

Taylor Dupuy, Department of Mathematics and Statistics, Innovation Hall E220, 82 University Place, Burlington, VT, 05405, USA
Email address: taylor.dupuy@gmail.com
URL: http://tdupu.github.io

Stefano Marseglia, Laboratoire Jean Alexandre Dieudonné, Université Côte d'Azur, 06108 Nice Cedex 2, France
Email address: stefano.marseglia@univ-cotedazur.fr
URL: https://stmar89.github.io

David Roe, Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA
Email address: roed@mit.edu
URL: https://math.mit.edu/~roed

Christelle Vincent, Department of Mathematics and Statistics, Innovation Hall E220, 82 University Place, Burlington, VT, 05405, USA
Email address: christelle.vincent@uvm.edu
URL: https://www.uvm.edu/~cvincen1