Isogeny graphs with maximal real multiplication

Sorina Ionica, Emmanuel Thomé

Isogeny graphs with maximal real multiplication

Sorina Ionica[1,2] and Emmanuel Thomé[3]

[1] Institut de Mathématiques de Bordeaux & Inria Bordeaux - Sud-Ouest
200, avenue de la Vieille Tour–33405 Talence – France
[2] Université de Picardie Jules Verne
33 Rue Saint Leu Amiens 80039–France
[3] CARAMBA Project – INRIA Nancy Grand Est
615 rue du Jardin Botanique–54602 Villiers-les-Nancy – France

Abstract. An isogeny graph is a graph whose vertices are principally polarizable abelian varieties and whose edges are isogenies between these varieties. In his thesis, Kohel describes the structure of isogeny graphs for elliptic curves and shows that one may compute the endomorphism ring of an elliptic curve defined over a finite field by using a depth-first search (DFS) algorithm in the graph. In dimension 2, the structure of isogeny graphs is less understood and existing algorithms for computing endomorphism rings are very expensive. In this article, we show that, under certain conditions, the problem of determining the endomorphism ring can also be solved in genus 2 with a DFS-based algorithm. We consider the case of genus-2 Jacobians with complex multiplication, with the assumptions that the real multiplication subring has class number one and is locally maximal at ℓ, for ℓ a fixed prime. We describe the isogeny graphs in that case, by considering cyclic isogenies of degree ℓ, under the assumption that there is an ideal $\mathfrak{l}$ of norm ℓ in K_0 which is generated by a totally positive algebraic integer. The resulting algorithm is implemented over finite fields, and examples are provided. To the best of our knowledge, this is the first DFS-based algorithm in genus 2.

1 Introduction

Isogeny graphs are graphs whose vertices are simple principally polarizable abelian varieties (p.p.a.v.) and whose edges are isogenies between these varieties. Isogeny graphs were first studied by Kohel [22], who proves that in the case of elliptic curves, we may use these structures to compute the endomorphism ring of an elliptic curve. Kohel identifies three types of ℓ-isogenies (i.e. of degree ℓ) in the graph: ascending, descending and horizontal. The ascending (descending) type corresponds to the case of an isogeny between two elliptic curves, such that the endomorphism ring of the domain (co-domain) curve is contained in the endomorphism ring of the co-domain (domain) curve. The horizontal type is that of an isogeny between two genus 1 curves with isomorphic endomorphism rings. As a consequence, computing the ℓ-adic valuation of the conductor of the endomorphism ring can be done by a depth-first search algorithm in the isogeny graph [22]. In the case of genus-2 Jacobians, designing a similar algorithm for endomorphism ring computation requires a good understanding of the isogeny graph structure.

Let K be a primitive quartic CM field and K_0 its totally real subfield. In this paper, we study subgraphs of isogenies whose vertices are all genus-2 Jacobians with endomorphism ring isomorphic to an order of K whose real multiplication suborder is locally maximal at ℓ. Furthermore, we assume that $\mathcal{O}_{K_0}$ is principal, that there is a degree 1 ideal $\mathfrak{l}$ lying over ℓ in $\mathcal{O}_{K_0}$, and that this ideal is generated by a totally positive algebraic integer.

We show that the lattice of orders meeting these conditions has a simple 2-dimensional grid structure when we localize orders at ℓ. This results into a classification of isogenies in the isogeny graph into three types: ascending, descending and horizontal, where these qualificatives apply separately to the two "dimensions" of the lattice of orders. Moreover, we consider ℓ-isogenies, which are a generalization of ℓ-isogenies between elliptic curves to the higher dimensional principally polarized abelian varieties (see Definition 2). We show that any ℓ-isogeny that is such that the two endomorphism rings contain $\mathcal{O}_{K_0}$ is a composition of two isogenies of degree ℓ that preserve real multiplication. As a consequence, we design a depth-first search algorithm for computing endomorphism rings in the ℓ-isogeny graph, based on Cosset and Robert's algorithm for constructing ℓ-isogenies over finite fields. To the best of our knowledge, this is the first depth-first search algorithm for computing locally at small prime numbers ℓ the endomorphism ring of an ordinary genus-2 Jacobian. With our method, as well as with the Eisenträger-Lauter algorithm [13], the dominant part of the complexity is given by the computation of a subgroup of the ℓ-torsion. Our analysis shows that our algorithm performs faster, since a smaller torsion subgroup is computed, defined over a smaller field.

This paper is organized as follows. Section 2 provides background material concerning isogeny graphs, $\mathcal{O}_{K_0}$-orders of quartic CM fields, as well as the definition and some properties of the Tate pairing. In Section 3 we give formulae for cyclic isogenies between principally polarized complex tori with maximal real multiplication, and describe the structure of the graph whose edges are these isogenies. From this, in Section 4 we deduce the structure of the graph whose vertices are p.p.a.v. with maximal real multiplication, defined over finite fields, and whose edges are cyclic isogenies between these varieties. In Section 5 we show that the computation of the Tate pairing allows us to orient ourselves in the isogeny graph. Finally, in Section 6 we give our algorithm for endomorphism ring computation when the real multiplication is maximal, compare its performance to the one of Eisenträger and Lauter's algorithm, and report on practical experiments over finite fields.

Related work. Our work is publicly available at `https://arxiv.org/abs/1407.6672` and focuses on studying a graph structure between principally polarized abelian varieties. For generalizations of this work to the case where the vertices of the graph are abelian varieties with non-principal fixed polarizations, the reader is referred on the one hand to the the more recent work of Hunter Brooks *et al.* [6] that takes a p-adic approach to prove this graph structure. The recently defended thesis of Chloe Martindale [27] also revisits this construction, using a complex-analytic approach.

We present results regarding an isomorphism between an isogeny graph between abelian varieties defined over finite fields and the graph of their canonical lifts (Section 4). To the best of our knowledge, these results are not to be found anywhere else in the literature. This graph isomorphism is used in several steps of the proof developed in [6] (e.g. proof of Proposition 5.1 in [6], as well as the remark on page 20 on that same paper, regarding the fact that the Shimura class group action is free).

Finally, from an algorithmic point of view, [6] focuses on applications that need to compute, from a given abelian variety with CM, an isogeny path towards an abelian variety with maximal complex multiplication. The present work proposes an algorithm for computing endomorphism rings, via a depth first search method. To this purpose, we present several results on the Tate pairing (see Section 5) which are not to be found elsewhere in the literature.

Acknowledgements

This work originates from discussions during a visit at University of Caen in November 2011. We are indebted to John Boxall for sharing his ideas regarding the computation of isogenies preserving the real multiplication, and providing guidance for improving the writing of this paper. We thank David Gruenewald, Ben Smith and Damien Robert for helpful and inspiring discussions. Finally, we are grateful to Marco Streng and to Gaetan Bisson for proofreading an early version of this manuscript.

2 Background and notations

It is well known that in the case of elliptic curves with complex multiplication by an imaginary quadratic field K, the lattice of orders of K has the structure of a tower. This results in an easy way to classify isogenies and navigate in isogeny graphs [22,14,20]. Throughout this paper, we are concerned with the genus 2 case.

Let then K be a primitive quartic CM field, with totally real subfield K_0. Principally polarized abelian surfaces considered in this paper are assumed to be *simple*, i.e. not isogenous to a product of elliptic curves over the algebraic closure of their field of definition. The quartic CM field K is primitive, i.e. it does not contain a totally imaginary subfield. A CM-type Φ is a pair of non-complex conjugate embeddings of K in $\mathbb{C}$

$$\Phi(z) = \{\phi_1(z), \phi_2(z)\}.$$

We assume that K_0 has class number one. This implies in particular that the maximal order $\mathcal{O}_K$ is a module over the principal ideal ring $\mathcal{O}_{K_0}$, whence we may define η such that

$$\mathcal{O}_K = \mathcal{O}_{K_0} + \mathcal{O}_{K_0}\eta. \tag{1}$$

The notation η will be retained throughout the paper. For an abelian variety A defined over a perfect field F we denote by $\mathrm{End}(A)$ the endomorphism ring of A over the algebraic closure of F and by $\mathrm{End}^0(A) = \mathrm{End}(A) \otimes \mathbb{Q}$.

Several results of the article will involve a prime number ℓ and also the finite field $\mathbb{F}_q$ ($q = p^n$, with p prime). We always implicitly assume that ℓ is coprime to p. For an order $\mathcal{O}$ in K or K_0, we denote its localization at ℓ by $\mathcal{O}_\ell = \mathcal{O} \otimes \mathbb{Z}_\ell$. Note that the case which matters for our point of view is when ℓ splits as two distinct degree-one prime ideals $\mathfrak{l}_1$ and $\mathfrak{l}_2$ in $\mathcal{O}_{K_0}$. How the ideals $\mathfrak{l}_1$ and $\mathfrak{l}_2$ split in $\mathcal{O}_K$ is not determined a priori, however.

2.1 Isogeny graphs: definitions and terminology

In this paper, we are interested in isogeny graphs whose nodes are all isomorphism classes of principally polarizable abelian surfaces (i.e. Jacobians of hyperelliptic genus-2 curves) with CM by K and whose edges are isogenies between them, up to isomorphism.

Definition 1. *Let $I : A \to B$ be an isogeny between polarized abelian varieties and let λ be a fixed polarization on B. The induced polarization on A, that we denote by $I^*\lambda$, is defined by*

$$I^*\lambda = \hat{I} \circ \lambda \circ I.$$

We denote by (A, λ) a polarized abelian variety with a fixed polarization λ. We recall here the definition of an ℓ-isogeny.

Definition 2. *Let $I : (A, \lambda_A) \to (B, \lambda_B)$ be an isogeny between principally polarized abelian varieties. We will say that I is an ℓ-isogeny if $I^*\lambda_B = \ell\lambda_A$.*

One can easily see that these isogenies have degree ℓ^2 and have kernel isomorphic to $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$. The fact that for $I : (A, \lambda_A) \to (B, \lambda_B)$, one has $I^*\lambda_B = \ell\lambda_A$ is equivalent to $\mathrm{Ker}\, I$ being maximal isotropic with respect to the Weil pairing, i.e. the ℓ-Weil pairing restricts trivially to $\mathrm{Ker}\, I$ and $\mathrm{Ker}\, I$ is not properly contained in any other such subgroup (see [21, Prop. 13.8]). Note that in the literature these isogenies are sometimes called (ℓ, ℓ)-isogenies (see for instance [25,9]). Since ℓ-isogenies are a generalization of genus-1 ℓ-isogenies, a natural idea would be to consider the graph given by *ℓ-isogenies* between principally polarized abelian surfaces. Recent developments on the construction of ℓ-isogenies [25,9] allowed us to compute examples of isogeny graphs over finite fields, whose edges are rational ℓ-isogenies [3]. It was noticed in this way that the corresponding lattice of orders has a much more complicated structure when compared to its genus-1 equivalent. Figure 1 displays an example of an ℓ-isogeny graph. Identification of each variety to its dual, makes this graph non-oriented. The corresponding lattice of orders contains two orders of index 3 (in the maximal order), which are not contained one in the other. The existence of rational isogenies between Jacobians corresponding to these two orders shows that we cannot classify isogenies into ascending/descending and horizontal ones. This is a major obstacle to designing a depth-first search algorithm for computing the endomorphism ring.

Finally, to introduce the isogeny graph of principally polarized abelian varieties with complex multiplication, we will also need the following result, which was communicated to us by Damien Robert [31].

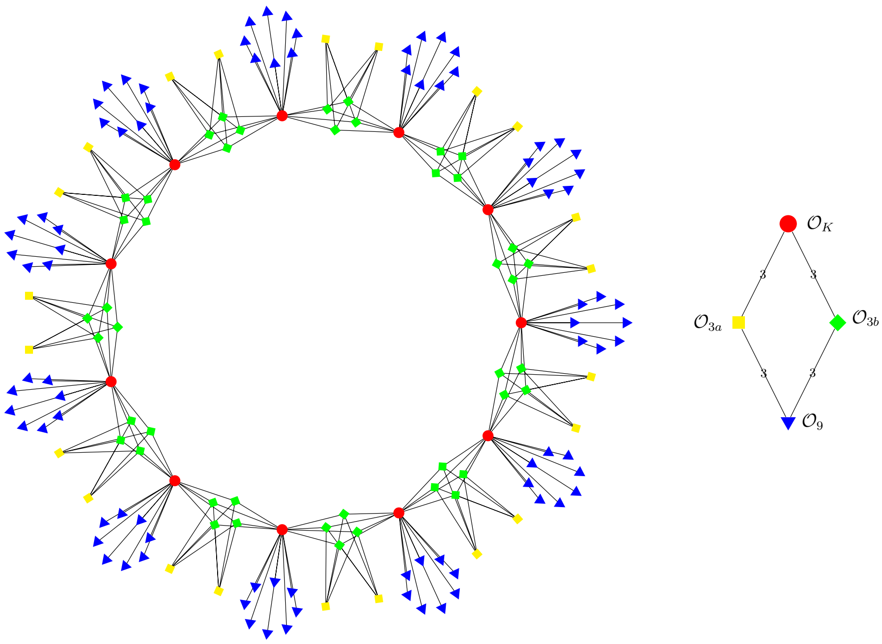


Fig. 1. Example of an ℓ-isogeny graph for $\ell = 3$ defined over a finite field $\mathbb{F}_p$, with $p = 211$ and K defined by $\alpha^4 + 81\alpha^2 + 1181$.

Lemma 3. *If $I : (A, \lambda_A) \to (B, \lambda_B)$ is an isogeny between principally polarizable abelian varieties, then the homomorphism corresponding to the induced polarization can be written as $I^*\lambda_B = \lambda_A \circ \phi$, where ϕ is a real endomorphism.*

We recall the definition of an abelian variety with complex (respectively real) multiplication.

Definition 4. *Let A be a principally polarized abelian variety. Let K be a quartic CM field, and K_0 its totally real subfield.*

1. *We say that a pair (A, ι) is an* abelian variety with complex multiplication *by an order $\mathcal{O} \subset K$ if there is a morphism of $\mathbb{Q}$-algebras $\iota : K \hookrightarrow \mathrm{End}^0(A)$ such that $\iota^{-1}(\mathrm{End}(A)) = \mathcal{O}$ induces a ring isomorphism between $\mathcal{O}$ and $\mathrm{End}(A)$.*
2. *Similarly, we say that a pair (A, ι_0) is an* abelian variety with real multiplication *by an order $\mathcal{O}_0 \subset K_0$ if there is a morphism of $\mathbb{Q}$-algebras $\iota_0 : K_0 \hookrightarrow \mathrm{End}^0(A)$ and such that $\iota_0^{-1}(\mathrm{End}(A) \cap \iota_0(K_0)) = \mathcal{O}_0$.*

By the definition above, an abelian variety may have complex (resp. real) multiplication by only one isomorphism class of orders of the lattice of orders of K (resp. K_0). We also note that if (A, ι) has complex multiplication by $\mathcal{O} \subset K$, then $(A, \iota|_{K_0})$ has real multiplication by $\mathcal{O} \cap K_0$. In this work, we fix a quartic CM field K and we consider abelian varieties having complex multiplication by an order in K.

Let A and B be two principally polarized abelian varieties with real (resp. complex) multiplication by an order $\mathcal{O}$ and let $I : A \to B$ be a separable isogeny. We denote by e_I the exponent of I (i.e. the exponent of the finite group $\mathrm{Ker}(I)$). Since $\mathrm{Ker}(I) \subset A[e_I]$ (where $A[e_I]$ is the e_I-torsion subgroup of A), there is a unique isogeny I' such that $II' = [e_I]$. We define the following map:

$$\Theta_B : \mathrm{End}^0(B) \to \mathrm{End}^0(A)$$
$$\phi \to \frac{1}{e_I} I' \circ \phi \circ I.$$

With this in hand, we say that I is an *isogeny between abelian varieties with real (resp. complex) multiplication* by a field K_0 (resp. K) if the following diagram involving the solid arrows is commutative. (Equivalently, the diagram obtained by using Θ_A instead of Θ_B is also commutative.)

$$\begin{array}{ccc} K_0(\text{resp. } K) & \xrightarrow{\iota_B} & \mathrm{End}^0(B) \\ & \searrow^{\iota_A} & \Theta_B \downarrow \;\; \uparrow \Theta_A \\ & & \mathrm{End}^0(A) \end{array}$$

In this work, we denote by (A, λ, ι) a principally polarized abelian variety with complex multiplication. Note that here and throughout the paper, we shall only distinguish isogenies up to isomorphism, regarding isogenies $I_1 : A \to B$ and $I_2 : A \to B$ as equivalent if $I_1 = i_2 \circ I_2 \circ i_1$ for any automorphisms $i_1 : A \to B$ and $i_2 : A \to B$. The approach we will take here is to consider the graph of *all* (equivalence classes of) isogenies between principally polarizable abelian surfaces and decompose it into subgraphs whose vertices are abelian surfaces with real multiplication by a fixed order $\mathcal{O}$ of K_0.

Definition 5. *Let F be a perfect field. An isogeny graph of principally polarized abelian varieties defined over F is a graph such that:*

1. *The vertices are isomorphism classes of principally polarized abelian varieties (A, λ, ι) with complex multiplication.*
2. *There is an edge between two classes (A, λ_A, ι_A) and (B, λ_B, ι_B) whenever there is an isogeny $I : A \to B$ between abelian varieties with CM, such that $\lambda_B I^* = \lambda_A \circ \phi$, for ϕ some real endomorphism.*

Definition 6. *With the notation above, let (A, ι_A) and (B, ι_B) two abelian varieties with complex multiplication by a CM field K and $I : A \to B$ an isogeny between them. We say that I preserves real multiplication by an order $\mathcal{O}$ in K_0 if both A and B have real multiplication by $\mathcal{O}$.*

As a consequence, for an order $\mathcal{O}$ in K_0, we call *$\mathcal{O}$-layer in the graph given by Definition 5* the subgraph whose vertices are all equivalence classes of p.p.a.v with RM by $\mathcal{O}$ and whose edges are isogenies preserving real multiplication by $\mathcal{O}$. Understanding the structure of the graph then comes down to explaining the structure of each layer and in a later step classifying isogenies beween two vertices lying at different layers of the graph.

In this paper, we fully describe the structure of the $\mathcal{O}_{K_0}$-layer. Working towards this goal, we first identify cyclic isogenies of degree ℓ between principally polarizable abelian varieties with maximal real multiplication. We will show in Section 3 that a sufficient condition to guarantee the existence of isogenies of degree ℓ between principally polarized abelian varieties is that there is a principal ideal in $\mathcal{O}_{K_0}$ of degree 1 and norm ℓ, whose generator is totally positive.

As a consequence, we chose to focus on the case where ℓ splits in $\mathcal{O}_{K_0}$ into two principal ideals. Under these restrictions, we describe the simple and interesting structure of the graph of cyclic isogenies, which fits into the ascending/descending and horizontal framework. Using this graph structure, we characterize all isogenies between principally polarized abelian surfaces which preserve maximal real multiplication. This leads in particular to viewing Figure 1 as derived from a more structured graph, whose characteristics are well explained.

The case when ℓ is ramified the graph structure is similar, as explained in Section 3 (Remark 22). In the case of ℓ inert, one can see easily from Lemma 3 that there are no degree ℓ isogenies between principally polarizable abelian varieties with CM by K, preserving real multiplication. Indeed, if there were, this would imply the existence of a norm ℓ element $\alpha \in \mathcal{O}_{K_0}$. We chose not to treat the case of ℓ inert in this work.

2.2 The lattice of $\mathcal{O}_{K_0}$-orders in a quartic CM field K

A major obstacle to explaining the structure of genus 2 isogeny graphs is that the lattice of orders of K lacks a concise description. Given an isogeny $I : A \to B$ between two abelian surfaces with degree ℓ, the corresponding endomorphism rings are such that $\ell\mathcal{O}_A \subset \mathcal{O}_B$ and $\ell\mathcal{O}_B \subset \mathcal{O}_A$. Hence, even if a inclusion relation is guaranteed $\mathcal{O}_B \subset \mathcal{O}_A$, the index of one order in the other is bounded by ℓ^3. Since the $\mathbb{Z}$-rank of orders is 4, there could be several suborders of $\mathcal{O}_A$ with the same index.

In this paper, we study the structure of the isogeny graph between abelian varieties with maximal real multiplication. The first step in this direction is to describe the structure of the lattice of orders of K which contain $\mathcal{O}_{K_0}$. Following [16], we call such an order an $\mathcal{O}_{K_0}$-order. We study the conductors of such orders. We recall that the conductor of an order $\mathcal{O}$ is the ideal

$$\mathfrak{f}_{\mathcal{O}} = \{x \in \mathcal{O}_K \mid x\mathcal{O}_K \subset \mathcal{O}\}.$$

Lemma 7. *Let K be a quartic CM-field and K_0 its real multiplication subfield. Assume that the class number of K_0 is 1. Then the following hold:*

1. *Given $\alpha \in \mathcal{O}_{K_0}$, $\mathcal{O} = \mathcal{O}_{K_0}[\alpha\eta]$ is an $\mathcal{O}_{K_0}$-order of conductor $\alpha\mathcal{O}_{K_0}$.*
2. *For any $\mathcal{O}_{K_0}$-order $\mathcal{O}$ of K there is $\alpha \in \mathcal{O}_{K_0}$, $\alpha \neq 0$ such that $\mathcal{O} = \mathcal{O}_{K_0}[\alpha\eta]$. The element α is unique up to units of $\mathcal{O}_{K_0}$.*

Proof. Statements 1 and 2 were given by Goren and Lauter [16], and characterize $\mathcal{O}_{K_0}$-orders completely in our case.

As a consequence, we get the following result.

Lemma 8. *Any $\mathcal{O}_{K_0}$-order is a Gorenstein order.*

Proof. This is a consequence of the fact that $\mathcal{O}$ is monogenic over $\mathcal{O}_{K_0}$, hence the argument of [7, Example 2.8 and Prop. 2.7] applies. □

A first consequence of Lemma 7 is that there is a bijection between $\mathcal{O}_{K_0}$-orders and principal ideals in $\mathcal{O}_{K_0}$, which associates to every order the ideal $\mathfrak{f} \cap \mathcal{O}_{K_0}$. For brevity we still call the latter the conductor and denote it by $\mathfrak{f}$.

Using the particular form of $\mathcal{O}_K$ as a monogenic $\mathcal{O}_{K_0}$-module, we may rewrite the conductor differently. For a fixed element $\omega \in \mathcal{O}_K$, we define the conductor of $\mathcal{O}$ with respect to ω to be the ideal

$$\mathfrak{f}_{\omega,\mathcal{O}} = \{x \in \mathcal{O}_K \mid x\omega \in \mathcal{O}\}.$$

The following statement is an immediate consequence of Lemma 7.

Lemma 9. *For any $\mathcal{O}_{K_0}$-order $\mathcal{O}$ and any η such that $\mathcal{O}_K = \mathcal{O}_{K_0}[\eta]$, we have $\mathfrak{f}_{\mathcal{O}} = \mathfrak{f}_{\eta,\mathcal{O}}$.*

Now let $\mathcal{O}$ be an order in K with locally maximal real multiplication at ℓ (i.e. $(\mathcal{O}_{K_0})_\ell \subset \mathcal{O}_\ell$). Assume that the index of $\mathcal{O}$ is divisible by a power of ℓ and that ℓ splits in $\mathcal{O}_{K_0}$ and let $\ell = \mathfrak{l}_1\mathfrak{l}_2$. Then $\mathcal{O}_\ell$ is isomorphic to the localization of a $\mathcal{O}_{K_0}$-order, whose conductor $\mathfrak{f}$ has a unique factorization into prime ideals containing $\mathfrak{l}_1^{e_1}\mathfrak{l}_2^{e_2}$. Locally at ℓ, the lattice of orders of index divisible by ℓ has the form given in Figure 2. This is equivalent to the following statement.

Lemma 10. *Let $\mathcal{O}$ be an order in K, with locally maximal real multiplication. The position of $\mathcal{O}_\ell$ within the lattice of $\mathcal{O}_{K_0}$-orders localized at ℓ is given by the valuations $\nu_{\mathfrak{l}_i}(\mathfrak{f}_{\mathcal{O}})$, for $i = 1, 2$.*

We call level in the lattice of orders the set of all orders having the same ℓ-adic valuation of the norm of the conductor. For example, level 2 in Figure 2 is formed by three orders with conductors $\mathfrak{l}_1^2, \mathfrak{l}_1\mathfrak{l}_2$ and $\mathfrak{l}_2^2$, respectively. This distribution of orders on levels leads to a classification of isogenies into descending and ascending ones, which is the key point to a DFS algorithm for navigating in the isogeny graph, just like in the elliptic curve case. This will be furthered detailed in Section 4.

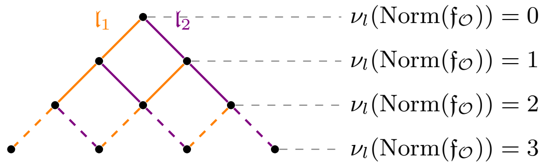


Fig. 2. The lattice of orders

2.3 The Tate pairing

Let A be a polarized abelian surface, defined over a perfect field F. We denote by $A[m]$ the m-torsion subgroup. We denote by μ_m the group of m-th roots of unity and by

$$W_m : A[m] \times \hat{A}[m] \to \mu_m$$

the m-Weil pairing on the abelian surface.

In this paper, we are only interested in the Tate pairing over finite fields. We give a specialized definition of the pairing in this case, following [32,18]. More precisely, let $F = \mathbb{F}_q$ and suppose that we have $m \,|\, \#A(\mathbb{F}_q)$. We denote by k the *embedding degree with respect to* m, i.e. the smallest integer $k \geq 0$ such that $m \,|\, q^k - 1$. Moreover, we assume that $A[m]$ is defined over $\mathbb{F}_{q^k}$. We define the Tate pairing as

$$T_m(\cdot,\cdot) : \begin{cases} A(\mathbb{F}_{q^k})/mA(\mathbb{F}_{q^k}) \times \hat{A}[m](\mathbb{F}_{q^k}) \to \mu_m \\ \qquad\qquad\qquad\qquad (P, Q) \mapsto W_m(\pi_k(\bar{P}) - \bar{P}, Q), \end{cases}$$

where π_k is k-th power of the Frobenius endomorphism of A and $\bar{P}$ is any point such that $m\bar{P} = P$. Note that since $A[m] \subseteq A(\mathbb{F}_{q^k})$, this definition is independent of the choice of $\bar{P}$. Indeed, if $\bar{P}_1$ is a second point such that $m\bar{P}_1 = P$, then $\bar{P}_1 = \bar{P} + T$, where T is a m-torsion point, and $\pi_k(\bar{P}_1) - \bar{P}_1 = \pi_k(\bar{P}) - \bar{P}$.
For a fixed polarization $\lambda : A \to \hat{A}$ we define a pairing on A itself

$$T_m^{\lambda}(\cdot,\cdot) : \begin{cases} A(\mathbb{F}_{q^k})/mA(\mathbb{F}_{q^k}) \times A[m](\mathbb{F}_{q^k}) \to \mu_m \\ \qquad\qquad\qquad\qquad (P, Q) \mapsto t_m(P, \lambda(Q)). \end{cases}$$

If A has a distinguished principal polarization and there is no risk of confusion, we write simply $T_m(\cdot,\cdot)$ instead of $T_m^{\lambda}(\cdot,\cdot)$.

Lichtenbaum [24] describes a version of the Tate pairing on Jacobian varieties. Since we use Lichtenbaum's formula for computations, we briefly recall it here. Let $D_1 \in A(\mathbb{F}_{q^k})$ and $D_2 \in A[m](\mathbb{F}_{q^k})$ be two divisor classes, represented by two divisors such that $\mathrm{supp}(D_1) \cap \mathrm{supp}(D_2) = \emptyset$. Since D_2 has order m, there is a function f_{m,D_2} such that $\mathrm{div}(f_{m,D_2}) = mD_2$. The Lichtenbaum pairing of the divisor classes D_1 and D_2 is computed as

$$t_m(D_1, D_2) = f_{m,D_2}(D_1).$$

The output of this pairing is defined up to a coset of $(\mathbb{F}_{q^k}^*)^m$. Given that $\mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^m \simeq \mu_m$, we obtain a pairing defined as

$$T_m(\cdot,\cdot) : A(\mathbb{F}_{q^k})/mA(\mathbb{F}_{q^k}) \times A[m](\mathbb{F}_{q^k}) \to \mu_m$$
$$(P, Q) \to t_m(P, Q)^{(q^k-1)/m}.$$

The function $f_{m,D_2}(D_1)$ is computed using Miller's algorithm [29] in $O(\log m)$ operations in $\mathbb{F}_{q^k}$.

3 Isogenies preserving real multiplication

Let K be a quartic CM field and $\Phi = (\phi_1, \phi_2)$ be a CM-type. The notation $\mathcal{O}^\dagger$ denotes the complementary module of an order $\mathcal{O}$, i.e. $\mathcal{O}^\dagger = \{\alpha \in K | \operatorname{Tr}_{K/\mathbb{Q}}(\alpha\mathcal{O}) \subseteq \mathbb{Z}\}$. In this Section all abelian varieties are defined over $\mathbb{C}$, unless specifically stated otherwise. A principally polarized abelian surface over $\mathbb{C}$ with complex multiplication by an order $\mathcal{O} \subset K$ is of the form $A = \mathbb{C}^2/\Phi(\mathfrak{a})$, where $\mathfrak{a}$ is a fractional ideal of $\mathcal{O}$ and such that

$$\xi \mathfrak{a}\bar{\mathfrak{a}} = \mathcal{O}^\dagger, \tag{2}$$

with ξ purely imaginary such that $\phi_i(\xi)$ lies on the positive imaginary axis for $i \in \{1, 2\}$. The variety given by $(\mathfrak{a}, \xi)$ is said to be of CM-type $(\mathcal{O}, \Phi)$. The imaginary part of any Riemann form on $\mathbb{C}^2/\Phi(\mathfrak{a})$ writes as

$$E_\xi(z, w) = \sum_{r=1}^{2} \xi^{\phi_r}(x'^{\phi_r} y^{\phi_r} - x^{\phi_r} y'^{\phi_r}),$$

with $z = x + y\tau, w = x' + y'\tau$, where $x, y, x', y' \in \mathbb{R}$.
This defines a principal polarization [1] that we denote by λ_ξ. By extension, for a given isogeny $I : (\mathbb{C}^2/\Phi(\mathfrak{a}), \lambda_\xi) \to (\mathbb{C}^2/\Phi(\mathfrak{b}), \lambda_{\xi'})$, we call induced polarization $I^* E_{\xi'}(u, v) = E_{\xi'}(I(u), I(v))$, for all $u, v \in \mathbb{C}^2$.
Recall that we focus on the case where $\mathcal{O}_{K_0} \subset \mathcal{O}$.

Lemma 11. *Let K be a quartic CM field and K_0 its maximal real subfield with class number 1 and let δ be the generator of $(\mathcal{O}^\dagger_{K_0})^{-1}$ and μ a generator for the conductor of $\mathcal{O}$. For every p.p.a.v. of CM-type $(\mathcal{O}, \Phi)$ given by $(\mathfrak{a}, \xi)$ there exists $\tau \in K$ such that*

1. $\mathfrak{a} = \mathcal{O}_{K_0} + \mathcal{O}_{K_0}\tau$
2. $\xi = -1/\delta\mu(\tau - \bar{\tau})$
3. $(\tau^{\phi_1}, \tau^{\phi_2}) \in \mathbb{H}_1 \times (\mathbb{C} \setminus \mathbb{R})$, *where $\mathbb{H}_1$ is the upper-half plane.*

Proof. Since $\mathcal{O}_{K_0}$ is a Dedekind domain and the ideal $\mathfrak{a}$ is an $\mathcal{O}_{K_0}$-module, we may then write it as $\mathfrak{a} = \Lambda_1\alpha + \Lambda_2\beta$, with $\alpha, \beta \in K$, and $\Lambda_{1,2}$ two $\mathcal{O}_{K_0}$-ideals. Hence we have $A \cong \mathbb{C}^2/\Phi(\Lambda)$ and $\Lambda = \alpha^{-1}\mathfrak{a} = \Lambda_1 + \Lambda_2\tau$, with Λ_1 and Λ_2 lattices in K_0 and $\tau = \frac{\beta}{\alpha} \in K$. Note that since K_0 has class number one, it follows that we can choose $\Lambda_1 = \Lambda_2 = \mathcal{O}_{K_0}$.

For the proof of 2, we use the computations in [34, Prop. 4.2] which shows that

$$\mathfrak{a}\bar{\mathfrak{a}} = (\frac{\tau - \bar{\tau}}{\eta - \bar{\eta}}),$$

where η is the one defined by Equation (1). Note that $\mathcal{O}^\dagger = \{\alpha \in K | \operatorname{Tr}_{K/\mathbb{Q}}(\alpha\mathcal{O}) \subseteq \mathbb{Z}\} = \{\alpha \in K | \operatorname{Tr}_{K/K_0}(\alpha\mathcal{O}) \subseteq \mathcal{O}_{K_0}\}\mathcal{O}^\dagger_{K_0}$. From this and by using [7, Example 2.8], we get that $\mathcal{O}^\dagger = \frac{1}{\mu(\eta - \bar{\eta})\delta}\mathcal{O}$. We conclude that $\xi = -1/\delta\mu(\tau - \bar{\tau})$.

To prove 3, we look at the equality obtained in 2. The fact that $(\tau^{\phi_1}, \tau^{\phi_2}) \in \mathbb{H}_1 \times (\mathbb{C} \setminus \mathbb{R})$ follows from the fact that ξ^{ϕ_i}, $i = 1, 2$ is on the positive imaginary axis and that we may assume, without restricting the generality, that $(\delta\mu)^{\phi_1}$ is positive. □

The isogenies discussed by the following proposition were brought to our attention by John Boxall.

Proposition 12. *Let K and K_0 be as previously stated. Let ℓ be a prime, and $\mathfrak{l} \subset \mathcal{O}_{K_0}$ a prime $\mathcal{O}_{K_0}$-ideal of norm ℓ. Let $A = \mathbb{C}^2/\Phi(\Lambda)$ be an abelian surface over $\mathbb{C}$ with complex multiplication by an $\mathcal{O}_{K_0}$-order $\mathcal{O} \subset K$, with $\Lambda = \Lambda_1 + \Lambda_2\tau$. A set of representatives of the cyclic subgroups of $(\mathfrak{l}^{-1}\Lambda)/\Lambda$, and more precisely of the isogenies on A having these subgroup as kernels is given by $\{I_\infty\} \cup \{I_\rho,\ \rho \in \Lambda_1\Lambda_2^{-1}/\mathfrak{l}\Lambda_1\Lambda_2^{-1}\}$, where:*

$$I_\infty : \begin{cases} A \to \mathbb{C}^2/\Phi(\mathfrak{l}^{-1}\Lambda_1 + \Lambda_2\tau), \\ z \mapsto z, \end{cases} \quad I_\rho : \begin{cases} A \to \mathbb{C}^2/\Phi(\Lambda_1 + \mathfrak{l}^{-1}\Lambda_2(\tau + \rho)), \\ z \mapsto z. \end{cases} \tag{3}$$

Proof. Our hypotheses imply that Λ is an $\mathcal{O}_{K_0}$-module of rank two, from which it follows that $(\mathfrak{l}^{-1}\Lambda)/\Lambda$ is isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^2$. The $\ell+1$ cyclic subgroups of $(\mathfrak{l}^{-1}\Lambda)/\Lambda$ are the kernels of the isogenies given in the Proposition. □

The isogenies given by Equation (3) are examples of $\mathfrak{l}$-isogenies, that we define as follows.

Definition 13. *Let $\mathfrak{l}$ be an prime ideal of $\mathcal{O}_{K_0}$ of norm a prime number ℓ. Then the $\mathfrak{l}$-torsion of an abelian variety A defined over a perfect field F with real multiplication by $\mathcal{O}_{K_0}$ is given by*

$$A[\mathfrak{l}] = \{x \in A(\overline{F}) \text{ s.t. } \alpha x = 0, \ \forall \alpha \in \mathfrak{l}\}.$$

Isogenies with kernel a cyclic subgroup of $A[\mathfrak{l}]$ of order ℓ are called $\mathfrak{l}$-isogenies.

For the commonly encountered case where $\mathfrak{l} = \alpha\mathcal{O}_{K_0}$ for some generator $\alpha \in \mathcal{O}_{K_0}$ (which occurs in our setting since $\mathcal{O}_{K_0}$ is assumed principal), the notation $A[\mathfrak{l}]$ above matches with the notation $A[\alpha]$ representing the kernel of the endomorphism represented by α. In this situation, the cyclic isogenies introduced in Definition 13 are also called α-isogenies.

In the remainder of this paper, we assume that $\mathfrak{l}$ is a prime ideal of norm ℓ. This implies that ℓ is either split or ramified in K_0. In this paper, we deliberately chose to focus on the split case. This restriction allows us to further design an algorithm for endomorphism ring computation, as we will explain in Section 6.

Given Definition 13, Proposition 12 can be regarded as giving formulae for a set of representatives for isomorphism classes of $\mathfrak{l}$-isogenies over the complex numbers.

The following trivial observation that $\mathfrak{l}$-isogenies preserve the maximal real multiplication follows directly from $\mathrm{End}(\mathfrak{l}^{-1}\Lambda_i) = \mathrm{End}(\Lambda_i)$. Later in this article we will show that a converse to this statement also holds: an isogeny which preserves the maximal real multiplication is an $\mathfrak{l}$-isogeny (Proposition 32).

Proposition 14. *Let A be an abelian surface defined over $\mathbb{C}$ with* $\mathrm{End}(A)$ *an $\mathcal{O}_{K_0}$-order. Let $I : A \to B$ be an $\mathfrak{l}$-isogeny. Then* $\mathrm{End}(B)$ *is also an $\mathcal{O}_{K_0}$-order.*

The following proposition shows how polarizations can be transported through $\mathfrak{l}$-isogenies. We use here the fact that $\mathcal{O}_{K_0}$ is assumed to have class number one.

Proposition 15. *Let A be an abelian surface with* $\mathrm{End}(A)$ *an $\mathcal{O}_{K_0}$-order. Let $I : A \to B$ be an $\mathfrak{l}$-isogeny (following the notations of Proposition 12). Let E_ξ define a principal polarization of A. If $\mathfrak{l} = (\alpha)$ with $\alpha \in K_0$ totally positive, $E_{\alpha\xi}$ defines a principal polarization on B. Moreover, $I^*E_{\alpha\xi} = \alpha E_\xi$.*

Proof. We follow notations of Proposition 12 and take $I = I_\infty$ as an example (the other cases are similar). We can write

$$E_\xi(x + y\tau, x' + y'\tau) = E_{\alpha\xi}(\frac{x}{\alpha} + y\tau, \frac{x'}{\alpha} + y'\tau).$$

Hence if E_ξ defines a principal polarization on $\mathbb{C}^2/\Phi(\Lambda_1 + \Lambda_2\tau)$ and α is totally positive then $E_{\alpha\xi}$ defines principal polarizations on the variety $\mathbb{C}^2/\Phi(\frac{\Lambda_1}{\alpha} + \Lambda_2\tau)$ (we just showed that the matrices of the corresponding Riemann forms are equal).

The fact that $I^*E_{\alpha\xi} = \alpha E_\xi$ follows from the definition of I^*, and of the Riemann forms E_ξ and $E_{\alpha\xi}$. □

Lemma 16. *Let A be a principally polarized abelian variety under the assumptions in Proposition 15. The dual of an α-isogeny starting from A is an α-isogeny.*

Proof. This follows trivially from $I^*E_{\alpha\xi} = \alpha E_\xi$, since this implies that $\alpha\lambda_\xi = \hat{I} \circ \lambda_{\alpha\xi} \circ I$, where λ_ξ and and $\lambda_{\alpha\xi}$ are the isogenies corresponding to polarizations E_ξ and $E_{\alpha\xi}$. □

In the remainder of this paper, we assume that α as in Proposition 15 exists and is totally positive. It becomes clear then that the α-isogenies we introduced are edges in the graph given by Definition 5. By Proposition 14 they are edges in the $\mathcal{O}_{K_0}$-layer of this graph.

Remark 17. If ℓ is a prime number such that $\ell\mathcal{O}_{K_0} = \mathfrak{l}_1\mathfrak{l}_2$, we denote by α_i, $i = \{1, 2\}$, elements of $\mathcal{O}_{K_0}$ such that $\mathfrak{l}_i = \alpha_i\mathcal{O}_{K_0}$. Let $I : A \to B$ be an $\mathfrak{l}_1$-isogeny. Proposition 15 implies that for a given polarization ξ on A, $\ell\lambda_\xi = \hat{I} \circ (\alpha_2\lambda_{\alpha_1\xi}) \circ I$.

Note that if ℓ is such that $\ell\mathcal{O}_{K_0} = \mathfrak{l}_1\mathfrak{l}_2$, with $\mathfrak{l}_1 + \mathfrak{l}_2 = (1)$, then the factorization of ℓ yields a symplectic basis for the ℓ-torsion. Indeed, we have $J[\ell] = J[\mathfrak{l}_1] + J[\mathfrak{l}_2]$, and the following proposition establishes the symplectic property.

Proposition 18. *Let J be a principally polarized abelian surface defined over a number field L. With the notations above, we have $W_\ell(P_1, P_2) = 1$ for any $P_1 \in J[\mathfrak{l}_1]$ and $P_2 \in J[\mathfrak{l}_2]$.*

Proof. This can be easily checked on the complex torus $\mathbb{C}^2/\Phi(\Lambda_1 + \Lambda_2\tau)$. Let $P_1 = \frac{x_1}{\alpha_1} + \frac{x_2}{\alpha_1}\tau \in J[\alpha_1]$ and $P_2 = \frac{y_1}{\alpha_2} + \frac{y_2}{\alpha_2}\tau \in J[\alpha_2]$, where $x_1, y_1 \in \Lambda_1$ and $x_2, y_2 \in \Lambda_2$. Then $W_\ell(P_1, P_2) = \exp(-2\pi i\ell\frac{E_\xi(x_1+x_2\tau, y_1+y_2\tau)}{\ell})) = 1$. □

The following lemma allows us to count the number of principally polarized abelian varieties with CM by an $\mathcal{O}_{K_0}$-order $\mathcal{O}$.. Along the lines of its proof, we also show that the action of Shimura class group of $\mathcal{O}$ on the set of p.p.a.v. with CM by $\mathcal{O}$ is simple and transitive.

Lemma 19. *Let $\mathcal{O}$ be an $\mathcal{O}_{K_0}$-order in a CM quartic field K. The number of isomorphism classes of principally polarized abelian surfaces with CM type $(\mathcal{O}, \Phi)$ is*

$$\frac{\#\,\mathrm{Cl}(\mathcal{O})}{\#\,\mathrm{Cl}^+(\mathcal{O}_{K_0})} \cdot \#(\mathcal{O}_{K_0}^\times)^+/N_{K/K_0}(\mathcal{O}^\times).$$

Proof. Note first that when $\mathcal{O}$ is an $\mathcal{O}_{K_0}$-order, then all principally polarized abelian varieties over $\mathbb{C}$ are of the form $\mathbb{C}^2/\Phi(\mathfrak{a})$, with $\mathfrak{a}$ an invertible ideal of $\mathcal{O}$. This follows from Equation (2) because $\mathcal{O}$ is Gorenstein (see Lemma 7), and thus $\mathcal{O}^\dagger$ is invertible. Just like in the case of $\mathcal{O} = \mathcal{O}_K$ treated by Shimura, it then follows that there is a transitive simple action of the Shimura class group of $\mathcal{O}$, denoted by $\mathfrak{C}(\mathcal{O})$, on the set of principally polarized abelian varieties with CM by $\mathcal{O}$. The number of p.p.a.v. with CM by $\mathcal{O}$ is thus $\#\mathfrak{C}(\mathcal{O})$. Let us now compute the cardinality of $\#\mathfrak{C}(\mathcal{O})$. For this, we use the following sequence:

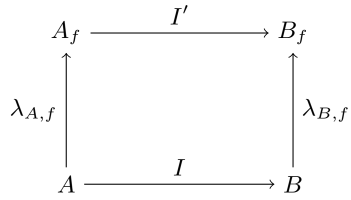
$$0 \to (\mathcal{O}_{K_0}^\times)^+/N_{K/K_0}(\mathcal{O}^\times) \to \mathfrak{C}(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O}) \xrightarrow{N_{K/K_0}} \mathrm{Cl}^+(K_0) \to 0.$$

For $\mathcal{O} = \mathcal{O}_K$, the exactness of this sequence is proven in [35] or [5]. When $\mathcal{O} \neq \mathcal{O}_K$, the proof follows closely the lines of the proof for the maximal order for the exacteness at $(\mathcal{O}_{K_0}^\times)^+/N_{K/K_0}(\mathcal{O}^\times)$, $\mathfrak{C}(\mathcal{O})$ and $\mathrm{Cl}(\mathcal{O})$. For the surjectiveness of the norm map, $N_{K/K_0} : \mathrm{Cl}(\mathcal{O}) \to \mathrm{Cl}^+(\mathcal{O}_{K_0})$ we use the fact that it writes as a composition of two surjective maps $\mathrm{Cl}(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O}_K) \to \mathrm{Cl}^+(\mathcal{O}_{K_0})$. □

In the remainder of this paper, unless stated otherwise, we consider principally polarized abelian surfaces with complex multiplication by an order $\mathcal{O}$ which has locally maximal real multiplication at $\mathfrak{l}$, i.e. $\mathcal{O}_{K_0,\mathfrak{l}} \subset \mathcal{O}_\mathfrak{l}$. In this case, we may extend the notion of $\mathfrak{l}$-isogeny. Indeed, if A has CM by such an order, then the isogenies with kernel a subgroup of order ℓ of $A[\mathfrak{l}]$ are called $\mathfrak{l}$-isogenies by extension.

Lemma 20. *Let A be an principally polarized abelian variety with locally maximal real multiplication at $\mathfrak{l}$. Let $I : A \to B$ be a an $\mathfrak{l}$-isogeny. Then B is principally polarized and has locally maximal real multiplication at $\mathfrak{l}$.*

Fig. 3.



Proof. Note first that $\ell\mathcal{O}_B \subset \mathcal{O}_A$. Hence, if f is the conductor of the real multiplication order of A and f' is the real multiplication order of B, we have that $f \mid \ell f'$. Since f is prime to ℓ, it follows that $f \mid f'$. Then following [33, §7.1, Prop. 7], there are $f\mathcal{O}_K$-transforms $\lambda_{A,f} : A \to A_f$ and $\lambda_{B,f} : B \to B_f$. We know that A_f is principally polarized and has RM by $\mathcal{O}_{K_0}$. Then there is a $\mathfrak{l}$-isogeny $I'_{\mathfrak{l}} : A_f \to B_f$ such that the diagram in Figure 3 is commutative.

Since I' is an $\mathfrak{l}$-isogeny starting from an p.p.a.v. with RM by $\mathcal{O}_{K_0}$, then it follows that $B_{\mathfrak{l}}$ has RM by $\mathcal{O}_{K_0}$. We conclude that $f\mathcal{O}_{K_0} \subset \mathrm{End}(B)$, hence B has locally maximal real multiplication at $\mathfrak{l}$. □

Let $I : A \to B$ be a separable isogeny between two p.p.a.v. defined over a perfect field. Denote by $\mathcal{O}_A = \mathrm{End}(A)$ and $\mathcal{O}_B = \mathrm{End}(B)$ and assume that these orders contain a suborder of $\mathcal{O}_{K_0}$ which is locally maximal at $\mathfrak{l}$. If $\mathcal{O}_A \simeq \mathcal{O}_B$, we say that the isogeny is *horizontal*. If not, then the localizations of the orders at $\mathfrak{l}$ lie on consecutive levels of the lattice given by Figure 2. If $(\mathcal{O}_B)_{\mathfrak{l}}$ is properly contained in $(\mathcal{O}_A)_{\mathfrak{l}}$, we say that the isogeny is *descending*. In the opposite situation, we say the isogeny is *ascending*.

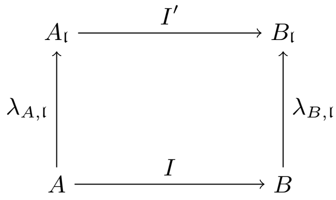
Associated to an ordinary principally polarized abelian surface defined over a perfect field and whose endomorphism ring is an order with locally maximal real multiplication at $\mathfrak{l}$, we define the $\mathfrak{l}$-*isogeny graph* to be the graph whose vertices are isomorphism classes of principally polarized abelian surfaces (A, ι, λ) with locally maximal real multiplication at $\mathfrak{l}$ (following the notation from Section 2.1) and whose edges are equivalence classes of $\mathfrak{l}$-isogenies between these surfaces. Note that by Lemma 16, we may identify an abelian variety to its dual and consider this as non-oriented graph. With this terminology, we state our main results regarding the structure of the $\mathfrak{l}$-isogeny graph for p.p.a.v defined over a number field.

Proposition 21. *Let A be a principally polarizable abelian surface defined over $\mathbb{C}$, with endomorphism ring an order $\mathcal{O}$ in a CM quartic field K different from $\mathbb{Q}(\zeta_5)$. Let $\mathfrak{l}$ be an ideal of prime norm ℓ in $\mathcal{O}_{K_0}$ and assume that $\mathcal{O}$ is locally maximal at $\mathfrak{l}$.*

1. *Assume that $\mathfrak{l}\mathcal{O}_K$ is prime with the conductor of $\mathcal{O}$, that we denote by $\mathfrak{f}$. Then we have:*
   - (a) *If $\mathfrak{l}$ splits into two ideals in $\mathcal{O}_K$, then there are, up to an isomorphism, exactly two horizontal $\mathfrak{l}$-isogenies starting from A and all the others are descending.*
   - (b) *If $\mathfrak{l}$ ramifies in $\mathcal{O}_K$, up to an isomorphism, there is exactly one horizontal $\mathfrak{l}$-isogeny starting from A and all the others are descending.*
   - (c) *If $\mathfrak{l}$ is inert in K, all $\ell + 1$ $\mathfrak{l}$-isogenies starting from A are descending.*
2. *If $\mathfrak{l}$ is not coprime to $\mathfrak{f}$, then up to an isomorphism, there is exactly one ascending $\mathfrak{l}$-isogeny and ℓ descending ones starting from A.*

Proof. (1) We treat first the case where $\mathcal{O}$ is an $\mathcal{O}_{K_0}$-order. If $\mathcal{O} = \mathcal{O}_K$, then the number of horizontal $\mathfrak{l}$-isogenies between p.p.a.v. equals the number of ideal classes in the Shimura class group of $\mathcal{O}_K$ given by ideals of norm ℓ (see [33, §7.5, Prop. 23] and [33, §14.4, Prop. 7]). Assume now that $\mathcal{O}$ is an order of conductor $\mathfrak{f}$ prime to $\mathfrak{l}$ and that there is an horizontal $\mathfrak{l}$-isogeny between abelian varieties defined over $\mathbb{C}$ having endomorphism ring $\mathcal{O}$. Following [33, §7.1, Prop. 7], there are $\mathfrak{f}$-transforms towards $\lambda_{A,\mathfrak{l}} : A \to A_{\mathfrak{l}}$ and $\lambda_{B,\mathfrak{l}} : B \to B_{\mathfrak{l}}$, where $A_{\mathfrak{l}}$ and $B_{\mathfrak{l}}$ have CM by $\mathcal{O}_K$. Then there is an isogeny $I' : A \to B$ such that the diagram in Figure 3 is commutative:

Fig. 4.



Then I' is an isogeny corresponding to a projective ideal $\mathfrak{l}_1$, lying over $\mathfrak{l}$ in $\mathcal{O}_K$. Since $\mathfrak{l}$ is prime to the conductor $\mathfrak{f}$, it follows that I corresponds to the ideal $\mathfrak{l}_1 \cap \mathcal{O}$ in $\mathcal{O}$. We conclude that the number of horizontal $\mathfrak{l}$-isogenies is 2 if $\mathfrak{l}$ is split in K, 1 if $\mathfrak{l}$ is ramified in K and 0 if $\mathfrak{l}$ is inert.

In order to count descending isogenies, we count the abelian surfaces lying at a given level in the graph (up to isomorphism). To do this, let $\mathcal{O}$ be the order of conductor $\mathfrak{f}$ and assume $\mathfrak{f}$ is prime to $\mathfrak{l}$. We use Lemma 19 to compute $\#\mathfrak{C}(\mathcal{O})$, and thus the number of p.p.a.v. with CM by $\mathcal{O}$, in terms of $\#\operatorname{Cl}(\mathcal{O})$.

To compute $\#\operatorname{Cl}(\mathcal{O})$, we will apply class number relations. More precisely, we have the exact sequence:

$$1 \to \mathcal{O}^\times \to \mathcal{O}_K^\times \to (\mathcal{O}_K/\mathfrak{f}\mathcal{O}_K)^\times/(\mathcal{O}/\mathfrak{f}\mathcal{O}_K)^\times \to \operatorname{Cl}(\mathcal{O}) \to \operatorname{Cl}(\mathcal{O}_K) \to 1. \tag{4}$$

Hence we have the formula for the class number

$$\#\operatorname{Cl}(\mathcal{O}) = \frac{\#\operatorname{Cl}(\mathcal{O}_K)}{[\mathcal{O}_K^\times : \mathcal{O}^\times]} \frac{\#(\mathcal{O}_K/\mathfrak{f}\mathcal{O}_K)^\times}{\#(\mathcal{O}/\mathfrak{f}\mathcal{O}_K)^\times}.$$

We have that $\mathcal{O}_K^\times = \mu_K \mathcal{O}_{K_0}^\times$, where $\mu_K = \{\pm 1\}$ (see [35, Lemma II.3.3]). Since $\mathcal{O}_{K_0} \subset \mathcal{O}$, it follows that $[\mathcal{O}_K^\times : \mathcal{O}^\times] = 1$.

We note that $\mathcal{O}/\mathfrak{f}\mathcal{O}_K \simeq \mathcal{O}_{K_0}/\mathfrak{f}\mathcal{O}_{K_0}$. We denote by N the norm of ideals in $\mathcal{O}_K$. Moreover, we have that

$$\#(\mathcal{O}_K/\mathfrak{f}O_K)^\times = N(\mathfrak{f}) \prod_{\mathfrak{p}|\mathfrak{f}} (1 - \frac{1}{N(\mathfrak{p})}), \tag{5}$$

where the ideals in the product are all prime ideals of $\mathcal{O}_K$, dividing the conductor. Let $\mathcal{O}_{\mathfrak{l}}$ be the $\mathcal{O}_{K_0}$-order of conductor $\mathfrak{l}\mathfrak{f}$. By writing the exact sequence (4) for the order $\mathcal{O}_{\mathfrak{l}}$, we obtain that

$$\begin{aligned}\#\operatorname{Cl}(\mathcal{O}_{\mathfrak{l}}) &= \#\operatorname{Cl}(\mathcal{O}) \frac{\#(\mathcal{O}/\mathfrak{f}\mathcal{O}_K)^\times}{\#(\mathcal{O}_{\mathfrak{l}}/\mathfrak{f}\mathfrak{l}\mathcal{O}_K)^\times} \cdot \frac{\#(\mathcal{O}_K/\mathfrak{f}\mathfrak{l}\mathcal{O}_K)^\times}{\#(\mathcal{O}_K/\mathfrak{f}\mathcal{O}_K)^\times}, \\ &= \#\operatorname{Cl}(\mathcal{O}) \frac{1}{\ell - 1} N(\mathfrak{l}) \prod_{\mathfrak{p}|\mathfrak{l}} (1 - \frac{1}{N(\mathfrak{p})}),\end{aligned}$$

where we used the fact that $\#(\mathcal{O}_l/\mathfrak{f}\mathfrak{l}\mathcal{O}_K)^\times = (\ell - 1) \times \#(\mathcal{O}/\mathfrak{f}\mathcal{O}_K)^\times$.

Hence there are $(\ell - 1) \cdot \#Cl(\mathcal{O})$ p.p.a.v. with CM by $\mathcal{O}_{\mathfrak{l}}$ when $\mathfrak{l}$ is split in K, $\ell \cdot \#Cl(\mathcal{O})$ when $\mathfrak{l}$ is ramified and $(\ell + 1) \cdot \#Cl(O)$ when $\mathfrak{l}$ is inert.

Moreover, by a simple symmetry argument, the number of descending isogenies is the same for every node lying at the $\mathcal{O}$-level. Indeed, let A and B be two nodes at the $\mathcal{O}$-level. Then there is a projective ideal $\mathfrak{a}$ in $\mathcal{O}_K$ (which may be taken to be prime with both $\mathfrak{l}$ and $\mathfrak{f}$), giving an horizontal isogeny $\lambda_{\mathfrak{a}} : A \to B$, corresponding to the ideal $\mathfrak{a} \cap \mathcal{O}$. Assume that A has a descending $\mathfrak{l}$-isogeny towards a variety $A_{\mathfrak{l}}$ lying at the $\mathcal{O}_{\mathfrak{l}}$-level $I_{\mathfrak{l}} : A \to A_{\mathfrak{l}}$. Note that there is a variety $B_{\mathfrak{l}}$ at the $\mathcal{O}_{\mathfrak{l}}$-level such that $\lambda'_{\mathfrak{a}} : A_{\mathfrak{l}} \to B_{\mathfrak{l}}$ is the horizontal isogeny corresponding to the ideal $\mathfrak{a} \cap \mathcal{O}_{\mathfrak{l}}$. Then there is a $\mathfrak{l}$-isogeny $I'_{\mathfrak{l}} : B \to B_{\mathfrak{l}}$ such that the following diagram is commutative:

$$\begin{array}{ccc} A & \xrightarrow{\lambda_{\mathfrak{a}}} & B \\ {\scriptstyle I_{\mathfrak{l}}}\downarrow & & \downarrow{\scriptstyle I'_{\mathfrak{l}}} \\ A_{\mathfrak{l}} & \xrightarrow{\lambda'_{\mathfrak{a}}} & B_{\mathfrak{l}} \end{array}$$

By comparing the number of abelian varieties at one level and the one below it and taking into account this symmetry, we conclude that all descending isogenies starting from each a.v. with CM by an order of conductor prime to $\mathfrak{l}$ reach non-isomorphic nodes. Moreover, each a.v. with CM by the order of conductor $\mathfrak{l}$ has exactly one ascending isogeny.

Finally, let $\mathcal{O}_0$ is an order in K_0 which is locally maximal at $\mathfrak{l}$ and let $\mathfrak{f}$ be the conductor of this order. Assume that $I : A \to B$ is an $\mathfrak{l}$-isogeny and that A and B have real multiplication by $\mathcal{O}_0$. Then there are $\mathfrak{f}$-transforms from A and B towards two abelian varieties with maximal real multiplication. Then one obtains an $\mathfrak{l}$-isogeny similar to the one in Figure 3 and I has the same direction (i.e. horizontal, ascending or descending) as I'.

(2) If $\mathfrak{l}$ divides $\mathfrak{f}$, we have

$$\#\,\mathrm{Cl}(\mathcal{O}_{\mathfrak{l}}) = \#\,\mathrm{Cl}(\mathcal{O}) \frac{\#(\mathcal{O}/\mathfrak{f}\mathcal{O}_K)^\times}{\#(\mathcal{O}_{\mathfrak{l}}/\mathfrak{f}\mathfrak{l}\mathcal{O}_K)^\times}.$$

By a similar argument to the one above, we conclude that the number of ascending isogenies is 1 and the number of descending isogenies is ℓ, for all p.p.a.v. with CM by the $\mathcal{O}_{K_0}$-order of conductor $\mathfrak{f}$. □

Remark 22. Note that Proposition 21 concerns also the case where ℓ is ramified in $\mathcal{O}_{K_0}$. The structure of the $\mathfrak{l}$-graph in this case is similar to the one in the split case.

Remark 23. We have excluded the case $K = \mathbb{Q}(\zeta_5)$ because in this case $\mathcal{O}_K^\times = \mu_K \mathcal{O}_{K_0}$, where μ_K is the group of roots of unity with order 10. However, a nearly equivalent statement may be given for the structure of the $\mathfrak{l}$-graph in this case. Only the degrees of vertices having CM by $\mathcal{O}_K$ are affected.

Let π be a q-Weil number in K, with q prime to ℓ. Suppose that in order to obtain a finite graph, we restrict to considering the subgraph of the $\mathfrak{l}$-graph whose vertices are p.p.a.v. A with endomorphism ring such that $\mathbb{Z}[\pi, \bar{\pi}] \subset \mathrm{End}(A)$ and whose edges are $\mathfrak{l}$-isogenies between these abelian varieties. By extension, in the remainder of this paper, we will call this subgraph the $\mathfrak{l}$-isogeny graph. From Proposition 21, we deduce that the structure of a connected component of the $\mathfrak{l}$-isogeny graph is exactly the one of an ℓ-isogeny graph between elliptic curves, called *volcano* [22,14]. By extension, in the remainder of this paper, we call this graph the $\mathfrak{l}$-isogeny graph. Furthermore, we show in the following Section that this graph is isomorphic to a graph whose edges are ordinary p.p.a.v. defined over $\mathbb{F}_q$ and with maximal real multiplication, and whose edges are equivalence classes of rational $\mathfrak{l}$-isogenies.

4 The structure of the real multiplication isogeny graph over finite fields

In this Section, we study the structure of the graph given by rational isogenies between principally polarizable abelian surfaces defined over a finite field, such that the corresponding endomorphism rings have locally maximal real multiplication at $\mathfrak{l}$. The endomorphism ring of a p.p.a.v. A over a finite field $\mathbb{F}_q$ ($q = p^n$) is an order in the quartic CM field K such that

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

where $\mathbb{Z}[\pi, \bar{\pi}]$ denotes the order generated by π, the Frobenius endomorphism and by $\bar{\pi}$, the Verschiebung. Moreover, the assumption that $\mathrm{End}(A)$ is an order with locally maximal real multiplication at $\mathfrak{l}$ implies that its localization contains $(\mathcal{O}_{K_0}\mathbb{Z}[\pi, \bar{\pi}])_{\mathfrak{l}}$.

4.1 The $\mathfrak{l}$-isogeny graph

The notion of $\mathfrak{l}$-isogeny defined in Definition 13 has been used so far for abelian surfaces defined over $\mathbb{C}$. We remark than whenever an abelian variety defined over a finite field $\mathbb{F}_q$ has endomorphism ring some order with locally maximal real multiplication at $\mathfrak{l}$, we may define the notion of $\mathfrak{l}$-isogeny exactly in the same way.

Proposition 24. *Let $\mathfrak{l}$ be a prime ideal of degree 1 over ℓ in $\mathcal{O}_{K_0}$, with $\ell \neq p$. Let A be a principally polarized ordinary abelian variety defined over a finite field $\mathbb{F}_q$ of characteristic p and having locally maximal real multiplication at $\mathfrak{l}$. Then a $\mathfrak{l}$-isogeny $I : A \to A'$ preserves real multiplication and the target variety A' is principally polarizable.*

Proof. We choose a canonical lift $\tilde{A}$ of A as defined in [26]. We may assume without loss of generality that this is defined over a number field L [8], such that A is isomorphic to the reduction of $\tilde{A}$ modulo a ideal $\mathfrak{P}$ lying over p in L. We have that $A[\mathfrak{l}] \simeq \tilde{A}[\mathfrak{l}]$ and the reductions of $\mathfrak{l}$-isogenies starting from $\tilde{A}$ give $\ell + 1$ (equivalence classes of) isogenies starting from A. Hence there is an isogeny $\tilde{I} : \tilde{A} \to A_1$ such that A_1 has good reduction $\pmod{\mathfrak{P}}$ and its reduction is isomorphic to A'. Since the reduction map $\mathrm{End}(A_1) \to \mathrm{End}(A')$ is injective, it follows that $\mathrm{End}(A')$ is an order with locally maximal real multiplication at $\mathfrak{l}$. By reducing polarizations given in Proposition 15 (see [10] for the reduction of polarizations), we deduce that if A is principally polarized, then A' is also principally polarized. □

The following result is a generalization of [23, Theorem 5 (ii) Chapter 13 §2]. The proof follows closely the lines of [23], but we reproduce it here for completeness.

Lemma 25. *Let A be an ordinary abelian variety defined over a finite field $\mathbb{F}_q$ of characteristic p. Then the prime p does not divide the conductor of the order $\mathcal{O} = \mathrm{End}(A)$.*

Proof. Denote by $\mathcal{O}_0$ the real multiplication order of A. Assume that p divides the conductor $\mathfrak{f}$ of $\mathcal{O}$. Let π be the Frobenius endomorphism of A. There is an element $\alpha \in \mathcal{O}_0$ such that

$$\pi = \alpha + c\eta,$$

with $c \in \mathfrak{f}$. Then we have

$$q\delta = \pi\bar{\pi} = \alpha^2 \pmod{\mathfrak{f}},$$

for some $\delta \in \mathcal{O}^\times$. This implies that p divides α in $\mathcal{O}_0$. Since A is ordinary and $A[p] \neq 0$, it follows that π kills points of order p in A. This is a contradiction, because π is purely inseparable. □

The following result is a generalization of [23, Theorem 12 (b) Chapter 13 §4].

Theorem 26. *Let A be an abelian variety defined over a number field L, with complex multiplication by an order $\mathcal{O}$. Let $\mathfrak{p}$ be a prime ideal in L over a prime number p, and assume that A has good reduction $A = \bar{A} \pmod{\mathfrak{p}}$ and that $\mathrm{End}_L(A) = \mathrm{End}(A)$. Let $\mathfrak{f}$ be the conductor of $\mathcal{O}$. Then if p does not divide $\mathfrak{f}$, the reduction map $\alpha \to \bar{\alpha}$ is an isomorphism of $\mathrm{End}(A)$ onto $\mathrm{End}(\bar{A})$.*

Proof. Let ℓ be a prime number. Let S_ℓ be the multiplicative monoid of positive integers prime to ℓ and let $\mathcal{O}_{(\ell)} = S_\ell^{-1}\mathcal{O}$ be the localization of $\mathcal{O}$ at ℓ. First, we know from general theory on the reduction of abelian varieties [33] that the reduction map

$$\mathrm{End}(A) \to \mathrm{End}(\bar{A})$$

is an injection. Since we have $T_\ell(A) \simeq T_\ell(\bar{A})$, for all $\ell \neq p$, it follows that $\mathrm{End}(A)$ and $\mathrm{End}(\bar{A})$ have the same localizations at ℓ, by [23, Ch.13 §3 Lemma 1] (whose generalization to abelian varieties is straightforward). On the other hand, because p does not divide the conductor $\mathfrak{f}$, we have that $\mathcal{O}_{K,(p)} \simeq \mathcal{O}_{(p)}$, which means that $\mathcal{O}_{(p)}$ is integrally closed. It follows that it will coincide with the localization at p of $\mathrm{End}(\bar{A})$. We conclude that $\mathrm{End}(A) \simeq \mathrm{End}(\bar{A})$ because they have the same localization at all primes. □

With this in hand, we show that there is a graph isomorphism between an $\mathfrak{l}$-isogeny graph between p.p.a.v. defined over finite fields and a certain graph whose vertices are p.p.a.v defined over a number field.

Corollary 27. *Let $\mathcal{G}$ be an $\mathfrak{l}$-isogeny graph with vertices principally polarized abelian surfaces defined over $\mathbb{F}_q$ and whose endomorphism ring is an order in K, with locally maximal real multiplication at $\mathfrak{l}$. Let π be a q-Weil number, giving the Frobenius endomorphism for any of the abelian surfaces in $\mathcal{G}$. Then $\mathcal{G}$ is isomorphic to a graph $\mathcal{G}'$, whose vertices are isomorphism classes of principally polarized abelian surfaces defined over a number field L and having CM by an order whose localization at $\mathfrak{l}$ contains $(\mathcal{O}_{K_0}[\pi,\bar{\pi}])_{\mathfrak{l}}$, and whose edges are equivalence classes of $\mathfrak{l}$-isogenies between these surfaces.*

Proof. We choose A_1 and A_2 two abelian surfaces corresponding to vertices in the graph $\mathcal{G}$ connected by an edge $I : A_1 \to A_2$ of kernel G a cyclic group in $A_1[\mathfrak{l}]$. We take $\tilde{A}_1$ the canonical lift of A_1. As explained in the proof of Lemma 24, we may assume that there is a number field L and a prime $\mathfrak{p}$ lying over p in L such that A_1 is isomorphic to $\tilde{A}_1 \pmod{\mathfrak{p}}$ and that $\mathrm{End}(\tilde{A}_1)$ is defined over L. We denote by $\mathcal{G}'$ the $\mathfrak{l}$-isogeny graph whose vertices are p.p.a.v defined over L whose endomorphism ring localized at $\mathfrak{l}$ contains $(\mathcal{O}_{K_0}[\pi,\bar{\pi}])_{\mathfrak{l}}$. We will show that the graph $\mathcal{G}$ is isomorphic to $\mathcal{G}'$. There are $\ell+1$ cyclic groups in $\tilde{A}_1[\mathfrak{l}]$ and we denote by $\tilde{G}$ the one such that the reduction of points gives an isomorphism $\tilde{G} \simeq G$. We consider the $\mathfrak{l}$-isogeny of kernel $\tilde{G}$, $I' : \tilde{A}_1 \to A_2'$. Then $A_2' \pmod{\mathfrak{p}} = A_2$ and we know that $\mathrm{End}(A_2') \to \mathrm{End}(A_2)$ is an injection. Since p does not divide the conductor of $\mathrm{End}(\tilde{A}_1)$ (because by Lemma 25 it does not divide the conductor of A_1), it follows p cannot divide the conductor of A_2'. Hence by Theorem 26 it follows that A_2' is isomorphic to the canonical lift of A_2. ☐

We are now interested in determining the field of definition of $\mathfrak{l}$-isogenies starting from a p.p.a.v A. For that, we need several definitions.

Let $\mathfrak{l}$ be an ideal in $\mathcal{O}_{K_0}$ and α a generator of this ideal. Let $\mathcal{O}$ be an order of K with locally maximal real multiplication at $\mathfrak{l}$ and let $\theta \in \mathcal{O}$. We define the $\mathfrak{l}$-adic exponent of θ in $\mathcal{O}$ with respect to $\mathcal{O}_{K_0}$ as

$$\nu_{\mathfrak{l},\mathcal{O}}(\theta) := \max_{m\geq 0}\{m : \theta_{\mathfrak{l}} \in \mathcal{O}_{K_0,\mathfrak{l}} + \mathfrak{l}^m\mathcal{O}_{\mathfrak{l}}\},$$

where $\theta_{\mathfrak{l}}$ is the image of θ via the homomorphism $\mathcal{O} \to \mathcal{O}_{\mathfrak{l}}$. Recall that for a p.p.a.v A with maximal real multiplication, we are interested (by Lemma 10) in computing the $\mathfrak{l}$-adic valuation of the conductor of the endomorphism ring $\mathcal{O}_A$. We remark that it suffices to determine $\nu_{\mathfrak{l},\mathcal{O}_A}(\pi)$. Indeed, we have $\mathcal{O}_{A,\mathfrak{l}} = \mathcal{O}_{K_0,\mathfrak{l}} + \mathfrak{f}_{\eta,\mathcal{O}_A}\eta_{\mathfrak{l}}$ and

$$\nu_{\mathfrak{l}}(\mathfrak{f}_{\eta,\mathcal{O}_A}) = \nu_{\mathfrak{l},\mathcal{O}_K}(\pi) - \nu_{\mathfrak{l},\mathcal{O}_A}(\pi). \tag{6}$$

In the remainder of this paper, we denote by $\nu_{\mathfrak{l},A}(\pi) := \nu_{\mathfrak{l},\mathcal{O}_A}(\pi)$.

Example 28. Let H be the genus-2 curve given by the equation

$$y^2 = 31x^6 + 79x^5 + 109x^4 + 130x^3 + 62x^2 + 164x + 56$$

defined over $\mathbb{F}_{211}$. The Jacobian J has complex multiplication by a quartic CM field K with defining equation X^4+81X^2+1181. The real subfield is $K_0 = \mathbb{Q}(\sqrt{1837})$, and has class number 1. The endomorphism ring of J contains the real maximal order $\mathcal{O}_{K_0}$. In the real subfield K_0, we have $3 = \alpha_1\alpha_2$, with $\alpha_1 = \frac{43+\sqrt{1837}}{2}$ and α_2 its conjugate. We have that $\nu_{(\alpha_i),\mathcal{O}_K}(\pi) = 1$, for $i = 1, 2$, where π has relative norm 211 in $\mathcal{O}_K$.

Since $\mathfrak{l}$ is principal in the real multiplication order of A, it follows that $A[\mathfrak{l}]$ is the kernel of an endomorphism. Since A is ordinary, all endomorphisms are $\mathbb{F}_q$-rational. Consequently, we have that $\pi(A[\mathfrak{l}^n]) \subset A[\mathfrak{l}^n]$, for $n \geq 0$. The following result relates the computation of the $\mathfrak{l}$-adic exponent of π to that of the matrix of the Frobenius on the $\mathfrak{l}$-torsion.

Proposition 29. *Let A be a p.p.a.v. defined over a finite field $\mathbb{F}_q$ and having CM by an order with locally maximal real multiplication at $\mathfrak{l}$. Then the largest integer n such that the Frobenius matrix on $A[\mathfrak{l}^n]$ is of the form*

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \bmod \ell^n \tag{7}$$

is $\nu_{\mathfrak{l},A}(\pi)$.

Proof. First we assume that $\nu_{\mathfrak{l},A}(\pi) = n$ and we show that the matrix of the Frobenius has the form given by equation (7). Let D be an element of $A[\mathfrak{l}^n]$. Then π acts on D as an element of $\mathcal{O}_{K_0}/\mathfrak{l}^n \simeq \mathbb{Z}/\ell^n\mathbb{Z}$. Hence $\pi(D) = \lambda D$ for some $\lambda \in \mathbb{Z}$.

Conversely, suppose that the matrix of the Frobenius on $A[\mathfrak{l}^n]$ is of the form (7) and take α a real multiplication endomorphism such that $\alpha(D) = \lambda D$, for all $D \in A[\mathfrak{l}^n]$ (Since any real multiplication endomorphism acts on $A[\mathfrak{l}^n]$ as λI_2, it is easy to see that such an α exists). Then $\pi - \alpha$ is zero on $A[\mathfrak{l}^n]$, which implies that this is an element of $\mathfrak{l}^n\mathcal{O}$ (by [13, Proposition 7]). □

Remark 30. Let $\mathbb{F}_{q^k}$ be the smallest field extension such that $A[\mathfrak{l}^n]$ is defined over $\mathbb{F}_{q^k}$. A natural consequence of Proposition 29 is that the cyclic subgroups of $A[\mathfrak{l}^n]$ are rational (i.e. stable under the action of $Gal(\mathbb{F}_{q^k}/\mathbb{F}_q)$) if and only if $\nu_{\mathfrak{l},A}(\pi) \geq n$. In particular, the $\ell + 1$ isogenies whose kernels are cyclic subgroups of $A[\mathfrak{l}]$ are rational if and only if $\nu_{\mathfrak{l},A}(\pi) > 0$.

By Proposition 21 and Corollary 27 we get the following structure of connected components of the non-oriented $\mathfrak{l}$-isogeny graph over finite fields.

1. At each level, if $\nu_{\mathfrak{l},A}(\pi) > 0$, there are $\ell + 1$ rational isogenies with kernel a cyclic subgroup of $A[\mathfrak{l}]$.
2. If $\mathfrak{l}$ is split in $\mathcal{O}_{K_0}$ then there are two horizontal $\mathfrak{l}$-isogenies at all levels such that the corresponding order is locally maximal at $\mathfrak{l}$ (i.e. $\mathcal{O}_{\mathfrak{l}} \simeq \mathcal{O}_{K,\mathfrak{l}}$). At every intermediary level (i.e. $\nu_{\mathfrak{l},A}(\pi) > 0$), there are $\ell + 1$ rational $\mathfrak{l}$-isogenies: an ascending one and ℓ descending ones.
3. If $\nu_{\mathfrak{l},A}(\pi) = 0$, then no smaller order (whose conductor has larger $\mathfrak{l}$-valuation) contains π. There are no rational descending $\mathfrak{l}$-isogeny, and there is exactly one ascending $\mathfrak{l}$-isogeny.

We will show that all rational isogenies of degree ℓ preserving locally maximal real multiplication at $\mathfrak{l}$ are $\mathfrak{l}$-isogenies, for some ideal $\mathfrak{l}$ of degree 1.

Lemma 31. *Let A and B be two abelian varieties defined and isogenous over $\mathbb{F}_q$ and denote by $\mathcal{O}_A$ and $\mathcal{O}_B$ the corresponding endomorphism rings. Let $\mathfrak{l}$ be an ideal of norm ℓ in $\mathcal{O}_{K_0}$. Assume that the $\mathfrak{l}$-adic valuations of the conductors of $\mathcal{O}_A$ and $\mathcal{O}_B$ are different. Then for any isogeny $I : A \to B$ defined over $\mathbb{F}_q$ we have* $\operatorname{Ker} I \cap A[\mathfrak{l}] \neq \{0\}$.

Proof. We prove the contrapositive statement. Assume that there is an isogeny $I : A \to B$ defined over $\mathbb{F}_q$ with $\operatorname{Ker} I \cap A[\mathfrak{l}] = \{0\}$. We then have that $I(A[\mathfrak{l}^n]) = B[\mathfrak{l}^n]$, for all $n \geq 1$. Since $\pi_B \circ I = I \circ \pi_A$, it follows that the $\mathfrak{l}$-adic exponents $\nu_{\mathfrak{l},\mathcal{O}_A}(\pi_A)$ and $\nu_{\mathfrak{l},\mathcal{O}_B}(\pi_B)$ are equal. By equation (6), it follows that the $\mathfrak{l}$-adic valuations of the conductors of endomorphism rings of A and B are equal. □

The converse of Lemma 31 does not hold, as it is possible for an $\mathfrak{l}$-isogeny to have a kernel within $A[\mathfrak{l}]$, and yet leave the $\mathfrak{l}$-valuation of the conductor of the endomorphism ring unchanged. The following statement is a converse to Proposition 14.

Proposition 32. *Let ℓ be an odd prime number, split in K_0. All cyclic isogenies of degree ℓ between principally polarizable abelian varieties defined over $\mathbb{F}_q$ having locally maximal real multiplication at ℓ are $\mathfrak{l}$-isogenies, for some degree 1 ideal $\mathfrak{l}$ in $\mathcal{O}_{K_0}$.*

Proof. Let $\ell\mathcal{O}_{K_0} = \mathfrak{l}_1\mathfrak{l}_2$. Let $I : A \to B$ be a rational degree-ℓ isogeny which preserves the real multiplication $\mathcal{O}_{K_0}$. The endomorphism rings $\mathcal{O}_A$ and $\mathcal{O}_B$ are orders whose localizations are located in the lattice of orders described by Figure 2. First, by [5, Section 8], we have that either $\ell\mathcal{O}_A \subset \mathcal{O}_B$, and $\ell\mathcal{O}_B \subset \mathcal{O}_A$. Hence the two orders lie either on the same level, either on consecutive levels in the lattice of orders. If $\mathcal{O}_A$ and $\mathcal{O}_B$ lie on consecutive levels, then there is an ideal $\mathfrak{l}$ of norm ℓ in $\mathcal{O}_{K_0}$ such that the $\mathfrak{l}$-adic valuation of the conductors is different. By Lemma 31, it follows that the kernel of any cyclic ℓ-isogeny between A and B is a cyclic subgroup of $A[\mathfrak{l}]$.

Assume now that $\mathcal{O}_A$ and $\mathcal{O}_B$ are $_{K_0}$-orders and that they lie at the same level in the lattice of orders. Then by using the Shimura class group action, an horizontal isogeny between A and B corresponds to an invertible ideal $\mathfrak{u}$ of $\mathcal{O}_A$. Moreover we have $\mathfrak{u}\bar{\mathfrak{u}} = \mathfrak{l}$, with $\mathfrak{l}$ an ideal of norm ℓ in $\mathcal{O}_{K_0}$. Hence it is an $\mathfrak{l}$-isogeny, for some ideal $\mathfrak{l}$. Secondly, if $\mathcal{O}_A$ and $\mathcal{O}_B$ contain a suborder of $\mathcal{O}_{K_0}$ of conductor f prime to ℓ, then we consider $f\mathcal{O}_K$-transforms towards abelian varieties with RM by $\mathcal{O}_{K_0}$ and reduce the problem to the first case.

Finally, if the two orders lie at the same level and are not isomorphic, then both the $\mathfrak{l}_1$-adic and $\mathfrak{l}_2$-adic valuations of the corresponding conductors are different. It then follows that the kernel of any isogeny from A to B contains a subgroup of $A[\mathfrak{l}_1]$ and one of $A[\mathfrak{l}_2]$. This is not possible if the isogeny is cyclic. □

4.2 The ℓ-isogeny graph

Associated to an ordinary principally polarizable abelian surface defined over $\mathbb{F}_q$ and having locally maximal real multiplication at ℓ, we define the $\{\mathfrak{l}_1, \mathfrak{l}_2\}$-*isogeny graph* to be the labeled graph whose edges are all equivalence classes of $\mathfrak{l}_1$- or $\mathfrak{l}_2$-isogenies, and whose vertices are isomorphism classes of principally polarizable abelian surfaces over $\mathbb{F}_q$ reached (transitively) by such isogenies. An edge is labeled as $\mathfrak{l}_1$ or $\mathfrak{l}_2$, if it corresponds to a $\mathfrak{l}_1$-isogeny or to a $\mathfrak{l}_2$-isogeny, respectively.

A natural consequence of Proposition 32 is that over finite fields, the $\{\mathfrak{l}_1, \mathfrak{l}_2\}$-isogeny graph is the graph of all isogenies of degree ℓ between principally polarizable abelian surfaces having locally maximal real multiplication at ℓ.

Note that the $\{\mathfrak{l}_1, \mathfrak{l}_2\}$-isogeny graph can be seen, by the results above, as the union of two graphs which share all their characteristics with genus one isogeny volcanoes. In particular, the generalization of the top rim of the volcano turns into a torus if both $\mathfrak{l}_1$ and $\mathfrak{l}_2$ split. If only one of them splits, the top rim is a circle, and if both are inert we have a single vertex corresponding to a maximal endomorphism ring (since all cyclic isogenies departing from that abelian variety increase both the $\mathfrak{l}_1$- and the $\mathfrak{l}_2$-valuation of the conductor of the endomorphism ring).

MAGMA experiments. Let A be a p.p.a.v. defined over $\mathbb{F}_q$ with maximal real multiplication at ℓ. We do not have formulas for computing cyclic isogenies over finite fields (Section 6 works around this difficulty for the computation of endomorphism rings). Instead, we experiment over the complex numbers, and use the graph isomorphism between the $\mathfrak{l}$-isogeny graph having A as a vertex and the graph of its canonical lift.

To draw the graph corresponding to Example 28, it is straightforward to compute the period matrix Ω associated to a complex analytic torus $\mathbb{C}^2/\Lambda_1 + \tau\Lambda_2$, and compute a representative in the fundamental domain for the action of Sp_4 using Gottschling's reduction algorithm[1].

All this can be done symbolically, as the matrix Ω is defined over the reflex field K^r. As a consequence, we may compute isogenies of type (3) and follow the edges of the graph of isogenies between complex abelian surfaces having complex multiplication by an order $\mathcal{O}$ containing $\mathcal{O}_{K_0}[\pi, \bar{\pi}]$. The exploration terminates when outgoing edges from each node have been visited. This yields Figure 5. Violet and orange edges in Figure 5 are α_1 and α_2-isogenies, respectively. Note that since α_1 and α_2 are totally positive, all varieties in the graph are principally polarized.

[1] By Gottschling's reduction algorithm, we refer to the reduction algorithm as stated in e.g. [12, chap. 6] or [36, §6.3], and which relies crucially on Gottschling's work [17] for defining the 19 matrices which come into play

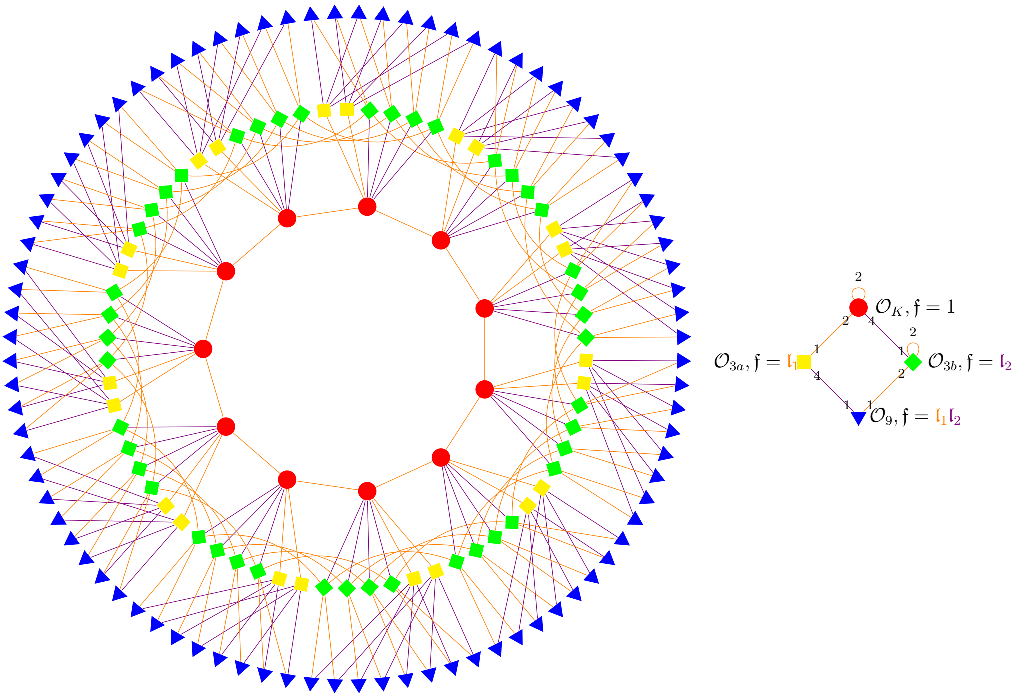


Fig. 5. Graph of ℓ-isogenies preserving real multiplication, for $\ell = 3$, K defined by $\alpha^4+81\alpha^2+1181$, and $\mathcal{O}_{K_0}[\pi]$ defined by the Weil number $\pi = \frac{1}{2}(\alpha^2 + 3\alpha + 45)$, with $p = \mathrm{Norm}_{K/K_0}\,\pi = 211$.

In a computational perspective, we are interested in ℓ-isogenies, which are accessible to computation using the algorithms developed by [9]. Our description of the $\mathfrak{l}_1$- and $\mathfrak{l}_2$-isogenies is key to understanding the ℓ-isogenies due to the following result.

Proposition 33. *Let $\ell \geq 3$ be a prime number such that $\ell\mathcal{O}_{K_0} = \mathfrak{l}_1\mathfrak{l}_2$. Then all ℓ-isogenies between p.p.a.v. defined over $\mathbb{F}_q$ and having locally maximal real multiplication at ℓ are a composition of an $\mathfrak{l}_1$-isogeny with an $\mathfrak{l}_2$-isogeny.*

Proof. Let A and B be two p.p.a.v. defined over $\mathbb{F}_q$ and let $I : A \to B$ be an ℓ-isogeny preserving the real multiplication order, which is locally maximal at ℓ. We denote by $\mathcal{O}_A = \mathrm{End}(A)$ and $\mathcal{O}_B = \mathrm{End}(B)$. If the endomorphism rings are both isomorphic to an order $\mathcal{O}_{K_0}$-order denoted by $\mathcal{O}$, then the isogeny corresponds, under the action of the Shimura class group $\mathfrak{C}(\mathcal{O})$, to an ideal class $\mathfrak{a}$ such that $\mathfrak{a}\bar{\mathfrak{a}} = \ell\mathcal{O}$. It follows that both $\mathfrak{l}_1$ and $\mathfrak{l}_2$ split in $\mathcal{O}$. Let $\mathfrak{l}_{i,j}$, $i, j \in \{1, 2\}$, be such that $\mathfrak{l}_{i,1}\mathfrak{l}_{i,2} = \mathfrak{l}_i$. Then, we may assume that the isogeny I corresponds to the ideal $\mathfrak{l}_{1,1}\mathfrak{l}_{2,1}$ under the action of the Shimura class group. We conclude that I is a composition of an $\mathfrak{l}_1$-isogeny with an $\mathfrak{l}_2$-isogeny.
If $\mathcal{O}_A$ and $\mathcal{O}_B$ are isomorphic to an order in K which contains a suborder of $\mathcal{O}_{K_0}$ of conductor f prime to ℓ, then the result follows by choosing $f\mathcal{O}_K$-transforms and reducing the problem to finding a horizontal isogeny between two p.p.a.v. with CM by $\mathcal{O}_K$, as in the proof of Proposition 21.
Assume now that $\mathcal{O}_A$ and $\mathcal{O}_B$ are not isomorphic. This implies that $\nu_{\mathfrak{l},\mathcal{O}_A}(\pi)$ and $\nu_{\mathfrak{l},\mathcal{O}_B}(\pi)$ differ for some $\mathfrak{l}$, and we may without loss of generality assume $\mathfrak{l} = \mathfrak{l}_1$. By considering the dual isogeny $\hat{I}$ instead of I, we may also assume $\nu_{\mathfrak{l}_1,\mathcal{O}_A}(\pi) > \nu_{\mathfrak{l}_1,\mathcal{O}_B}(\pi)$.
Let $n = \nu_{\mathfrak{l}_1,\mathcal{O}_A}(\pi)$. We then have that any cyclic subgroup of $A[\mathfrak{l}_1^n]$ is rational. By Proposition 29, there is a cyclic subgroup of $B[\mathfrak{l}_1^n]$ which is not rational. Since $I(A[\mathfrak{l}_1^n]) \subset B[\mathfrak{l}_1^n]$ and the isogeny I is rational, it follows that $\mathrm{Ker}\, I$ contains an element $D_1 \in A[\mathfrak{l}_1]$. Let $I_1 : A \to C$ be the isogeny whose kernel is generated by D_1. This isogeny preserves the real multiplication and is an $\mathfrak{l}_1$-isogeny

(Proposition 32). By [13, Prop 7], there is an isogeny $I_2 : C \to B$ such that $I = I_2 \circ I_1$. Obviously, I_2 also preserves real multiplication.
Let now $\langle D_1, D_2 \rangle = \operatorname{Ker} I$. Since $\operatorname{Ker} I \subset A[\mathfrak{l}_1] + A[\mathfrak{l}_2]$, we may write $D_2 = D_{2,1} + D_{2,2}$ with $D_{2,i} \in A[\mathfrak{l}_i]$. As $\operatorname{Ker} I$ is Weil-isotropic, we may choose D_2 so that $D_{2,1} = 0$, whence $D_2 \in A[\mathfrak{l}_2]$. We have $I_1(D_2) \neq 0$, so that I_2 is an $\mathfrak{l}_2$-isogeny. Note that given the $D_2 \in A[\mathfrak{l}_2]$ which we have just defined, we may also consider the $\mathfrak{l}_2$-isogeny $I'_2 : A \to C'$ with kernel $\langle D_2 \rangle$, and similarly define the $\mathfrak{l}_1$-isogeny I'_1 which is such that $I = I'_1 \circ I'_2$.

□

The proposition above leads us to consider properties of ℓ-isogenies with regard to the $\mathfrak{l}_i$-isogenies they are composed of. Let $I = I_1 \circ I_2$ be an ℓ-isogeny, with I_i an $\mathfrak{l}_i$-isogeny (for $i = 1, 2$). We say that I is $\mathfrak{l}_1$-ascending (respectively $\mathfrak{l}_1$-horizontal, $\mathfrak{l}_1$-descending) if the $\mathfrak{l}_1$-isogeny I_1 is ascending (respectively horizontal, descending). This is well-defined, since by Lemma 31 there is no interaction of I_1 with the $\mathfrak{l}_2$-valuation of the conductor of the endomorphism ring.

Proposition 33 is a way to interpret Figure 1 as derived from Figure 5 as follows. Vertices are kept, and we use as edges all compositions of one $\mathfrak{l}_1$-isogeny and one $\mathfrak{l}_2$-isogeny. This fact will serve as a basis for our algorithms for computing endomorphism rings, detailed in Section 6.

5 Pairings on the real multiplication isogeny graph

Let $\ell\mathcal{O}_{K_0} = \mathfrak{l}_1\mathfrak{l}_2$. In this Section, $\mathfrak{l}$ denotes any of the ideals $\mathfrak{l}_1, \mathfrak{l}_2$. Let A be a p.p.a.v. defined over $\mathbb{F}_q$, with complex multiplication by an order which is locally maximal at $\mathfrak{l}$.

We relate some properties of the Tate pairing to the isomorphism class of the endomorphism ring of the abelian variety, by giving a similar result to the one of [20] for genus-1 isogeny graphs. More precisely, we show that the nondegeneracy of the Tate pairing restricted to the kernel of an $\mathfrak{l}$-isogeny determines the type of the isogeny in the graph, at least when $\nu_{\mathfrak{l}}(\pi)$ is below some bound. This result is then exploited to efficiently navigate in isogeny graphs.

Let r be the smallest integer such that $A[\mathfrak{l}] \subset A(\mathbb{F}_{q^r})$. Let n be the largest integer such that $A[\mathfrak{l}^n] \subset A[\mathbb{F}_{q^r}]$. We define $k_{\mathfrak{l},A}$ to be

$$k_{\mathfrak{l},A} = \max_{P \in A[\mathfrak{l}^n]} \{k \mid T_{\ell^n}(P,P) \in \mu_{\ell^k} \backslash \mu_{\ell^{k-1}}\}.$$

Definition 34. *Let G be a cyclic group of $A[\mathfrak{l}^n]$. We say that the Tate pairing is $k_{\mathfrak{l},A}$-non-degenerate (or simply non-degenerate) on $G \times G$ if its restriction*

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

is surjective. Otherwise, we say that the Tate pairing is $k_{\mathfrak{l},A}$-degenerate (or simply degenerate) on $G \times G$.

The following result shows that computing the $\mathfrak{l}$-adic valuation of π is equivalent to computing $k_{\mathfrak{l},A}$.

Proposition 35. *Let r be the smallest integer such that $A[\mathfrak{l}] \subset A(\mathbb{F}_{q^r})$. Let n be the largest integer such that $A[\mathfrak{l}^n] \subset A[\mathbb{F}_{q^r}]$. Then if $\nu_{\mathfrak{l},A}(\pi^r) < 2n$, we have*

$$k_{\mathfrak{l},A} = 2n - \nu_{\mathfrak{l},A}(\pi^r).$$

Proof. Let Q_1, Q_2 form a basis for $A[\mathfrak{l}^{2n}]$. Then $\pi^r(Q_i) = \sum a_{ij} Q_j$, for $i, j = 1, 2$. We have

$$T_{\ell^n}(\ell^n Q_i, \ell^n Q_i) = W_{\ell^{2n}}(\pi(Q_i) - Q_i, Q_i) = W_{\ell^{2n}}(Q_k, Q_i)^{a_{ik}} \in \mu_{\ell^{k_{\mathfrak{l},A}}},$$

with $k \equiv i + 1 \pmod 2$. By the non-degeneracy of the Weil pairing, this implies $a_{12} \equiv a_{21} \equiv 0 \pmod{\ell^{2n - k_{\mathfrak{l},A}}}$. Moreover, the antisymmetry condition on the Weil pairing says that

$$T_{\ell^n}(\ell^n Q_1, \ell^n Q_2) T_{\ell^n}(\ell^n Q_2, \ell^n Q_1) \in \mu_{\ell^{k_{\mathfrak{l},A}}}.$$

Since $T_{\ell^n}(\ell^n Q_i, \ell^n Q_j) = W_{\ell^{2n}}(Q_i, Q_j)^{a_{jj}-1}$, for $i \neq j$, we have that

$$W_{\ell^{2n}}(Q_1, Q_2)^{a_{11}-1} W_{\ell^{2n}}(Q_2, Q_1)^{a_{22}-1} = W_{\ell^{2n}}(Q_1, Q_2)^{a_{11}-a_{22}} \in \mu_{\ell^{k_{\mathfrak{l},A}}}.$$

We conclude that $\ell^{2n-k_{\mathfrak{l},A}}$ divides all of a_{12}, a_{21}, and $a_{11} - a_{22}$. By Proposition 29, this implies that $2n - k_{\mathfrak{l},A} \leq \nu_{\mathfrak{l},A}(\pi^r)$.

Conversely, let $k = 2n - \nu_{\mathfrak{l},A}(\pi^r)$. We know (by Proposition 29) that $\pi = \lambda I_2 + \ell^{2n-k} A$, for $A \in M_2(\mathbb{Z})$ and for some λ coprime to ℓ. Then for $P \in A[\mathfrak{l}^n]$ and $\bar{P}$ such that $\ell^n \bar{P} = P$, we have $T_{\ell^n}(P, P) = W_{\ell^{2n}}(\bar{P}, \lambda \bar{P} + A(\ell^{2n-k}\bar{P})) \in \mu_{\ell^k}$. Hence $k \geq k_{\mathfrak{l},A}$ and this concludes the proof. □

From this proposition, it follows that if $\nu_{\mathfrak{l},A}(\pi) > 2n$, the self-pairings of all kernels of $\mathfrak{l}$-isogenies are degenerate. At a certain level in the $\mathfrak{l}$-isogeny graph, when $\nu_{\mathfrak{l},A}(\pi) < 2n$, there is at least one kernel with non-degenerate pairing (i.e. $k_{\mathfrak{l},A} = 1$). Following the terminology of [19], we call this level *the second stability level*. As we descend to the floor, $k_{\mathfrak{l},A}$ increases. The *first stability level* is the level at which $k_{\mathfrak{l},A}$ equals n.

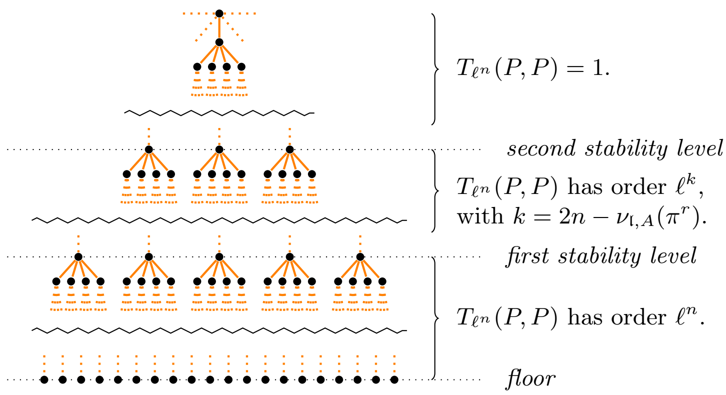


Fig. 6. Stability levels in the $\mathfrak{l}$-graph

We now show that from a computational point of view, we can use the Tate pairing to orient ourselves in the $\mathfrak{l}$-isogeny graph. More precisely, cyclic subgroups of the $\mathfrak{l}$-torsion with degenerate self-pairing correspond to kernels of ascending and horizontal isogenies, while subgroups with non-degenerate self pairing are kernels of descending isogenies. Before proving this result, we need the following lemma.

Lemma 36. *If $k_{\mathfrak{l},A} > 0$, then there are at most two subgroups of order ℓ in $A[\mathfrak{l}^n]$ such that points in these subgroups have degenerate self-pairing.*

Proof. We use the shorthand notation $\lambda_{U,V} = \log(T_{\ell^n}(U, V))$ for U, V any two $\mathfrak{l}^n$-torsion points, and where log is a discrete logarithm function in μ_{ℓ^n}.

Suppose that P and Q are two linearly independent $\mathfrak{l}^n$-torsion points. Since all $\mathfrak{l}^n$-torsion points R can be expressed as $R = aP + bQ$, bilinearity of the ℓ^n-Tate pairing gives

$$\lambda_{R,R} = a^2 \lambda_{P,P} + ab\,(\lambda_{P,Q} + \lambda_{Q,P}) + b^2 \lambda_{Q,Q} \pmod{\ell^n},$$

We now claim that the polynomial

$$S(a, b) = a^2 \lambda_{P,P} + ab\,(\lambda_{P,Q} + \lambda_{Q,P}) + b^2 \lambda_{Q,Q} \tag{8}$$

is identically zero modulo $\ell^{n-k_{\mathfrak{l},A}-1}$ and nonzero modulo $\ell^{n-k_{\mathfrak{l},A}}$. Indeed, if it were identically zero modulo ℓ^{n-k}, with $k < k_{\mathfrak{l},A}$, then we would have $T_{\ell^n}(R, R) \in \mu_{\ell^k}$, which contradicts the definition of $k_{\mathfrak{l},A}$. If it were different from zero modulo $\ell^{n-k_{\mathfrak{l},A}-1}$, then there would be $R \in A[\mathfrak{l}^n]$ such that $T_{\ell^n}(R,R)$ is an $\ell^{k_{\mathfrak{l},A}+1}$-th primitive root of unity, again contradicting the definition of $k_{\mathfrak{l},A}$.

Points with degenerate self-pairing are roots of L. Hence there are at most two subgroups of order ℓ with degenerate self-pairing. □

In the remainder of this paper, we define by

$$S_{\mathfrak{l},A}(a,b) = a^2\lambda_{P,P} + ab(\lambda_{P,Q} + \lambda_{Q,P}) + b^2\lambda_{Q,Q}$$

any polynomial defined by a basis $\{P,Q\}$ of $A[\mathfrak{l}^n]$ in a manner similar to the proof of Lemma 36, and using the same notation λ.

Theorem 37. *Let A be an p.p.a.v. defined over a finite field $\mathbb{F}_q$ and having locally maximal real multiplication at $\mathfrak{l}$. Let P be an $\mathfrak{l}$-torsion point and let r be the smallest integer such that $A[\mathfrak{l}] \subset A(\mathbb{F}_{q^r})$. Let n be the largest integer such that $A[\mathfrak{l}^n] \subset A[\mathbb{F}_{q^r}]$. Assume that $k_{\mathfrak{l},A} > 0$. Consider G a subgroup of $A[\mathfrak{l}^n]$ such that $\ell^{n-1}G$ is the subgroup generated by P. Then the isogeny of kernel P is descending if and only if the Tate pairing is non-degenerate on G. It is horizontal or ascending otherwise.*

Proof. We assume $n > 1$ and that $k_{\mathfrak{l},A} > 1$. Otherwise, we consider A defined over and extension field of $\mathbb{F}_{q^r}$ and apply [18, Lemma 6]. Let $I : A \to A'$ the isogeny of kernel generated by P.

Assume first that P has non-degenerate self-pairing. Let $\bar{P} \in G$ such that $\ell^{n-1}\bar{P} = P$. Then by [30, Lemma 16.2c] and Lemma 17, we have

$$T_{\ell^{n-1}}(I(\bar{P}), \alpha(I(\bar{P}))) \in \mu_{\ell^{k_{\mathfrak{l},A}-1}} \backslash \mu_{\ell^{k_{\mathfrak{l},A}-2}},$$

where α is a generator of the principal ideal $\mathfrak{l}'$ such that $\mathfrak{l}\mathfrak{l}' = \ell\mathcal{O}_{K_0}$. Since $\mathcal{O}_{K_0}/\alpha\mathcal{O}_{K_0} \simeq \mathbb{Z}/\ell\mathbb{Z}$, then for any $R \in A'[\mathfrak{l}^n]$, we have $\alpha(R) = \lambda R$, for some $\lambda \in \mathbb{Z}/\ell\mathbb{Z}$. Hence we have

$$T_{\ell^{n-1}}(I(\bar{P}), I(\bar{P})) \in \mu_{\ell^{k_{\mathfrak{l},A}-1}} \backslash \mu_{\ell^{k_{\mathfrak{l},A}-2}},$$

There are two possibilities. Either $A'[\mathfrak{l}^n]$ is not defined over $\mathbb{F}_{q^r}$, or $A'[\mathfrak{l}^n]$ is defined over $\mathbb{F}_{q^r}$. In the first case, we have $\nu_{\mathfrak{l},A'}(\pi^r) < \nu_{\mathfrak{l},A}(\pi^r)$ and the isogeny is descending.

Assume now that $A'[\mathfrak{l}^n]$ is defined over $\mathbb{F}_{q^r}$. Then let P_1 such that $I(\bar{P}) = \ell P_1$. Then

$$T_{\ell^n}(P_1, P_1)) \in \mu_{\ell^{k_{\mathfrak{l},A}+1}} \backslash \mu_{\ell^{k_{\mathfrak{l},A}}}.$$

By using Proposition 35, it follows that $\nu_{\mathfrak{l},A'}(\pi^r) < \nu_{\mathfrak{l},A}(\pi^r)$. Hence the isogeny is descending.

Suppose now that the point P has degenerate self-pairing and that the isogeny I is descending. Since there are at most 2 points in $A[\mathfrak{l}^n]$ with degenerate self-pairing, there is at least one point in $A[\mathfrak{l}^n]$ with non-degenerate self-pairing. This point, that we denote by Q, generates the kernel of a descending isogeny $I' : A \to A''$ such that $\mathrm{End}(A') \simeq \mathrm{End}(A'')$. We assume first that $A'[\mathfrak{l}^n]$ and $A''[\mathfrak{l}^n]$ are not defined over $\mathbb{F}_{q^r}$. Then we have

$$T_{\ell^{n-1}}(I(\bar{P}), I(\bar{P}))) \in \mu_{\ell^{k_{\mathfrak{l},A}-2}}, \quad T_{\ell^{n-1}}(\ell I(\bar{Q}), \ell(I(\bar{Q}))) \in \mu_{\ell^{k_{\mathfrak{l},A}-3}}$$
$$T_{\ell^{n-1}}(\ell I'(\bar{P}), \ell I'(\bar{P})) \in \mu_{\ell^{k_{\mathfrak{l},A}-4}}, T_{\ell^{n-1}}(I'(\bar{Q}), I'(\bar{Q}))) \in \mu_{\ell^{k_{\mathfrak{l},A}-1}} \backslash \mu_{\ell^{k_{\mathfrak{l}}-2}}$$

Hence $k_{\mathfrak{l},A'} \neq k_{\mathfrak{l},A''}$, which is a contradiction. The case where $A'[\mathfrak{l}^n]$ and $A''[\mathfrak{l}^n]$ are defined over $\mathbb{F}_{q^r}$ is similar. □

6 Endomorphism ring computation - a depth-first algorithm

We keep the same setting and notations. In particular, ℓ is a fixed odd prime, and we assume that $\ell\mathcal{O}_{K_0} = \mathfrak{l}_1\mathfrak{l}_2$. We take J to be the Jacobian of a genus 2 curve defined over $\mathbb{F}_q$, which will allow us to compute the Tate pairing efficiently (as explained in Section 2.3). We intend to compute the endomorphism ring of J, with prior knowledge of the Zeta function of J, and the fact that $\mathrm{End}(J)_\ell$ contains $\mathcal{O}_{K_0,\ell}$. We note that this property holds trivially in the case where $\mathbb{Z}[\pi,\bar{\pi}]_\ell$ contains $\mathcal{O}_{K_0,\ell}$, although this is not a necessary condition for the algorithm here to work.

6.1 Description of the algorithm

A consequence of Proposition 33 is that there are at most $(\ell+1)(\ell+1)$ rational ℓ-isogenies preserving the real multiplication. Since we can compute ℓ-isogenies over finite fields [9,3], we use this result to give an algorithm for computing $\nu_{\mathfrak{l},J}(\pi)$, and determine endomorphism rings locally at ℓ, by placing them properly in the order lattice as represented in Figure 2.

We define u_i to be the smallest integer such that $\pi^{u_i} - 1 \in \mathfrak{l}_i \mathcal{O}_K$, and u the smallest integer such that $\pi^u - 1 \in \ell\mathcal{O}_K$ (we have $u = \mathrm{lcm}(u_1, u_2)$). The value of u depends naturally on the splitting of ℓ in K (see [15, Prop. 6.2]). As the algorithm proceeds, the walk on the isogeny graph considers Jacobians over the extension field $\mathbb{F}_{p^u}$.

Idea of the algorithm. As noticed by Lemma 10, we can achieve our goal by considering *separately* the position of the endomorphism ring within the order lattice with respect to $\mathfrak{l}_1$ first, and then with respect to $\mathfrak{l}_2$. The algorithm below is in effect run twice.

Each move in the isogeny graph corresponds to taking an ℓ-isogeny, which is a computationally accessible object. In our prospect to understand the position of the endomorphism ring with respect to $\mathfrak{l}_1$ in Figure 2, we shall not consider what happens with respect to $\mathfrak{l}_2$, and vice-versa. Our input for computing an ℓ-isogeny is a Weil-isotropic kernel. Because we are interested in isogenies preserving the real multiplication, this entails that we consider kernels of the form $K_1 + K_2$, with K_i, $i = \overline{1, 2}$, a cyclic subgroup of $J[\mathfrak{l}_i]$. By Proposition 18, such a group is Weil-isotropic. There are up to $(\ell+1)^2$ such subgroups.

Let $\mathfrak{l}$ be either $\mathfrak{l}_1$ or $\mathfrak{l}_2$. The algorithm computes $\nu_{\mathfrak{l},J}(\pi)$ in two stages.

Our algorithm stops when the floor of rationality has been hit in $\mathfrak{l}$, i.e. the only rational cyclic group in $J[\mathfrak{l}]$ is the one generating the kernel of the ascending $\mathfrak{l}$-isogeny. If $(u, \ell) = 1$, one may prove that testing rationality for the isogenies is equivalent to $J[\mathfrak{l}] \subset J(\mathbb{F}_{q^u})$. Otherwise, in order to test rationality for the isogeny at each step in the algorithm, one has to check whether the kernel of the isogeny is $\mathbb{F}_q$-rational.

Step 1. The idea is to walk the isogeny graph until we reach a Jacobian which is on the second stability level or below (which might already be the case, in which case we proceed to Step 2). If the Jacobian J is above the second stability level, we need to construct several chains of ℓ-isogenies, not backtracking with respect to $\mathfrak{l}$, to make sure at least one of them is descending in the $\mathfrak{l}$-direction. This proceeds exactly as in [14]. The number of chains depends on the number of horizontal isogenies and thus on the splitting of $\mathfrak{l}$ in K (due to the action of the Shimura class group). If $\mathfrak{l}$ is split, one needs three isogeny chains to ensure that one path is descending.

If an isogeny in the chain is descending, then the path continues descending, assuming the isogeny walk does not backtrack with respect to $\mathfrak{l}$ (this aspect is discussed further below). We are done constructing a chain when we have reached the second stability level for $\mathfrak{l}$, which can be checked by computing self-pairing of appropriate ℓ^n-torsion points. The length of the shortest path gives the correct level difference between the second stability level and the Jacobian J. The pseudocode for this step is given in Algorithm 1.

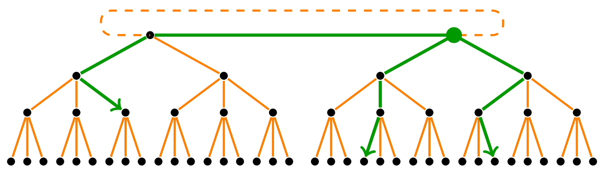


Fig. 7. At least one in three non-backtracking paths has minimum distance to a given level.

Figure 7 represents for $\ell = 3$ a situation where only three non-backtracking paths can guarantee that at least one of them is consistently descending.

Step 2. We now assume that J is on the second stability level or below, with respect to $\mathfrak{l}$. We construct a non-backtracking path of ℓ-isogenies, which are consistently descending with respect to $\mathfrak{l}$. In virtue of Theorem 37, this can be achieved by picking Weil-isotropic kernels whose $\mathfrak{l}$-part (which is cyclic) correspond to a non-degenerate self-pairing $T_{\ell^n}(P, P)$. We stop when we have reached the floor of rationality in $\mathfrak{l}$, at which point the valuation $\nu_{\mathfrak{l},J}(\pi)$ is obtained.

Note that at each step taken in the graph, if $J[\mathfrak{l}']$ (where $\mathfrak{l}'$ is the other ideal) is not rational, then we ascend in the $\mathfrak{l}'$-direction, in order to compute an ℓ-isogeny. As said above, this has no impact on the consideration of what happens with respect to $\mathfrak{l}$. This step is summarized in Algorithm 2.

Ensuring isogeny walks are not backtracking As said above, ensuring that the isogeny walk in Step 2 is not backtracking is essentially guaranteed by Theorem 37. Things are more subtle for Step 1. Let J_1 be a starting Jacobian, and $I : J_1 \to J_2$ an ℓ-isogeny whose kernel is $V \subset J[\ell]$. Recall that there are at most $(\ell + 1)^2$ Weil-isotropic kernels of the form $K_1 + K_2$ within $J_2[\mathfrak{l}_1] + J_2[\mathfrak{l}_2]$ for candidate isogenies $I' : J_2 \to J_1$. All such isogenies whose kernel has the same component on $J_2[\mathfrak{l}_1]$ as the dual isogeny $\hat{I}$ are backtracking with respect to $\mathfrak{l}_1$ in the isogeny graph. One must therefore identify the dual isogeny $\hat{I}$ and its kernel. Since $\hat{I}$ is such that $\hat{I} \circ I = [\ell]$, we have that $\operatorname{Ker} \hat{I} = I(J_1[\ell])$. If computing $I(J_1[\ell])$ is possible[2], this solves the issue. If not, then enumerating all possible kernels until the dual isogeny is identified is possible, albeit slower.

Algorithm 1 Computing the endomorphism ring: Step 1

INPUT: A Jacobian J of a genus-2 curve defined over $\mathbb{F}_q$ with CM by a field K, and α such that $\mathfrak{l} = \alpha\mathcal{O}_K$ divides $\ell\mathcal{O}_K$. We require that J is above the second stability level with respect to $\mathfrak{l}$.

OUTPUT: A Jacobian J' on or below the second stability level with respect to $\mathfrak{l}$, and the distance from J to this Jacobian.

Let π be the Frobenius endomorphism of J and u be the smallest integer s.t. $\pi^u - 1 \equiv 0 \pmod{\ell\mathcal{O}_K}$.
Compute a basis of $J[\ell^\infty](\mathbb{F}_{q^u})$.
Compute $a, b \in \mathbb{Q}$ such that $\alpha = a + b(\pi + \bar{\pi})$.
Let n be the largest integer such that $J[\mathfrak{l}^n] \subset J(\mathbb{F}_{q^u})$.
$J_1 \leftarrow J$, $J_2 \leftarrow J$, $J_3 \leftarrow J$.
$\kappa_1 \leftarrow \{0\}$, $\kappa_2 \leftarrow \{0\}$, $\kappa_3 \leftarrow \{0\}$.
length $\leftarrow 0$.
while true do
  length $\leftarrow$ length $+ 1$.
  for all i=1,2,3 **do**
    Compute the matrix of π in $J_i[\ell^\infty](\mathbb{F}_{q^u})$.
    Compute bases for $J_i[\mathfrak{l}](\mathbb{F}_{q^u})$ and $J_i[\mathfrak{l}'](\mathbb{F}_{q^u})$ using $\alpha = a + b(\pi + \bar{\pi})$.
    Pick at random $P_i \in J_i[\mathfrak{l}](\mathbb{F}_{q^u})$ such that $P_i \notin \kappa_i$.
    Pick at random $P_i' \in J_i[\mathfrak{l}'](\mathbb{F}_{q^u})$.
    Compute the ℓ-isogeny $I : J_i \to J_i' = J_i/\langle P_i, P_i' \rangle$.
    $\kappa_i \leftarrow I(J[\mathfrak{l}])$; $J_i \leftarrow J_i'$.
    Compute $S_{\mathfrak{l},J}$.
    if $S_{\mathfrak{l},J} \neq 0$ **then**
      return length.
    end if
  end for
end while

[2] Computing isogenous Jacobians by isogenies is easier than computing images of divisors. The `avisogenies` software [3] performs the former since its inception, and the latter in its development version, as of 2014.

Algorithm 2 Computing the endomorphism ring: Step 2

INPUT: A Jacobian J of a genus-2 curve defined over $\mathbb{F}_q$ with CM by a field, and α such that $\mathfrak{l} = \alpha\mathcal{O}_K$ divides $\ell\mathcal{O}_K$. We require that J is on or below the second stability level with respect to $\mathfrak{l}$ (see Algorithm 1).

OUTPUT: The $\mathfrak{l}$-distance from J to the floor.

```
length ← 0.
while true do
    Let π be the Frobenius of J and let u the smallest integer s.t. π^u − 1 ≡ 0 (mod ℓO_K) and compute
    a basis of J[ℓ^∞](F_{q^u}).
    Let n the largest integer such that J[l^n] ⊂ J(F_{q^u}).
    if n = 0 then
        return length.
    end if
    Compute the matrix of π in J_i[ℓ^∞](F_{q^u}).
    Let l' = ℓ/l. Compute bases for J_i[l](F_{q^u}) and J_i[l'](F_{q^u})
    Consider P_1, P_2 a basis of J[l^n](F_{q^u})
    Compute S_{l,J} and take x_1, x_2 ∈ F_ℓ such that S_{l,J}(x_1, x_2) ≠ 0.
    P ← ℓ^{n−1}(x_1 P_1 + x_1 P_2).
    Pick at random P'_i ∈ J_i[l'](F_{q^u}).
    Compute the ℓ-isogeny I : J' ← J/⟨P, P'⟩
    J ← J'.
    length ← length + 1.
end while
```

6.2 Complexity analysis

In this Section, we give a complexity analysis of Algorithms 1 and 2 and compare their performance to that of the Eisenträger-Lauter algorithm for computing the endomorphism ring locally at ℓ, for small ℓ. If ℓ is large, one should use Bisson's algorithm [2]. Computing a bound on ℓ for which one should switch between the two algorithms and a full complexity analysis of the algorithm for determining the endomorphism ring completely is beyond the scope of this paper.

The Eisenträger-Lauter algorithm For completeness, we briefly recall the Eisenträger-Lauter algorithm [13]. For a fixed order $\mathcal{O}$ in the lattice of orders of K, the algorithm tests whether $\mathcal{O} \subset \mathrm{End}(J)$. This is done by computing a $\mathbb{Z}$-basis of $\mathcal{O}$ and checking whether its elements are endomorphisms of J or not. In order to test if $\alpha \in \mathcal{O}$ is an endomorphism, we write

$$\alpha = \frac{a_0 + a_1\pi + a_2\pi^2 + a_3\pi^3}{N},$$

with a_i integers whose greatest common divisor is coprime to N (N is the smallest integer such that $N\alpha \in \mathbb{Z}[\pi]$). Using [13, Prop. 7], we get $\alpha \in \mathrm{End}(J)$ if and only if $\sum_i a_i\pi^i$ acts as zero on the N-torsion.

Freeman and Lauter [15] work locally modulo prime divisors of N. For all orders such that $\mathbb{Z}[\pi] \subset \mathcal{O} \subset \mathcal{O}_K$, the denominators N considered are divisors of $[\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]]$ (see [15, Lemma 3.3 and Corollary 3.6]). Moreover, Freeman and Lauter show that if N factors as $\ell_1^{d_1}\ell_2^{d_2}\ldots\ell_r^{d_r}$, it suffices to check if

$$\frac{a_0 + a_1\pi + a_2\pi^2 + a_3\pi^3}{\ell_i^{d_i}},$$

is an endomorphism, for all i. The advantage of working locally is that instead of working over the extension field generated by the coordinates of the N-torsion points, we may work over the field of definition of the $\ell_i^{d_i}$-torsion, for every prime factor ℓ_i separately. Nevertheless, it should be noted that the exponent d_i can be as large as the ℓ_i-valuation of the conductor $[\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]]$.

We now set some notations for giving the complexity of algorithms from Section 6 as well as that of the Eisenträger-Lauter algorithm. We consider the complexity for one odd prime ℓ

dividing $[\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]]$, and assume that $(\ell, p) = 1$. Following the notation in Section 4, we denote $h_i = \nu_{\mathfrak{l}_i, \mathcal{O}_K}(\pi)$ for $i = 1, 2$. It follows that $\nu_\ell([\mathcal{O}_K : \mathcal{O}_{K_0}[\pi, \bar{\pi}]]) = h_1 + h_2$. The order $\mathbb{Z}[\pi, \bar{\pi}]$ might be smaller than $\mathcal{O}_{K_0}[\pi, \bar{\pi}]$, thus we denote $h_0 = \nu_\ell([\mathcal{O}_{K_0}[\pi, \bar{\pi}] : \mathbb{Z}[\pi, \bar{\pi}]])$. Note though that for most practical uses of our algorithm, we expect to gain knowledge that $\mathrm{End}(J)$ has maximal real multiplication from the fact that $\mathbb{Z}[\pi, \bar{\pi}]$ is an $\mathcal{O}_{K_0}$-order itself, which implies $h_0 = 0$. It makes sense to neglect h_0 in this case. Finally, we let as before u be the smallest integer such that $\pi^u \equiv 1 \mod \ell\mathcal{O}_K$, so that the ℓ-torsion on J is defined over $\mathbb{F}_{q^u}$. According to [15, Prop. 6.2], we have $u \in O(\ell^2)$ since ℓ splits in K_0.

We now give the complexity of the algorithm from Section 6. First we compute a basis of the "ℓ^∞-torsion over $\mathbb{F}_{q^u}$", i.e. the ℓ-Sylow subgroup of $J(\mathbb{F}_{q^u})$, which corresponds to $J[\ell^n](\mathbb{F}_{q^u})$ for some integer n. We assume that the zeta function of J and the factorization of $\#J(\mathbb{F}_{q^u}) = \ell^s m$ are given. We denote by $M(u)$ the number of a multiplications in $\mathbb{F}_q$ needed to perform one multiplication in the extension field of degree u. The computation of the Sylow subgroup basis costs $O(M(u)(u \log q + n\ell^2))$ operations in $\mathbb{F}_q$, as described in [4, §3].

Then we compute the matrix of the Frobenius on the ℓ-torsion. Using this matrix, we write down the matrices of α_1 and α_2 in terms of the the matrix of $\pi + \bar{\pi}$. Finally, computing $J[\mathfrak{l}_i]$ for $i = 1, 2$ is just linear algebra and has negligible cost. For each i, the cost of computing the Tate pairing is related to the integers r_i and n_i as defined in Proposition 35. We bound these by $r_i \leq u$, and $n_i \leq n$. Computing the Tate pairing thus costs $O(M(u)(n \log \ell + u \log q))$ operations in $\mathbb{F}_q$, where the first term is the cost of Miller's algorithm and the second one is the cost for the final exponentiation.

The cost of computing an ℓ-isogeny using the algorithm of Cosset and Robert [9] is $O(M(u)\ell^4)$ operations in $\mathbb{F}_q$. We conclude that the cost of Algorithms 1 and 2 is

$$\mathrm{cost}_{\text{algorithms } 1+2} = O(\max(h_1, h_2) M(u)(u \log q + n\ell^2 + \ell^4)).$$

The complexity of Freeman and Lauter's algorithm is dominated by the cost of computing the ℓ-Sylow subgroup of the Jacobian defined over the extension field containing the ℓ^d-torsion, where d is bounded by $\nu_\ell([\mathcal{O}_K : \mathbb{Z}[\pi]]) = \nu_\ell([\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]]) = h_0 + h_1 + h_2$ (recall that ℓ and π are coprime). The degree of this extension field is $u\ell^{d-1}$ by [15, Prop. 6.3]. This leads to

$$\mathrm{cost}_{\mathrm{EL}} = O(M(u\ell^{d-1})(u\ell^{d-1} \log q + (n + d - 1)\ell^2)).$$

Freeman and Lauter	This work (Algorithms 1 and 2)
$O(M(u\ell^{d-1})(u\ell^{d-1} \log q + (n + d - 1)\ell^2))$	$O(\max(h_1, h_2) M(u)(u \log q + n\ell^2 + \ell^4))$

Table 1. Cost for computing the endomorphism ring locally at ℓ; we have $u = O(\ell^2)$, $d \leq h_0 + h_1 + h_2$, and $h_0 = 0$ is a typical condition for this work to apply

.

6.3 Practical experiments

Let J be the Jacobian of the hyperelliptic curve defined by

$$y^2 = 17422020 + 847562x + 37917221x^2 + 268754x^3 + 4882157x^4 + 14143796x^5 + 50949756x^6$$

over $\mathbb{F}_p$, with $p = 53050573$. The curve has complex multiplication by $\mathcal{O}_K$, with $K = \mathbb{Q}(\zeta)$, defined by the equation $\zeta^4 + 175\zeta^2 + 6925 = 0$. A Weil number for this Jacobian, as well as the corresponding characteristic polynomial, are given as follows:

$$\pi = \frac{1}{15}(45\zeta^3 + 422\zeta^2 + 14940\zeta + 79450),$$
$$\pi^4 - s_1\pi^3 + s_2\pi^2 - s_1 p\pi + p^2 = 0, \text{ with } s_1 = 11340, \; s_2 = 135934954.$$

The real multiplication subfield K_0 has class number 1, and $\ell = 3$ splits in K_0 as $3 = \alpha_1\alpha_2$. The corresponding valuations of the Frobenius are $\nu_{\alpha_1,\mathcal{O}_K}(\pi) = 10$ and $\nu_{\alpha_2,\mathcal{O}_K}(\pi) = 2$. The analogue to Figure 2 is thus a lattice of 20 possible orders to choose from in order to determine $\mathrm{End}(J)$.

Our algorithm computes the 3-torsion group, which is defined over $\mathbb{F}_{p^2}$. Note that in contrast, the Eisenträger-Lauter algorithm computes the 3^{10}-torsion group, defined over $\mathbb{F}_{p^{39366}}$.

We report experimental results of our implementation, using Magma 2.20-6 and `avisogenies` 0.6, on a Intel Core i5-4570 CPU with clock frequency 3.2 GHz. Our computation of $\mathrm{End}(J)$ with Algorithms 1 and 2 goes as follows. Computation shows that the Tate pairing is degenerate on $J[\mathfrak{l}_1]$. We thus use Algorithm 1 to find a shortest path from J, not backtracking with respect to $\mathfrak{l}_1$, and reaching a Jacobian on or above the second stability level. This path is made of ℓ-isogenies defined over $\mathbb{F}_p$, and computed with `avisogenies` from their kernels (here, only what happens with respect to $\mathfrak{l}_1$ is interesting). Such a path with length 3 is found in 20 seconds, where most of the time (15 seconds) is spent on ensuring that the isogeny walks are non-backtracking (see remark on page 23). From there, a consistently descending path of length 5 down to the floor is constructed using Algorithm 2 in 3 seconds. This leads to $\nu_{\mathfrak{l}_1,J}(\pi) = 8$. As for $\mathfrak{l}_2$, the Jacobian J is below the second stability level, so Algorithm 2 applies, and finds $\nu_{\mathfrak{l}_2,J}(\pi) = 1$ in 1 second. In total, the computation $\mathrm{End}(J)$ in this example takes 24 seconds.

7 Conclusion

We have described the structure of the degree-ℓ isogeny graph between abelian surfaces with maximal real multiplication. From a computational point of view, we exploited the structure of the graph to describe an algorithm computing locally at ℓ the endomorphism ring of an abelian surface with maximal real multiplication.

In this work we used the assumption that K_0 has class number 1 to give the structure of the lattice of orders with locally maximal real multiplication at ℓ and also assumed that the ideal $\mathfrak{l}$ is trivial in the narrow class group of K_0. This allowed us to exhibit an $\mathfrak{l}$-isogeny graph between principally polarized abelian varieties.

For a generalization of this work the case where K_0 has class number greater the reader is referred to [6,27]. In particular, the assumption that $\mathfrak{l}$ is trivial in the narrow class group is left out in [6]. This leads to an $\mathfrak{l}$-isogeny graph between polarized abelian varieties, belonging to different polarization classes.

Further research is needed to extend these results to a general setting and compute endomorphism ring in the case where ℓ divides $[\mathcal{O}_{K_0} : \mathbb{Z}[\pi + \bar{\pi}]]$. Our belief is that the right approach to follow is first to determine the real multiplication order $\mathcal{O}_0$ and secondly to use an algorithm similar to ours, exploiting the structure of the isogeny graph between principally polarized abelian variety with real multiplication by $\mathcal{O}_0$.

The reader should also note recent results and ongoing work on the computation of $\mathfrak{l}$-isogenies (via modular polynomials [28,27] and [11]). It would be interesting to compare the performance of algorithms navigating into the $\mathfrak{l}$-isogeny graphs against that of navigating in ℓ-isogeny graphs, in order to see whether our methods for computing endomorphism rings can be improved.

References

1. C. Birkenhake and H. Lange. *Complex abelian varieties*, volume 302 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, second edition, 2004.
2. G. Bisson. Computing endomorphism rings of abelian varieties of dimension two. `http://eprint.iacr.org/2012/525`.
3. G. Bisson, R. Cosset, and D. Robert. Avisogenies. `http://avisogenies.gforge.inria.fr/`.
4. G. Bisson, R. Cosset, and D. Robert. On the practical computation of isogenies of jacobian surfaces. Manuscript in preparation, available within the source code of [3].
5. R. Bröker, D. Gruenewald, and K. Lauter. Explicit CM theory for level 2-structures on abelian surfaces. *Algebra & Number Theory*, 5(4):495–528, 2011.

6. E. Hunter Brooks, D. Jetchev, and B. Wesolowski. Isogeny graphs of ordinary abelian varieties. *Research in Number Theory*, 3(1):28, 2017.
7. J. Buchmann and H. Lenstra. Approximating rings of integers in number fields. *Journal de Théorie des Nombres de Bordeaux*, 6:221–260, 1994.
8. C. Chai, B. Conrad, and F. Oort. *Complex Multiplication and lifting problems*, volume 195 of *Mathematical Surveys and Monographs*. American Mathematical Society, 2014.
9. R. Cosset and D. Robert. Computing (ℓ, ℓ)-isogenies in polynomial time on jacobians of genus 2 curves. *Mathematics of Computation*, 2013.
10. P. Deligne. Variétés abéliennes ordinaires sur un corps fini. *Inventiones math.*, pages 238–243, 1969.
11. A. Dudeanu, D. Jetchev, D. Robert, and M. Vuille. Cyclic isogenies for abelian varieties with real multiplication, 2017.
12. R. Dupont. *Moyenne arithmético-géométrique, suites de Borchardt et applications*. Thèse, École Polytechnique, 2006. `www.lix.polytechnique.fr/Labo/Regis.Dupont/these_soutenance.pdf`.
13. K. Eisenträger and K. Lauter. A CRT algorithm for constructing genus 2 curves over finite fields. In *Arithmetic, Geometry and Coding Theory (AGCT -10), Séminaires et Congrès 21*, pages 161–176. Société Mathématique de France, 2009.
14. M. Fouquet and F. Morain. Isogeny volcanoes and the SEA algorithm. In C. Fieker and D. R. Kohel, editors, *ANTS-V*, volume 2369 of *Lecture Notes in Computer Science*, pages 276–291. Springer, 2002.
15. D. Freeman and K. Lauter. Computing endomorphism rings of jacobians of genus 2 curves. In *Symposium on Algebraic Geometry and its Applications, Tahiti*, 2006.
16. E. Goren and K. Lauter. The distance between superspecial abelian varieties with real multiplication. *Journal of Number Theory*, 129(6):1562–1578, 2009.
17. E. Gottschling. Explizite Bestimmung der Randflächen des Fundamentalbereiches der Modulgruppe zweiten Grades. *Math. Ann.*, 138:103–124, 1959.
18. S. Ionica. Pairing-based methods for genus 2 jacobians with maximal endomorphism ring. *Journal of Number Theory*, 133(11):3755–3770, 2013.
19. S. Ionica and A. Joux. Another approach to pairing computation in Edwards coordinates. In D. R. Chowdhury, V. Rijmen, and A. Das, editors, *Progress in Cryptography- Indocrypt 2008*, volume 5365 of *Lecture Notes in Computer Science*, pages 400–413. Springer, 2008.
20. S. Ionica and A. Joux. Pairing the volcano. *Mathematics of Computation*, 82:581–603, 2013.
21. J.S.Milne. Abelian varieties. `http://www.jmilne.org/math/CourseNotes/av.html`.
22. D. Kohel. *Endomorphism rings of elliptic curves over finite fields.* PhD thesis, University of California, Berkeley, 1996.
23. S. Lang. *Elliptic functions*, volume 112 of *Graduate Texts in Mathematics*. Springer, 1987.
24. S. Lichtenbaum. Duality theorems for curves over p-adic fields. *Invent.Math.7*, pages 120–136, 1969.
25. D. Lubicz and D. Robert. Computing isogenies between abelian varieties. *Compositio Mathematica*, 2012.
26. J. Lubin, J.-P. Serre, and J. Tate. Elliptic curves and formal groups. Lecture Notes at Woods Hole Summer Institute, 1964. `http://www.ma.utexas.edu/users/voloch/lst.html`.
27. C. Martindale. *Isogeny graphs, modular polynomials and applications.* PhD thesis, University of Leiden, 2018.
28. E. Milio and D. Robert. Modular polynomials on hilbert surfaces, 2017.
29. V. Miller. The Weil pairing, and its efficient calculation. *Journal of Cryptology*, 17(4):235–261, September 2004.
30. J. Milne. Abelian Varieties. `http://www.jmilne.org/math/CourseNotes/av.html`.
31. D. Robert. Isogeny graphs in dimension 2. `http://www.normalesup.org/~robert/pro/publications/slides/2014-12-Caen-Isogenies.pdf`, 2014. Cryptography Seminar, Caen.
32. S. L. Schmoyer. The Triviality and Nontriviality of Tate-Lichtenbaum Self-Pairings on Jacobians of curves, 2006. `http://www-users.math.umd.edu/~schmoyer/`.
33. G. Shimura. *Abelian varieties with complex multiplication and modular functions.* Princeton Mathematical Series. Princeton University Press, 1998.
34. A.-M. Spallek. *Kurven von Geschelcht 2 und ihre Anwendung in Public Key Kryptosystemen.* PhD thesis, Institut für Experimentelle Mathematik, Universität GH Essen, 1994.
35. M. Streng. *Complex multiplication of abelian surfaces.* PhD thesis, Universiteit Leiden, 2010.
36. M. Streng. Computing Igusa class polynomials. *Math. Comp.*, 83(285):275–309, 2014.

A Appendix: additional example

We consider the quartic CM field K with defining equation $X^4 + 81X^2 + 1181$. The real subfield is $K_0 = \mathbb{Q}(\sqrt{1837})$, and has class number 1. In the real subfield K_0, we have $3 = \alpha_1\alpha_2$, with $\alpha_1 = \frac{43+\sqrt{1837}}{2}$ and α_2 its conjugate. We consider a Weil number π of relative norm 85201 in $\mathcal{O}_K$. We have that $\nu_{\alpha_1}(\mathfrak{f}_{\mathbb{Z}[\pi,\bar{\pi}]}) = 2$ and $\nu_{\alpha_2}(\mathfrak{f}_{\mathbb{Z}[\pi,\bar{\pi}]}) = 1$. Note that $\mathfrak{l}_1$ is inert and $\mathfrak{l}_2$ is split in K. Our implementation with Magma produced the graph in Figure 8.

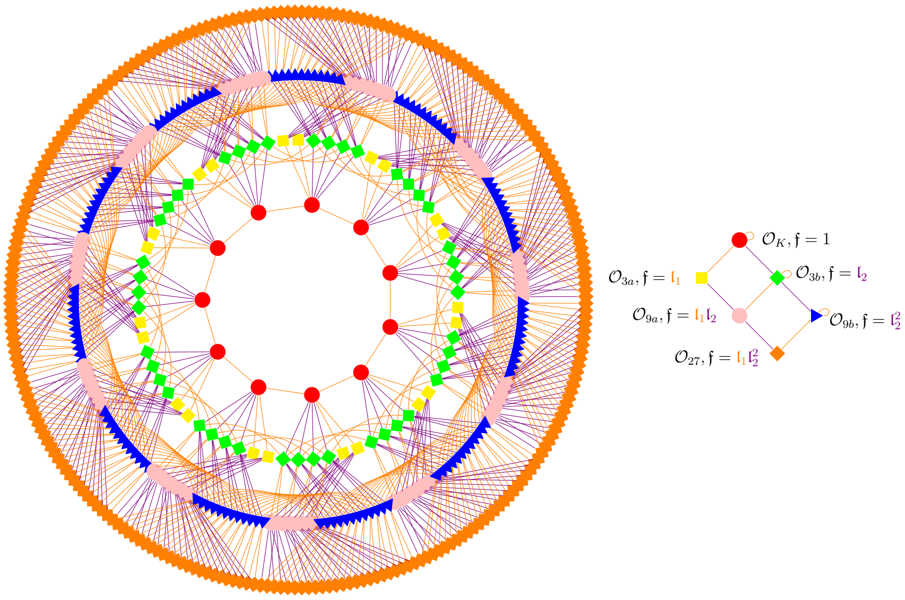


Fig. 8. A larger example