Isogeny graphs with maximal real multiplication

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

[1] Microsoft Research
One Microsoft Way – Redmond, WA, 98052 – USA
[2] CARAMEL 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 polarized abelian varieties and whose edges are isogenies between these varieties. In his thesis, Kohel described the structure of isogeny graphs for elliptic curves and showed that one may compute the endomorphism ring of an elliptic curve defined over a finite field by using a depth first search 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. Our setting considers genus 2 jacobians with complex multiplication, with the assumptions that the real multiplication subring is maximal and has class number one. We fully describe the isogeny graphs in that case. Over finite fields, we derive a depth first search algorithm for computing endomorphism rings locally at prime numbers, if the real multiplication is maximal. To the best of our knowledge, this is the first DFS-based algorithm in genus 2.

1 Introduction

Isogeny graphs are non-oriented graphs whose vertices are principally polarized simple abelian varieties and whose edges are isogenies between these varieties. Isogeny graphs were first studied by Kohel [14], who proved that in the case of elliptic curves, we may use these structures to compute the endomorphism ring of an elliptic curve. Kohel identified two types of ℓ-isogenies (i.e. of degree ℓ) in the graph: ascending-descending and horizontal. The first type corresponds to the case of an isogeny between two elliptic curves, such that the endomorphism ring of one curve is contained into the endomorphism ring of the other. The second type is that of an isogeny between two genus 1 curves with isomorphic endomorphism ring. As a consequence, Kohel shows that 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.

In the case of genus 2 jacobians, designing a similar algorithm for endomorphism ring computation requires a good understanding of the isogeny graph structure. Recent developments on the construction of isogenies between principally polarized abelian surfaces [16,5] allowed to compute examples of (ℓ,ℓ)-isogeny graphs [2]. It was noticed in this way that in the genus 2 case, a containement relation between the two orders giving the endomorphism rings is not guaranteed. This is a major obstacle into designing a depth first search algorithm for computing the endomorphism ring.

Let K be a primitive quartic CM field and K_0 its totally real subfield. In this paper, we study subgraphs of ℓ-isogenies whose vertices are all genus 2 jacobians with endomorphism ring isomorphic to an order of K which contains the maximal order $\mathcal{O}_{K_0}$. We show that the lattice of orders meeting this condition has a simple 2-dimensional grid structure. This results into a classification of isogenies in the graph: ascending-descending and horizontal, where these qualificatives apply separately to the two "dimensions" of the lattice of orders. Moreover, we show that any (ℓ, ℓ)-isogeny which is such that the two endomorphism rings contain $\mathcal{O}_{K_0}$ is a composition of two ℓ-isogenies which preserve real multiplication. As a consequence, we design a depth first search algorithm for computing endomorphism rings in the (ℓ, ℓ)-isogeny graph, based on Cosset and Robert's algorithm for constructing (ℓ, ℓ)-isogenies over finite fields. To the best of our knowledge, this is the first depth search algorithm for computing locally at small prime numbers ℓ the endomorphism ring of an ordinary genus 2 jacobian. We compare the complexity of our algorithm to that of existing algorithms [6] and show that, in most cases, our algorithm performs operations in a smaller degree extension field and is thus faster.

This paper is organized as follows. Section 2 provides background material concerning $\mathcal{O}_{K_0}$-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. The structure of the graph given by reductions over finite fields of these isogenies is proved in Section 4. In Section 5 we show that the computation of the Tate pairing allows to orient ourselves in the isogeny graph. Finally, in Section 6 we give our algorithm endomorphism ring computation when the real multiplication is maximal and in Section 7 we compare the its performance to the one of Eisenträger and Lauter's algorithm.

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 into a easy way to classify isogenies and navigate into isogeny graphs [14,7,13].

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. 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

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

The notation η will be retained throughout the paper.

Several results of the article will involve a prime number ℓ and also the finite field $\mathbb{F}_p$ or its extensions. We always implicitly assume that ℓ is coprime to p. Furthermore, 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 $\mathfrak{l}_{1,2}$ split in $\mathcal{O}_K$ is not determined a priori, however.

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

A major obstacle to depicting genus 2 isogeny graphs is that the structure of the lattice of orders of K lacks a concise description. Given an isogeny $I : J_1 \to J_2$ between two abelian surfaces with degree ℓ, the corresponding endomorphism rings are such that $\ell\mathcal{O}_{J_1} \subset \mathcal{O}_{J_2}$ or $\ell\mathcal{O}_{J_2} \subset \mathcal{O}_{J_1}$. Hence, even if a containement relation is guaranteed $\mathcal{O}_{J_2} \subset \mathcal{O}_{J_1}$, the index of one order into the other may be as high as ℓ^3. Since the $\mathbb{Z}$-rank of orders is 4, it is always possible to find several suborders of $\mathcal{O}_{J_1}$ 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 [9], 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

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

The following lemma was given by Goren and Lauter [9].

Lemma 1 *1. An $\mathcal{O}_{K_0}$-order of K is of the form $\mathcal{O}_{K_0}[m\eta]$, for some $m \in \mathcal{O}_{K_0}$, $m \neq 0$. This element is unique up to units of $\mathcal{O}_{K_0}$. The conductor of the order $\mathcal{O}[m\eta]$ is the principal $\mathcal{O}_K$-ideal $m\mathcal{O}_K$.*
2. For any element $m \in \mathcal{O}_{K_0}$, $\mathcal{O}_{K_0}[m\eta]$ is an order of conductor $m\mathcal{O}_K$.

A first consequence of Lemma 1 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 $\mathfrak{f} \cap \mathcal{O}_{K_0}$, which for brevity we still call the conductor and denote by $\mathfrak{f}$.

Using the particular shape of $\mathcal{O}_K$ as a monogenous $\mathcal{O}_{K_0}$-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 1.

Lemma 2 *For any $\mathcal{O}_{K_0}$-order $\mathcal{O}$, we have $\mathfrak{f}_{\mathcal{O}} = \mathfrak{f}_{\eta,\mathcal{O}}$.*

Let now $\mathcal{O}$ be an $\mathcal{O}_{K_0}$-order whose index is divisible by a power of ℓ. Assume that ℓ splits in $\mathcal{O}_{K_0}$ and let $\ell = \mathfrak{l}_1\mathfrak{l}_2$. Then by Lemma 1 the 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 1. This is equivalent to the following statement.

Lemma 3 *Let $\mathcal{O}$ be an $\mathcal{O}_{K_0}$-order in K. Locally at ℓ, the position of $\mathcal{O}$ within the lattice of $\mathcal{O}_{K_0}$-orders is given by the valuations $\nu_{\mathfrak{l}_i}(\mathfrak{f}_{\mathcal{O}})$, for $i = 1, 2$.*

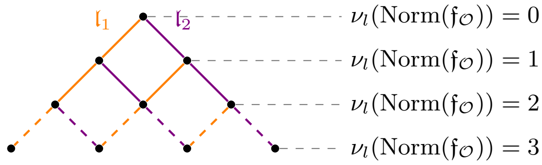

Fig. 1. The lattice of orders

2.2 The Tate pairing

Let J be an abelian surface, i.e. the jacobian of a genus 2 curve, defined over a field L. We denote by $J[m]$ the subgroup of m-torsion, i.e. the points of order m. We denote by μ_m the group of m-th roots of unity. Let

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

be the m-Weil pairing.

The definition of the Tate pairing involves the Weil pairing and Galois cohomology. In this paper, we are only interested in the Tate pairing over finite fields. Therefore, we specialize the definition to this case, following [18,11]. More precisely, suppose we have $m \mid \#J(\mathbb{F}_q)$ and denote by k the *embedding degree with respect to* m, i.e. the smallest integer $k \geq 0$ such that $m \mid q^k - 1$. We define the Tate pairing as

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

where π is the Frobenius automorphism of the finite field $\mathbb{F}_{q^k}$ and $\bar{P}$ is any point such that $m\bar{P} = P$. It is easy to check that this definition is independent of the choice of $\bar{P}$.

For a fixed principal polarization $\lambda : J \to \hat{J}$ we define a pairing on J itself

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

Most often, if J 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 [15] describes a version of the Tate pairing on Jacobian varieties. Since we use Lichtenbaum's formula for computations, we briefly recall it here. Let $D_1 \in J(\mathbb{F}_{q^k})$ and $D_2 \in J[m](\mathbb{F}_{q^k})$ 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 $(\mathbb{F}_{q^k})^r$. Given that $\mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^m \simeq \mu_m$, we obtain the Tate pairing as

$$\begin{aligned} t_m(\cdot,\cdot) : J(\mathbb{F}_{q^k})/mJ(\mathbb{F}_{q^k}) \times J[m](\mathbb{F}_{q^k}) &\to \mu_m \\ (P,Q) &\to T_m(P,Q)^{(q^k-1)/m}. \end{aligned}$$

The function $f_{m,D_2}(D_1)$ is computed using Miller's algorithm [17] in $O(\log m)$ operations in $\mathbb{F}_{q^k}$.

3 Isogenies preserving real multiplication

In this paper, we assume that principally polarized abelian surfaces are *simple*, i.e. not isogenous to a product of elliptic curves. The quartic CM field K is primitive, i.e. it does not contain a totally imaginary subfield. We assume that $K = \mathbb{Q}(\gamma)$, with $\gamma = i\sqrt{a+b\sqrt{d}}$ if $d \equiv 2,3 \mod 4$ or $\gamma = i\sqrt{a+b\left(\frac{-1+\sqrt{d}}{2}\right)}$ if $d \equiv 1 \mod 4$. A CM-type Φ is a pair of non-complex conjugate embeddings of K in $\mathbb{C}$

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

An abelian surface over $\mathbb{C}$ with complex multiplication by an order $\mathcal{O} \subset K$ is given by $A = \mathbb{C}^2/\Phi(\mathfrak{a})$, where $\mathfrak{a}$ is an ideal of $\mathcal{O}$ and Φ is a CM-type. This variety is said to be of CM-type (K, Φ). Recall that we focus on the case where $\mathcal{O}_{K_0} \subset \mathcal{O}$. Since $\mathcal{O}_{K_0}$ is a Dedekind domain and the ideal $\mathfrak{a}$ is a $\mathcal{O}_{K_0}$-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 $A = \mathbb{C}^2/\Phi(\Lambda)$ and $\Lambda = \Lambda_1 + \Lambda_2\tau$, with Λ_1 and Λ_2 lattices in K_0 and $(\tau^{\phi_1}, \tau^{\phi_2}) \in \mathbb{H}_1^2$. Note that in the more restrictive setting we have elected, K_0 is principal, which entails that we can choose $\Lambda_1 = \Lambda_2 = \mathcal{O}_{K_0}$.

Every Riemann form is of the form

$$H_\xi(z,w) = \sum_{r=1}^{2} \frac{\xi^{\phi_r} z_r \bar{w}_r}{\Im(\tau^{\phi_r})},$$

for $\xi \in K_0$ totally positive. The imaginary part E_ξ satisfies

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

with $z = x + y\Phi(\tau), w = x' + y'\Phi(\tau)$, where $x, y, x', y' \in \mathbb{R}^2$.

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

Proposition 4 *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 $\Lambda = \Lambda_1 + \Lambda_2\tau$. We have a one-to-one correspondence between cyclic subgroups of $(\Lambda/\mathfrak{l})/\Lambda$ and isogenies on A having these subgroup as kernels, which are written in the following form:*

$$\begin{array}{ll} A \to \mathbb{C}^2/\Phi(\dfrac{\Lambda_1}{\mathfrak{l}} + \Lambda_2\tau), & A \to \mathbb{C}^2/\Phi(\Lambda_1 + \dfrac{\Lambda_2}{\mathfrak{l}}(\tau+\rho)), \\ z \mapsto z, & z \mapsto z, \end{array} \tag{1}$$

where $\rho \in \mathfrak{l}\Lambda_1\Lambda_2^{-1}$.

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

Isogenies as described by Proposition 4 are called $\mathfrak{l}$-*isogenies*. Alternatively, if $\mathfrak{l}$ is a principal ideal $\alpha\mathcal{O}_{K_0}$ (which occurs in our setting since K_0 is assumed principal), we also use the term α-isogeny.

The following trivial observation that $\mathfrak{l}$-isogenies preserve the maximal real multiplication follows directly from $\mathrm{End}(\frac{\Lambda_i}{\mathfrak{l}}) = \mathrm{End}(\Lambda_i)$. We shall investigate a converse to this statement later in this article.

Proposition 5 *Let A be an abelian surface with $\mathrm{End}(A)$ an $\mathcal{O}_{K_0}$-order. Let $I : A \to B$ be a $\mathfrak{l}$-isogeny. Then $\mathrm{End}(B)$ is also an $\mathcal{O}_{K_0}$-order.*

Polarizations can be transported through $\mathfrak{l}$-isogenies, and particularly so in the case where K_0 is principal. We consider the cases where $\mathfrak{l}$ is generated by $\alpha \in K_0$, with α either totally positive or (if the narrow class group $\mathrm{Cl}^+(\mathcal{O}_{K_0})$ is not trivial, i.e. $\mathbb{Z}/2\mathbb{Z}$ in our case) of negative norm. In the first case, with α totally positive, we have

$$\begin{aligned} E_\xi(x + y\tau, x' + y'\tau) &= E_{\xi\alpha}(\frac{x}{\alpha} + y\tau, \frac{x'}{\alpha} + y'\tau), \\ &= E_{\xi\alpha}(x + \frac{y}{\alpha}(\tau+\rho), x' + \frac{y'}{\alpha}(\tau+\rho)). \end{aligned}$$

Hence if H_ξ defines a principal polarization on $\mathbb{C}^2/\Phi(\Lambda_1+\Lambda_2\tau)$, then $H_{\xi\alpha}$ defines principal polarizations on the varieties $\mathbb{C}^2/\Phi(\frac{\Lambda_1}{\alpha}+\Lambda_2\tau)$ and $\mathbb{C}^2/\Phi(\Lambda_1+\frac{\Lambda_2}{\alpha}(\tau+\rho))$. In the second case, then an $\mathfrak{l}$-isogeny maps a principally polarized abelian variety to a variety in the non-trivial polarization class and vice-versa.

In the sequel, we assume that ℓ is a prime number, such that $\ell\mathcal{O}_{K_0} = \mathfrak{l}_1\mathfrak{l}_2$. Take α_i, $i = \{1, 2\}$, elements of $\mathcal{O}_{K_0}$ such that $\mathfrak{l}_i = \alpha_i\mathcal{O}_{K_0}$. We show that from the principal polarization induced by an $\mathfrak{l}$-isogeny, we can compute a principal polarization on the target variety .

Proposition 6 *Let $I : J_1 \to J_2$ be a α_1-isogeny and let $\lambda_\xi : J_1 \to \hat{J}_1$ be the homomorphism corresponding to the polarization class ξ of J_1. Then the homomorphism $\lambda_I : J_2 \to \hat{J}_2$ such that $\hat{I} \circ \lambda_I \circ I = \ell\lambda_\xi$ is of the form $\alpha_2 \circ \lambda_{\alpha_1\xi}$, with $\lambda_{\alpha_1\xi} : J_2 \to \hat{J}_2$ corresponding to the polarization class of J_2.*

Proof. Without loss of generality, we consider the case where the isogeny I between complex tori is given by

$$\begin{aligned} \mathbb{C}^2/\Phi(\Lambda_1 + \Lambda_2\tau) &\to \mathbb{C}^2/\Phi(\frac{\Lambda_1}{\alpha_1} + \Lambda_2\tau) \\ z &\mapsto z \end{aligned} \tag{2}$$

Then I corresponds to a linear mapping from $\Lambda_1 + \Lambda_2\tau$ to $\frac{\Lambda_1}{\alpha_1} + \Lambda_2\tau$ given by the matrix

$$M = \begin{pmatrix} \Xi_{\alpha_1} & 0 \\ 0 & I_2 \end{pmatrix}$$

where Ξ_{α_1} denotes the matrix of the multiplication by $\alpha_1 \in K_0$. The transpose matrix M^t is the rational representation of the dual isogeny with respect to the dual basis. The dual isogeny is then given by

$$\begin{aligned} \mathbb{C}^2/\Phi(\frac{\Lambda_1}{\alpha_1} + \Lambda_2\bar{\tau}) &\to \mathbb{C}^2/\Phi(\Lambda_1 + \Lambda_2\bar{\tau}) \\ z &\mapsto \alpha_1 z. \end{aligned} \tag{3}$$

Hence the following diagram commutes:

$$\begin{tikzcd} \mathbb{C}^2/\Phi(\Lambda_1 + \Lambda_2\tau) \arrow[r, "I"] \arrow[d, "\ell\lambda_\xi"'] & \mathbb{C}^2/\Phi(\frac{\Lambda_1}{\alpha_1} + \Lambda_2\tau) \arrow[d, "\alpha_2 \circ \lambda_{\alpha_1\xi}"] \\ \mathbb{C}^2/\Phi(\Lambda_1 + \Lambda_2\bar{\tau}) & \mathbb{C}^2/\Phi(\frac{\Lambda_1}{\alpha_1} + \Lambda_2\bar{\tau}) \arrow[l, "\hat{I}"'] \end{tikzcd}$$

This concludes the proof. □

In the remainder of the paper, we denote by $J[\mathfrak{l}]$ the subgroup

$$J[\mathfrak{l}] = \{x \in J \mid \alpha x = 0, \forall \alpha \in \mathfrak{l}\},$$

for any ideal $\mathfrak{l}$ of norm ℓ in $\mathcal{O}_{K_0}$. For the commonly encountered case where $\mathfrak{l} = \alpha\mathcal{O}_{K_0}$ for some generator $\alpha \in \mathcal{O}_{K_0}$, this matches with the notation $J[\alpha]$ representing the kernel of the endomorphism reprensented by α.

Recall that 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 7 *Let J be an abelian surface defined over a 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 $W_\ell(P_1, P_2) = \exp(-2\pi i\ell\frac{E_\xi(x_1+x_2\tau, y_1+y_2\tau)}{\ell})) = 1$. □

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 abelian varieties defined over a finite field, such that the corresponding endomorphism rings are $\mathcal{O}_{K_0}$-orders. The endomorphism ring of an ordinary jacobian J over a finite field $\mathbb{F}_q$ $(q = p^n)$ is an order in the quartic CM field K such that

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

where $\mathbb{Z}[\pi, \bar{\pi}]$ denotes the order generated by π, the Frobenius endomorphism and by $\bar{\pi}$, the Verschiebung. For simplicity, in the remainder of this paper, we assume that $\mathbb{Z}[\pi, \bar{\pi}]$ is a $\mathcal{O}_{K_0}$-order.

By the theory of canonical lifts, we may choose abelian surfaces $\tilde{J}$ defined over an extension field L of the reflex field K_r, and a prime ideal $\mathfrak{p}$ in K_r such that J is isomorphic to the reduction of $\tilde{J}$ modulo a ideal $\mathfrak{P}$ lying over $\mathfrak{p}$ in L. Let $\ell \neq p$ be a prime with $\ell = \mathfrak{l}_1\mathfrak{l}_2$ in $\mathcal{O}_{K_0}$. For $i = 1, 2$ we have then $J[\mathfrak{l}_i] \simeq \tilde{J}[\mathfrak{l}_i]$ and the reductions of $\mathfrak{l}_i$-isogenies give $\ell + 1$ isogenies towards varieties whose endomorphism ring is a $\mathcal{O}_{K_0}$-order.

Associated to an abelian surface whose endomorphism ring is an $\mathcal{O}_{K_0}$-order, we define the $\{\mathfrak{l}_1, \mathfrak{l}_2\}$-*isogeny graph* whose edges are either $\mathfrak{l}_1$- or $\mathfrak{l}_2$-isogenies as defined by Proposition 4, and whose vertices are abelian surfaces over $\mathbb{F}_q$ reached (transitively) by such isogenies. We will prove that over finite fields, the $\{\mathfrak{l}_1, \mathfrak{l}_2\}$-isogeny graph is the graph of all isogenies of degree ℓ between abelian surfaces having maximal real multplication. We underline here that this holds as well for isogeny graphs between abelian varieties defined over the complex numbers, thanks to the following graph isomorphism.

Proposition 8 *Let $\mathcal{G}$ be an $\{\mathfrak{l}_1, \mathfrak{l}_2\}$-isogeny graph with vertices abelian surfaces defined over $\mathbb{F}_q$ and whose endomorphism ring is an $\mathcal{O}_{K_0}$-order within K. Let π be a q-Weil number, giving the Frobenius endomorphism for any of the abelian surfaces in $\mathcal{G}$. Then there is a number field L and a graph $\mathcal{G}'$ isomorphic to $\mathcal{G}$, whose vertices are abelian surfaces defined over L, having complex multiplication by a $\mathcal{O}_{K_0}$-order containing $\mathbb{Z}[\pi, \bar{\pi}]$, and whose edges are $\mathfrak{l}_1$- or $\mathfrak{l}_2$-isogenies between these surfaces.*

Proof. Let $I : J \to J'$ be an edge in $\mathcal{G}$. Let $\tilde{J}$ be the canonical lift of J, defined over an extension field L of the reflex field K_r, and a prime ideal $\mathfrak{p}$ in K_r such that J is isomorphic to the reduction of $\tilde{J}$ modulo a ideal $\mathfrak{P}$ lying over $\mathfrak{p}$ in L. By definition, I is obtained as the reduction of an $\mathfrak{l}$-isogeny from $\tilde{J}$ to another variety $\tilde{J}'$, whose reduction is isomorphic to J', by the uniqueness of the canonical lift. Since the reduction is an injective morphism from $\mathrm{Hom}(\tilde{J}, \tilde{J}')$ to $\mathrm{Hom}(J, J')$ [19, Sect. 11, Prop. 12], we conclude that $\tilde{I}$ is the unique isogeny whose reduction gives I. □

We are now interested in determining the field of definition of $\mathfrak{l}$-isogenies starting from J. 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 and let $\theta \in \mathcal{O}$. We define the $\mathfrak{l}$-adic valuation of θ in $\mathcal{O}$ as

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

Recall that for a jacobian J with maximal real multiplication, we are interested in computing the $\mathfrak{l}$-adic valuation of the conductor of the endomorphism ring $\mathcal{O}_J$. We remark that it suffices to determine $\nu_{\mathfrak{l},\mathcal{O}_J}(\pi - \bar{\pi})$. Indeed, we have $\mathcal{O}_J = \mathcal{O}_{K_0} + \mathcal{O}_{K_0}\mathfrak{f}_{\eta,\mathcal{O}_J}\eta$ and $\pi - \bar{\pi} \in \mathcal{O}_{K_0}\mathfrak{f}_{\eta,\mathcal{O}_J}\eta$. Then

$$\nu_{\mathfrak{l}}(\mathfrak{f}_{\eta,\mathcal{O}_J}) = \nu_{\mathfrak{l},\mathcal{O}_K}(\pi - \bar{\pi}) - \nu_{\mathfrak{l},\mathcal{O}_J}(\pi - \bar{\pi}). \tag{4}$$

In the sequel, we denote by $\nu_{\mathfrak{l}_i,J}(\pi - \bar{\pi}) := \nu_{\mathfrak{l},\mathcal{O}_J}(\pi - \bar{\pi})$.

Proposition 9 *Let ℓ be an odd prime number, such that $(\ell) = \mathfrak{l}_1\mathfrak{l}_2$ in $\mathcal{O}_{K_0}$. Then the largest integer n such that the Frobenius matrix on $J[\mathfrak{l}_i^n]$ is of the form*

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

is $\nu_{\mathfrak{l}_i,J}(\pi - \bar{\pi})$.

Proof. Assume that $\nu_{\mathfrak{l}_i,J}(\pi - \bar{\pi}) = n$. Then $(\pi - \bar{\pi})(J[\mathfrak{l}_i^n]) = 0$. Let D be an element of $J[\mathfrak{l}_i^n]$. Then $\pi + \bar{\pi}$ acts on D as an element of $\mathcal{O}_{K_0}/\mathfrak{l}_i^n \simeq \mathbb{Z}/\ell^n\mathbb{Z}$. Hence $(\pi + \bar{\pi})(D) = \lambda D$ for some λ. Since $(\pi - \bar{\pi})(J[\mathfrak{l}_i^n]) = 0$, it follows that $\pi(D) = \lambda' D$. Hence, if D_1, D_2 is a basis for $J[\mathfrak{l}_i^n]$, the matrix of the Frobenius for this basis is

$$\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}. \tag{5}$$

The matrix for the Verschiebung is then

$$\begin{pmatrix} \lambda_2 & 0 \\ 0 & \lambda_1 \end{pmatrix}. \tag{6}$$

Since $\pi - \bar{\pi}$ is zero on $J[\mathfrak{l}_i^n]$, it follows that $\lambda_1 = \lambda_2 \pmod{\ell^n}$. Hence any subgroup of $J[\mathfrak{l}_i^n]$ is rational. The reverse implication is obvious.

Remark 1. A natural consequence of Proposition 9 is that the cyclic subgroups of $J[\mathfrak{l}_i^n]$ are rational if and only if $\nu_{\mathfrak{l}_i,J}(\pi - \bar{\pi}) \geq n$. In particular, the $\ell + 1$ isogenies whose kernel is a cyclic subgroup of $J[\mathfrak{l}_i]$ are rational if and only if $\nu_{\mathfrak{l}_i}(\pi - \bar{\pi}) > 0$.

Example 1. 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. The 3-torsion is defined over an extension field of degree 6, but $J[\alpha_1] \subset J(\mathbb{F}_{q^6})$ and $J[\alpha_2] \subset J(\mathbb{F}_{q^2})$. We have that $\nu_{\alpha_i}(\mathfrak{f}_{\mathbb{Z}[\pi,\bar{\pi}]}) = 1$, for $i = 1, 2$, where π has relative norm 211 in $\mathcal{O}_K$.

In particular, Remark 1 implies that if a $\mathfrak{l}$-isogeny $I : J_1 \to J_2$ is such that $\mathbb{Z}[\pi, \bar{\pi}] \subset \mathrm{End}(J_1)$ and $\mathbb{Z}[\pi, \bar{\pi}] \subset \mathrm{End}(J_2)$, then I is an isogeny in the graph of rational isogenies preserving the real multiplication. We will show that the $\{\mathfrak{l}_1, \mathfrak{l}_2\}$-isogeny graph is in fact the subgraph of rational isogenies preserving the maximal real multiplication.

Lemma 10 *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* $\mathrm{Ker}\, I \cap A[\mathfrak{l}] \neq \emptyset$.

Proof. We prove the contrapositive statement. Assume that there is an isogeny $I : A \to B$ defined over $\mathbb{F}_q$ with $\mathrm{Ker}\, I \cap A[\mathfrak{l}] = \emptyset$. 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 valuations $\nu_{\mathfrak{l},\mathcal{O}_A}(\pi_A - \bar{\pi}_A)$ and $\nu_{\mathfrak{l},\mathcal{O}_B}(\pi_B - \bar{\pi}_B)$ are equal. By equation (4), it follows that the $\mathfrak{l}$-adic valuations of the conductors of endomorphism rings of A and B are equal. □

The converse of Lemma 10 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 5.

Proposition 11 *Let ℓ be an odd prime number, split in K_0. All cyclic isogenies of degree ℓ preserving the real multiplication 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 isogeny which preserves the real multiplication $\mathcal{O}_{K_0}$. The endomorphism rings $\mathcal{O}_A$ and $\mathcal{O}_B$ are orders in the lattice of orders described by Figure 1. First, by [4, Section 8], we have that either $\ell\mathcal{O}_A \subset \mathcal{O}_B$, or $\ell\mathcal{O}_B \subset \mathcal{O}_A$. 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 10, 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 $\mathcal{O}_B$ lie at the same level in the lattice of orders. If the two endomorphism rings are isomorphic, then the isogeny corresponds (under the class group action) to an invertible ideal $\mathfrak{u}$ of $\mathcal{O}_A$ such that $\mathfrak{u}\bar{\mathfrak{u}} = \mathfrak{l}$, with $\mathfrak{l}$ an ideal of norm ℓ in $\mathcal{O}_{K_0}$. The isogeny is then an $\mathfrak{l}$-isogeny, and $\mathfrak{l}$ is one of $\mathfrak{l}_{1,2}$.

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 $A[\mathfrak{l}_2]$. This is not possible if the isogeny is cyclic. □

A natural consequence of Proposition 11 is that we may classify cyclic isogenies preserving real multiplication (therefore, $\mathfrak{l}$-isogenies) into three categories. Let $\mathfrak{l}$ be such that the isogeny $I : A \to B$ being considered is an $\mathfrak{l}$-isogeny. If $\mathcal{O}_A \simeq \mathcal{O}_B$, we say that the isogeny is *horizontal*. If not, then the two orders lie on consecutive levels of the lattice given by Figure 1. If $\mathcal{O}_B$ is properly contained into $\mathcal{O}_A$, we say that the isogeny is *descending*. In the opposite situation, we say the isogeny is *ascending*.

Proposition 12 *Let A be an abelian surface defined over a finite field $\mathbb{F}_q$ such that its endomorphism ring $\mathcal{O}$ is an $\mathcal{O}_{K_0}$-order in a CM quartic field different from $\mathbb{Q}(\xi_5)$. Let $\mathfrak{l}$ be an ideal of prime norm ℓ in $\mathcal{O}_{K_0}$.*

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 exactly two horizontal $\mathfrak{l}$-isogenies starting from A and all the others are descending.*
   (b) *If $\mathfrak{l}$ ramifies in $\mathcal{O}_K$, 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 are descending.*
2. *If $\mathfrak{l}$ is not coprime to $\mathfrak{f}$, then there is exactly one ascending $\mathfrak{l}$-isogeny and ℓ descending ones, starting from A.*

Proof. The number of horizontal isogenies is given by the number of projective ideals of norm ℓ. In order to count descending isogenies, we count the abelian surfaces lying at a given level in the graph (up to isomorphism), by applying class number relations. More precisely, we have the exact sequence

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

Hence we have the formula for the class number

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

We have that $\mathcal{O}_K^\times = \mu_K \mathcal{O}_{K_0}^\times$, with $\mu_K = \{\pm 1\}$ (see [20, Lemma II.3.3]). Since $\mathcal{O}_{K_0} \subset \mathcal{O}$, it follows that $[\mathcal{O}_K^\times : \mathcal{O}_{K_0}^\times]$=1.

We note that $\mathcal{O}/\mathfrak{f}\mathcal{O} \simeq \mathbb{Z}/f\mathbb{Z}$, where $f = N(\mathfrak{f})$. Hence we have that $\#(\mathcal{O}/\mathfrak{f}\mathcal{O})^\times = f \prod_{p|f}(1 - \frac{1}{p})$. Moreover, we have

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

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 using a similar formula for the class number, we obtain that

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

if $\mathfrak{l}$ is prime to $\mathfrak{f}$. Hence the number of of descending isogenies is $\ell-1$ if $\mathfrak{l}$ is split, ℓ if $\mathfrak{l}$ is ramified and $\ell+1$ if $\mathfrak{l}$ is inert. If $\mathfrak{l}$ divides $\mathfrak{f}$, we have

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

which leads to the fact that the number of descending isogenies is ℓ.

Graph structure for $\mathrm{Cl}^+(\mathcal{O}_{K_0}) = 1$. In the case of K_0 having trivial narrow class group, Proposition 12 gives the following structure of connected components of the non-oriented isogeny graph.

1. At each level, if $\nu_{\mathfrak{l},J}(\pi-\bar{\pi}) > 0$, there are $\ell+1$ rational isogenies with kernel a cyclic subgroup of $J[\mathfrak{l}]$.
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 $\mathfrak{l}$. At every intermediary level (i.e. $\nu_{\mathfrak{l},J}(\pi-\bar{\pi}) > 0$), there is one ascending $\mathfrak{l}$-isogeny and ℓ descending ones.
3. If $\nu_{\mathfrak{l},J}(\pi-\bar{\pi}) = 0$ there is exactly one ascending $\mathfrak{l}$-isogeny.

The structure of this graph is similar to the one of an ℓ-isogeny graph between elliptic curves, called *volcanoes* [14,7]. If one considers an $\{\mathfrak{l}_1,\mathfrak{l}_2\}$-isogeny graphs and restricts to a connected component reached by edges which are $\mathfrak{l}_1$-isogenies, then the structure is *exactly* that of a volcano. More generally, an $\{\mathfrak{l}_1,\mathfrak{l}_2\}$-isogeny graph can be seen, by the results above, as a direct product of two graphs which share all their characteristics with genus one isogeny volcanoes. In particular the generalization of 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 J a Jacobian defined over $\mathbb{F}_q$ with maximal real multiplication. We do not have formulas for computing cyclic isogenies over finite fields. Instead, we experiment over the complex numbers, and use the fact that there is a graph isomorphism between the $\mathfrak{l}$-isogeny graph having J as a vertex and the graph of its canonical lift.

To draw the graph corresponding to Example 1, 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 [10].

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 (1) and follow the edges of the graph of isogenies between complex abelian surfaces having complex multiplication by an order $\mathcal{O}$ containing $\mathbb{Z}[\pi, \bar{\pi}]$. The exploration terminates when outgoing edges from each node have been visited. This yields Figure 2. Violet and orange edges in Figure 2 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. Identification of each variety to its dual, makes the graph of Figure 2 non-oriented.

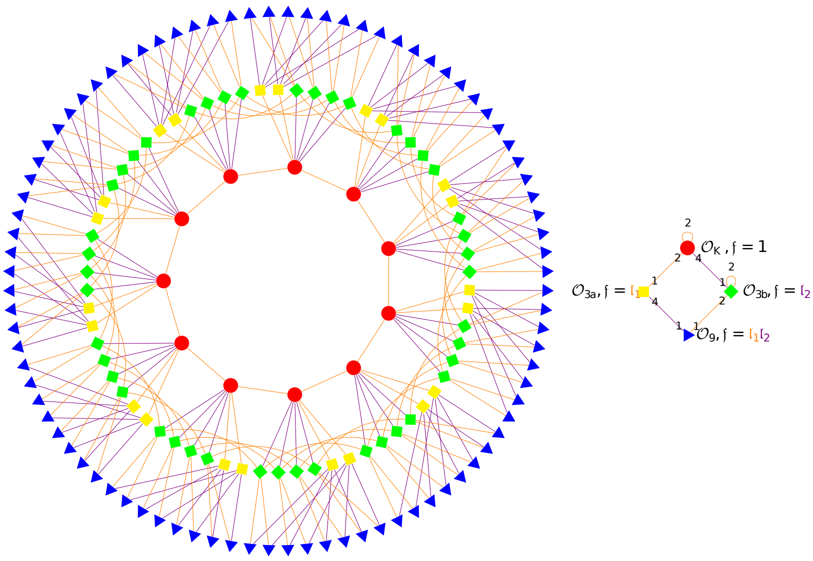

Fig. 2. Graph of ℓ-isogenies preserving real multiplication, for $\ell = 3$, K defined by $\alpha^4+81\alpha^2+1181$, and $\mathbb{Z}[\pi, \bar{\pi}]$ defined by the Weil number $\pi = \frac{1}{2}(\alpha^2+3\alpha+45)$, with $p = \mathrm{Norm}\,\pi = 211$.

4.1 Isogenies with Weil-isotropic kernel

In a computational perspective, we are interested in (ℓ, ℓ)-isogenies, which are accessible to computation using the algorithms developed by [5]. Our description of the $\mathfrak{l}_1$- and $\mathfrak{l}_2$-isogenies is key to understanding the (ℓ, ℓ)-isogenies due to the following result.

Proposition 13 *Let $\ell > 3$ be a prime number such that $\ell\mathcal{O}_{K_0} = \mathfrak{l}_1\mathfrak{l}_2$. Then all (ℓ,ℓ)-isogenies preserving the real multiplication are a composition of an $\mathfrak{l}_1$-isogeny with an $\mathfrak{l}_2$-isogeny.*

Proof. Let $I : A \to B$ be an (ℓ,ℓ)-isogeny preserving the real multiplication. Let $\mathcal{O}_A = \mathrm{End}(A)$ and $\mathcal{O}_B = \mathrm{End}(B)$. If the endomorphism rings are equal, then the isogeny corresponds, under the action of the Shimura class group $\mathfrak{C}(K)$ [19], to an ideal class $\mathfrak{a}$ such that $\mathfrak{a}\bar{\mathfrak{a}} = \ell\mathcal{O}_A$. It follows that both $\mathfrak{l}_1$ and $\mathfrak{l}_2$ split in K. 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 a $\mathfrak{l}_2$-isogeny.

Assume now that $\mathcal{O}_A$ and $\mathcal{O}_B$ are not isomorphic. This implies that $\nu_{\mathfrak{l},\mathcal{O}_A}(\pi - \bar{\pi})$ and $\nu_{\mathfrak{l},\mathcal{O}_B}(\pi-\bar{\pi})$ 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 $\nu_{\mathfrak{l}_1,\mathcal{O}_A}(\pi-\bar{\pi}) > \nu_{\mathfrak{l}_1,\mathcal{O}_B}(\pi-\bar{\pi})$.

Let $n = \nu_{\mathfrak{l}_1,\mathcal{O}_A}(\pi-\bar{\pi})$. We then have that any subgroup of $A[\mathfrak{l}_1^n]$ is rational. By Proposition 9, there is a 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 11). By [6, 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 $\langle D_1, D_2\rangle = \mathrm{Ker}\, I$. Since $\mathrm{Ker}\, I \subset A[\mathfrak{l}_1] + A[\mathfrak{l}_2]$, we may write $D_2 = D_{2,1} + D_{2,2}$ with $D_{2,i} \in A[\mathfrak{l}_i]$. As $\mathrm{Ker}\, I$ is Weil-isotropic, we may choose D_2 so that $D_{2,1} = 0$, whence $D_2 \in A[\mathfrak{l}_2]$. He 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,ℓ)-isogenies with regard to the $\mathfrak{l}_i$-isogenies they are composed of. Let $I = I_1 \circ I_2$ be an (ℓ,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 10 there is no interaction of I_2 with the $\mathfrak{l}_i$-valuation of the conductor of the endomorphism ring.

5 Pairings on the real multiplication isogeny graph

Let J be a jacobian defined over $\mathbb{F}_q$, with complex multiplication by a $\mathcal{O}_{K_0}$-order. Let $\ell\mathcal{O}_{K_0} = \mathfrak{l}_1\mathfrak{l}_2$. In this Section, $\mathfrak{l}$ denotes any of the ideals $\mathfrak{l}_1, \mathfrak{l}_2$.

We relate some properties of the Tate pairing to the isomorphism class of the endomorphism ring of the Jacobian, by giving a similar result to the one of Ionica and Joux [13] for genus 1 isogeny graphs. More precisely, we show that the nondegeneracy of the Tate pairing restricted to the kernel of a $\mathfrak{l}$-isogeny determines the direction of the isogeny in the graph, at least when $\nu_{\mathfrak{l}}(\pi - \bar{\pi})$ is below some bound. This result is then exploited to efficiently navigate in isogeny graphs.

Let r be the smallest integer such that $J[\mathfrak{l}] \subset J(\mathbb{F}_{q^r})$. Let n be the largest integer such that $J[\mathfrak{l}^n] \subset J[\mathbb{F}_{q^r}]$ and that $J[\mathfrak{l}^{n+1}] \not\subset J[\mathbb{F}_{q^r}]$. We define $k_{\mathfrak{l},J}$ to be

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

Definition 14 *Let G be a cyclic group of $J[\mathfrak{l}^n]$. We say that the Tate pairing is $k_{\mathfrak{l},J}$-non-degenerate (or simply non-degenerate) on $G \times G$ if its restriction*

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

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

For the following few paragraphs we will 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}.

Since $\mathfrak{l}$ is principal in the real quadratic order $\mathcal{O}_{K_0} \subset \mathrm{End}(J)$, it follows that $J[\mathfrak{l}]$ is the kernel of an endomorphism. Since J is ordinary, all endomorphisms are $\mathbb{F}_q$-rational. Consequently, we have that $\pi(J[\mathfrak{l}^n]) \subset J[\mathfrak{l}^n]$, for $n \geq 0$. The following result shows that computing the $\mathfrak{l}$-adic valuation of $\pi - \bar{\pi}$ is equivalent to computing $k_{\mathfrak{l},J}$.

Proposition 15 *Let r be the smallest integer such that $J[\mathfrak{l}] \subset J(\mathbb{F}_{q^r})$. Let n be the largest integer such that $J[\mathfrak{l}^n] \subset J[\mathbb{F}_{q^r}]$ and that $J[\mathfrak{l}^{n+1}] \not\subset J[\mathbb{F}_{q^r}]$. Then if $\nu_{\mathfrak{l},J}(\pi^r - \bar{\pi}^r) < 2n$, then we have*

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

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

$$T_{\ell^n}(\ell^n Q_i, \ell^n Q_i) = W_{\ell^{2n}}(\pi(Q_i) - Q_i, Q_i) = W_{\ell^{2n}}(Q_k, Q_i)^{a_{ik}},$$

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

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

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

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

We conclude that $\ell^{2n-k_{\mathfrak{l},J}}$ divides all of a_{12}, a_{21}, and $a_{11} - a_{22}$. By Proposition 9, this implies that $2n - k_{\mathfrak{l},J} \leq \nu_{\mathfrak{l},J}(\pi^r - \bar{\pi}^r)$. Conversely, let $k = 2n - \nu_{\mathfrak{l},J}(\pi^r - \bar{\pi}^r)$. We know that $\pi = \lambda I_2 + \ell^{2n-k} A$, for $A \in M_2(\mathbb{Z})$. Then for $P \in J[\mathfrak{l}^n]$ 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 $k \geq k_{\mathfrak{l},J}$ and this concludes the proof. ∎

From this proposition, it follows that if $\nu_{\mathfrak{l},J}(\pi - \bar{\pi}) > 2n$, the self-pairings of all kernels of $\mathfrak{l}$-isogenies are degenerate. At a certain level in the isogeny graph, when $\nu_{\mathfrak{l},J}(\pi - \bar{\pi}) < 2n$, there is at least one kernel with non-degenerate pairing (i.e. $k_{\mathfrak{l},J} = 1$). Following the terminology of [12], we call this level *the second stability level.* As we descend to the floor, $k_{\mathfrak{l},J}$ increases. The *first stability level* is the level at which $k_{\mathfrak{l},J}$ equals n.

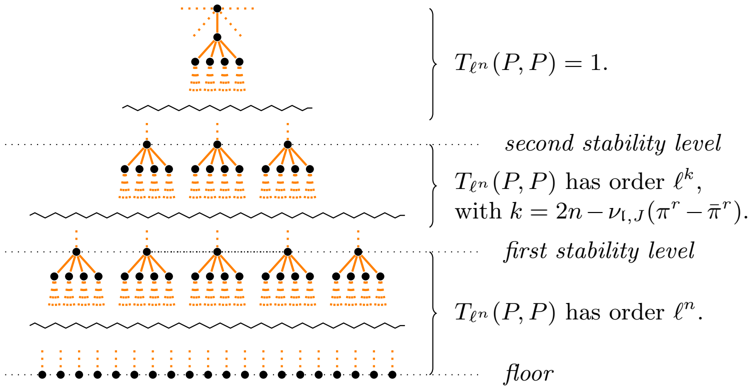

Fig. 3. Stability levels

We now show that from a computation 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 16 *If $k_{\mathfrak{l},J} > 0$, then there are at most two subgroups of order ℓ in $J[\mathfrak{l}^n]$ such that points in these subgroups have degenerate self-pairing.*

Proof. 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

$$S(a,b) = a^2\lambda_{P,P} + ab\,(\lambda_{P,Q} + \lambda_{Q,P}) + b^2\lambda_{Q,Q} \tag{7}$$

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

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

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

any polynomial defined by a basis $\{P,Q\}$ of $J[\mathfrak{l}^n]$ in a manner similar to the proof of Lemma 16.

Theorem 17. *Let P be a $\mathfrak{l}$-torsion point and let r be the smallest integer such that $J[\mathfrak{l}] \subset J(\mathbb{F}_{q^r})$. Let n be the largest integer such that $J[\mathfrak{l}^n] \subset J[\mathbb{F}_{q^r}]$ and that $J[\mathfrak{l}^{n+1}] \not\subset J[\mathbb{F}_{q^r}]$. Assume that $k_{\mathfrak{l},J} > 0$. Consider G a subgroup 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 $k_{\mathfrak{l},J} > 1$. Otherwise, we consider J' defined over and extension field of $\mathbb{F}_{q^r}$ and apply [11, Lemma 4]. Let $I : J \to J'$ the isogeny of kernel generated by P. Assume that P has non-degenerate self-pairing. Let $\bar{P} \in G$ such that $\ell^{n-1}\bar{P} = P$. Then by [11, Lemma 5b] and Lemma 6, we have

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

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 $R \in J'[\mathfrak{l}^n]$, we have $\alpha(R) = \lambda R$, for some $\lambda \in \mathbb{Z}/\ell\mathbb{Z}$. Hence we have

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

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

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

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

By using Proposition 15, it follows that $\nu_{\mathfrak{l},J'}(\pi^r - \bar{\pi}^r) < \nu_{\mathfrak{l},J}(\pi^r - \bar{\pi}^r)$. 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 $J[\mathfrak{l}^n]$ with degenerate self-pairing, there is at least one point in $J[\mathfrak{l}^n]$ with non-degenerate self-pairing. This point, that we denote by Q, generates the kernel of a descending isogeny

$I' : J \to J''$ such that $\mathrm{End}(J') \simeq \mathrm{End}(J'')$. We assume first that $J'[\mathfrak{l}^n]$ and $J''[\mathfrak{l}^n]$ are not defined over $\mathbb{F}_{q^r}$. Then we have

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

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

6 Endomorphism ring computation - a depth first algorithm

Let ℓ be a fixed prime. Assume that $\mathbb{Z}[\pi, \bar{\pi}]$ is a $\mathcal{O}_{K_0}$-order and that $\ell\mathcal{O}_{K_0} = \mathfrak{l}_1\mathfrak{l}_2$.

A consequence of Proposition 13 is that there are at most $(\ell+1)(\ell+1)$ rational (ℓ,ℓ)-isogenies preserving the real multiplication. Since we can compute (ℓ,ℓ)-isogenies over finite fields [5,2], we use this result to give an algorithm for computing $\nu_{\mathfrak{l},J}(\pi-\bar{\pi})$, and determine endomorphism rings locally at ℓ, by placing them properly in the order lattice as represented in Figure 1.

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 [8, 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 3 and the remark on page 4, 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,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 1, we shall not consider what happens with respect to $\mathfrak{l}_2$, and vice-versa. Our input for computing an (ℓ,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 a cyclic subgroup of $J[\mathfrak{l}_i]$. By Proposition 7, 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 $\nu_{\mathfrak{l},J}(\pi - \bar{\pi})$ 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, 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 [7]. 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.

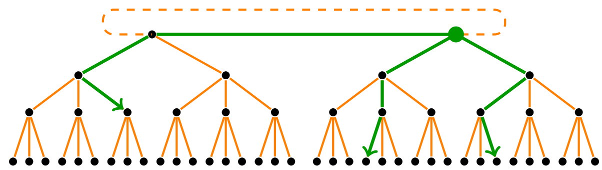

Fig. 4. At least one in three non-backtracking paths has minimum distance to a given level.

Figure 4 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 stability level or below, with respect to $\mathfrak{l}$. We construct a non-backtracking path of (ℓ, ℓ)-isogenies, which are consistently descending with respect to $\mathfrak{l}$. In virtue of Theorem 17, 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 $\nu_{\mathfrak{l},J}(\pi - \bar{\pi})$ 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, ℓ)-isogeny. As said above, this has no impact on the consideration of what happens with respect to $\mathfrak{l}$.

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 17. Things are more subtle for Step 1. Let J_1 be a starting Jacobian, and $I : J_1 \to J_2$ an (ℓ, 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[1], 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 $\mathbb{F}_q$ and u the smallest integer s.t. $\pi^u - 1 \equiv 0 \pmod{\ell\mathcal{O}_K}$, the Frobenius $\pi \in K$ where K is a quartic CM field, and $\alpha = a + b(\pi+\bar{\pi})$ such that $\mathfrak{l} = \alpha\mathcal{O}_K$ divides $\ell\mathcal{O}_K$, and $\mathfrak{l}' = \ell/\mathfrak{l}$.
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 n 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=1,3 **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,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

7 Complexity analysis

In this Section, we give a complexity analysis of Algorithms 1 and 2 and compare its 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 [1]. Computing a bound on ℓ for which one should switch between

[1] Computing isogenous Jacobians by isogenies is easier than computing images of divisors. The `avisogenies` software [2] 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 $\mathbb{F}_q$ and u the smallest integer s.t. $\pi^u - 1 \equiv 0 \pmod{\ell\mathcal{O}_K}$, the Frobenius $\pi \in K$ where K is a quartic CM field, and $\alpha = a + b(\pi + \bar{\pi})$ such that $\mathfrak{l} = \alpha\mathcal{O}_K$ divides $\ell\mathcal{O}_K$, and $\mathfrak{l}' = \ell/\mathfrak{l}$.
We require that J is on or below the second stability level with respect to $\mathfrak{l}$.

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

length $\leftarrow 0$.
while true do
    Compute a basis of $J[\ell^\infty](\mathbb{F}_{q^u})$.
    Let n the largest integer such that $J[\mathfrak{l}^n] \subset J(\mathbb{F}_{q^u})$.
    if $n = 0$ **then**
        return length.
    end if
    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 $\alpha = a + b(\pi + \bar{\pi})$.
    Consider P_1, P_2 a basis of $J[\mathfrak{l}^n](\mathbb{F}_{q^u})$
    Compute $S_{\mathfrak{l},J}$ and take $x_1, x_2 \in \mathbb{P}^1(\mathbb{F}_\ell)$ such that $S_{\mathfrak{l},J}(x_1, x_2) \neq 0$.
    $P \leftarrow \ell^{n-1}(x_1P_1 + x_1P_2)$.
    Pick at random $P_i' \in J_i[\mathfrak{l}'](\mathbb{F}_{q^u})$.
    Compute the (ℓ,ℓ)-isogeny $I : J' \leftarrow J/\langle P, P'\rangle$
    $J \leftarrow J'$.
    length $\leftarrow$ length $+ 1$.
end while

the two algorithms and a full complexity analysis of the algorithm for determining the endomorphism ring completely is beyond the scope of this paper. For completitude, we give a brief description of the Eisenträger-Lauter algorithm [6].

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

$$\alpha = \frac{a + b\pi + c\pi^2 + d\pi^3}{n}, \tag{8}$$

with a, b, c, d, n some integers such that a, b, c, d have no commun factor with n (n is the smallest integer such that $n\alpha \in \mathbb{Z}[\pi]$). Using [6, Prop. 7], we get $\alpha \in \mathrm{End}(J)$ if and only if $a + b\pi + c\pi^2 + d\pi^3$ acts as zero on the n-torsion. Freeman and Lauter show that n divides the index $[\mathcal{O}_K : \mathbb{Z}[\pi]]$ (see [8, Lemma 3.3]). Since $\mathbb{Z}[\pi, \bar{\pi}]$ is 1 or p, we have that n divides $[\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]]$ if $(n, p) = 1$. 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

$$\frac{a + b\pi + c\pi^2 + d\pi^3}{\ell_i^{d_i}},$$

for every prime factor ℓ_i in the factorization of n. The advantage of using this family of elements instead of α 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. Nevertheless, it should be noted that the exponent d_i can be as large as the ℓ_i-valuation of the conductor $[\mathcal{O}_K : \mathbb{Z}[\pi]]$.

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 $\mathbb{F}_q$ [3, §3].

Then we compute the matrix of the Frobenius on the ℓ-torsion. Using this matrix, we may write down the matrices of α_1 and α_2 in terms of the the matrix of $\pi + \bar{\pi}$. Finally, computing $J[\mathfrak{l}_i]$, $i = 1, 2$, is just linear algebra and has negligible cost. Computing the Tate pairing 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, ℓ)-isogeny using the algorithm of Cosset and Robert [5] is $O(M(u)\ell^4)$ operations in $\mathbb{F}_q$. Let h denote the depth of the graph, i.e. $h = \max(\nu_{\mathfrak{l}_1, \mathcal{O}_K}(\pi - \bar{\pi}), \nu_{\mathfrak{l}_2, \mathcal{O}_K}(\pi - \bar{\pi}))$. We conclude that the cost of Algorithms 1 and 2 is $O(hM(u)(u \log q + n\ell^2 + \ell^4))$.

The complexity of Freeman and Lauter's algorithm for endomorphism ring computation is dominated by the cost of computing the ℓ-Sylow group of the Jacobian defined over the extension field containing the $\ell^{u'}$-torsion, where u' is bounded by ℓ-valuation of $[\mathcal{O}_K : \mathbb{Z}[\pi]]$. The degree of this extension field is $u\ell^{u'-u}$ (by Proposition [6, Prop. 6.3]). The costs of the two algorithms are given in Table 1.

Table 1. Cost for computing the endomorphism ring locally at ℓ

Freeman and Lauter	This work (Algorithm 1)
$O(M(u\ell^{u'-u})(u\ell^{u'-u} \log q + u'\ell^2))$	$O(hM(u)(u \log q + n\ell^2 + \ell^4))$

Example 2. Let J be the jacobian of the hyperelliptic curve defined by

$$\begin{aligned} y^2 = {} & 37835078x^6 + 36463111x^5 + 37485984x^4 + 24269474x^3 + \\ & 41922947x^2 + 39564866x + 21448355, \end{aligned}$$

over $\mathbb{F}_p$, with $p = 53050573$. The curve has complex multiplication by $\mathcal{O}_K$, with $K = \mathbb{Q}(\sqrt{175 + 15\sqrt{13}})$. The real multiplication K_0 has class number 1 and 3 is split into K_0. The 3-torsion is defined over an extension of degree 2 and the corresponding valuations of the Frobenius are $\nu_{\alpha_1,\mathcal{O}_K}(\pi - \bar{\pi}) = 10$ and $\nu_{\alpha_2,\mathcal{O}_K}(\pi - \bar{\pi}) = 3$.

8 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. Further research is needed to extend our results to the general case. Our belief is that the good approach to follow is first to determine the real multiplication and secondly to use an algorithm similar to ours to fully compute the endomorphism ring.

9 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. We thank David Gruenewald, Ben Smith and Damien Robert for helpful and inspiring discussions. Finally, we are grateful to Marco Streng for proofreading an early version of this manuscript.

References

1. G. Bisson. Computing endomorphism rings of abelian varieties of dimension two. http://eprint.iacr.org/2012/525.
2. G. Bisson, R. Cosset, and D. Robert. Avisogenies. `http://avisogenies.gforge.inria.fr/`.
3. 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 [2].
4. 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.
5. R. Cosset and D. Robert. Computing (ℓ, ℓ)-isogenies in polynomial time on jacobians of genus 2 curves. *Mathematics of Computation*, 2013.
6. 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.
7. 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.
8. D. Freeman and K. Lauter. Computing endomorphism rings of jacobians of genus 2 curves. In *Symposium on Algebraic Geometry and its Applications, Tahiti*, 2006.

9. E. Goren and K. Lauter. The distance between superspecial abelian varieties with real multiplication. *Journal of Number Theory*, 129(6):1562–1578, 2009.
10. E. Gottschling. Explizite Bestimmung der Randflächen des Fundamentalbereiches der Modulgruppe zweiten Grades. *Math. Ann.*, 138:103–124, 1959.
11. S. Ionica. Pairing-based methods for genus 2 jacobians with maximal endomorphism ring. `http://fr.arxiv.org/abs/1204.0222`.
12. 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.
13. S. Ionica and A. Joux. Pairing the volcano. *Mathematics of Computation*, 82:581–603, 2013.
14. D. Kohel. *Endomorphism rings of elliptic curves over finite fields.* PhD thesis, University of California, Berkeley, 1996.
15. S. Lichtenbaum. Duality theorems for curves over p-adic fields. *Invent.Math.7*, pages 120–136, 1969.
16. D. Lubicz and D. Robert. Computing isogenies between abelian varieties. *Compositio Mathematica*, 2012.
17. V. Miller. The Weil pairing, and its efficient calculation. *Journal of Cryptology*, 17(4):235–261, September 2004.
18. S. L. Schmoyer. The Triviality and Nontriviality of Tate-Lichtenbaum Self-Pairings on Jacobians of curves, 2006. `http://www-users.math.umd.edu/~schmoyer/`.
19. G. Shimura. *Abelian varieties with complex multiplication and modular functions.* Princeton Mathematical Series. Princeton University Press, 1998.
20. M. Streng. *Complex multiplication of abelian surfaces.* Phd thesis, Universiteit Leiden, 2010.

10 Appendix A

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 5.

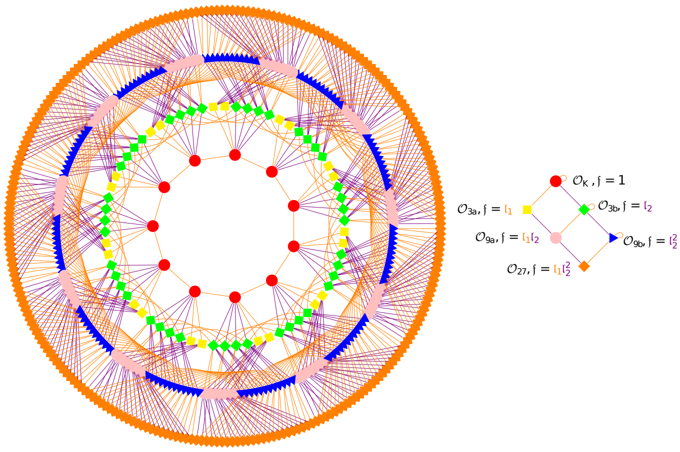

Fig. 5. A larger example