Pairing-based algorithms for jacobians of genus 2 curves with maximal endomorphism ring

Sorina Ionica

Ecole Normale Supérieure**
45 Rue d'Ulm, Paris, 75005, France
sorina.ionica@m4x.org

Abstract. Using Galois cohomology, Schmoyer characterizes cryptographic non-trivial self-pairings of the ℓ-Tate pairing in terms of the action of the Frobenius on the ℓ-torsion of the Jacobian of a genus 2 curve. We apply similar techniques to study the non-degeneracy of the ℓ-Tate pairing restrained to subgroups of the ℓ-torsion which are maximal isotropic with respect to the Weil pairing. First, we deduce a criterion to verify whether the jacobian of a genus 2 curve has maximal endomorphism ring. Secondly, we derive a method to construct horizontal (ℓ, ℓ)-isogenies starting from a jacobian with maximal endomorphism ring.

1 Introduction

A central problem in elliptic and hyperelliptic curve cryptography is that of constructing an elliptic curve or an abelian surface having a given number of points on their Jacobian. The solution to this problem relies on the computation of the Hilbert class polynomial for a quadratic imaginary field in the genus one case. The analogous genus 2 case needs the Igusa class polynomials for quartic CM fields. There are three different methods to compute these polynomials: an analytic algorithm [16], a p-adic algorithm [7] and a Chinese Remainder Theorem-based algorithm [5]. The last one relies heavily on an algorithm for determining endomorphism rings of the jacobians of genus 2 curves over prime fields. Eisenträger and Lauter [5] gave the first algorithm for computing endomorphism rings of Jacobians of genus 2 curves over finite fields. The algorithm takes as input a jacobian J over a finite field and a primitive quartic CM field K, i.e. a purely imaginary quadratic extension field of a real quadratic field with no proper imaginary quadratic fields. The real quadratic subfield K_0 has class number 1. The main idea is to compute a set of generators of an order $\mathcal{O}$ in the CM field and then to test whether these generators are endomorphisms of J, in order to decide whether the order $\mathcal{O}$ is the endomorphism ring $\mathrm{End}(J)$ or not. In view of application to the CRT method for Igusa class polynomial

** This work was carried during the author's stay at the Ecole Polytechnique, team TANC and at LORIA, Nancy, team CARAMEL.

computation, Freeman and Lauter bring a series of improvements to this algorithm, in the particular case where we need to decide whether $\mathrm{End}(J)$ is the maximal order or not. Note that the Eisenträger-Lauter CRT method for class polynomial computation searches for curves defined over some prime field $\mathbb{F}_p$ and belonging to a certain isogeny class. Once such a curve is found, the algorithm keeps the curve only if it has maximal endomorphism ring. This search is rather expensive and ends only when all curves having maximal endomorphism ring were found. Recent research in the area [1, 15, 4] has shown that we can significantly reduce the time of this search by using *horizontal isogenies*, i.e. isogenies between jacobians having the same endomorphism ring. Indeed, once a Jacobian with maximal endomorphism ring is found, many others can be generated from it by computing horizontal isogenies. In this paper, we propose a new method for checking if the endomorphism ring is locally maximal at ℓ, for $\ell > 2$ prime, and a method to compute kernels of horizontal (ℓ, ℓ)-isogenies. Our methods rely on the computation of the Tate pairing.

Let H be a genus 2 smooth irreducible curve defined over a finite field $\mathbb{F}_q$, J its jacobian and suppose that $J[\ell^n] \subseteq J(\mathbb{F}_q)$ and that $J[\ell^{n+1}] \nsubseteq J(\mathbb{F}_q)$, with ℓ different from p and $n \geq 1$. We denote by $\mathcal{W}$ the set of rank 2 subgroups in $J[\ell^n]$, which are isotropic with respect to the ℓ^n-Weil pairing. We define k_ℓ to be

$$k_\ell = \max_{G \in \mathcal{W}} \{k | \exists P, Q \in G \text{ and } T_{\ell^n}(P, Q) \in \mu_{\ell^k} \backslash \mu_{\ell^{k-1}}\}.$$

The jacobian J is ordinary, hence it has complex multiplication by an order in a quartic CM field K. We assume that $K = \mathbb{Q}(\eta)$, with $\eta = i\sqrt{a + b\sqrt{d}}$ if $d \equiv 2, 3 \mod 4$ or $\eta = i\sqrt{a + b\left(\frac{-1+\sqrt{d}}{2}\right)}$ if $d \equiv 1 \mod 4$. We consider the decomposition of the Frobenius endomorphism π over a basis of the ring of integers of K : $\pi = a_1 + a_2\frac{-1+\sqrt{d}}{2} + (a_3 + a_4\frac{-1+\sqrt{d}}{2})\eta$, if $d \equiv 1 \bmod 4$ and $\pi = a_1 + a_2\sqrt{d} + (a_3 + a_4\sqrt{d})\eta$, if $d \equiv 2, 3 \bmod 4$. We assume that the coefficients verify the following condition

$$\max(v_\ell(\frac{a_3 - a_4}{\ell}), v_\ell(\frac{a_3 - \ell a_4}{\ell^2})) < \min(v_\ell(a_3), v_\ell(a_4)). \tag{1}$$

We show that if condition (1) is satisfied, the computation of k_ℓ suffices to check whether the endomorphism ring is locally maximal at ℓ, in many cases. Moreover, our method to distinguish kernels of horizontal (ℓ, ℓ)-isogenies from other (ℓ, ℓ)-isogenies is also related to k_ℓ. Given G an element of $\mathcal{W}$, we say that the Tate pairing is k_ℓ-non-degenerate (or simply non-degenerate) on $G \times G$ if the restriction map

$$T_{\ell^n} : G \times G \to \mu_{\ell^{k_\ell}}$$

is surjective. Otherwise, we say that the Tate pairing is k_ℓ-degenerate (or simply degenerate) on $G \times G$. Our main result is the following theorem.

Theorem 1. *Let H be a genus 2 smooth irreducible curve defined over a finite field $\mathbb{F}_q$ and $\ell > 2$ a prime number. Let J be the jacobian of H, whose endomorphism ring is a locally maximal order at ℓ of a CM-field K. Assume that the real quadratic subfield K_0 has class number 1. Suppose that the Frobenius endomorphism π is such that $\pi - 1$ is exactly divisible by ℓ^n, $n \in \mathbb{Z}$ and that $k_\ell > 0$. Let G be a subgroup of rank 2 in $J[\ell]$ which is isotropic with respect to the Weil pairing. Let $\bar{G}$ be a rank 2 subgroup in $J[\ell^n]$ isotropic with respect to the ℓ^n-Weil pairing and such that $\ell^{n-1}\bar{G} = G$. Then the following hold*

1. *If the isogeny of kernel G is horizontal, then the Tate pairing is k_ℓ-degenerate over $\bar{G} \times \bar{G}$.*
2. *If the condition* (1) *is satisfied and the Tate pairing is k_ℓ-degenerate over $\bar{G} \times \bar{G}$, then the isogeny is horizontal.*

In view of application to the CRT method for Igusa class polynomial computation, we deduce an algorithm to compute kernels of horizontal isogenies efficiently. This generalizes a result on horizontal ℓ-isogenies for genus 1 curves [9].

This paper is organised as follows. In Section 2 we recall briefly the Eisenträger-Lauter algorithm for computing endomorphism rings. In Section 3 we give the definition and properties of the Tate pairing. Section 4 describes our algorithm for checking whether a Jacobian has locally maximal order at ℓ. In Section 5 we show that we can compute kernels of horizontal (ℓ, ℓ)-isogenies by some Tate pairing calculations. Finally, Section 6 gives complexity estimates for our algorithms and compares their performance to that of the Freeman-Lauter algorithm.

Notation and assumptions. In this paper, we assume that principally polarized abelian surfaces are *simple*, i.e. not isogenous to a product of elliptic curves. A quartic CM field K is a totally imaginary quadratic extension of a totally real field. We denote by K_0 the real quadratic subfield of K and we assume that K_0 has class number 1. A CM-type Φ is a couple of pairwise 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 $\mathcal{O}_K$ is given by $A(\mathbb{C}) = \mathbb{C}^2/\Phi(\mathfrak{a})$, where $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$ and Φ is a CM type. This variety is said to be of CM-type (K, Φ). A CM-type (K, Φ) is primitive if Φ cannot be obtained as a lift of a CM-type of a CM-subfield of K. The principally polarized abelian variety $\mathbb{C}^2/\Phi(\mathfrak{a})$ is simple if and only if its CM-type is *primitive* [14].

2 Computing the endomorphism ring of a jacobian

The endomorphism ring of an ordinary jacobian J over a finite field $\mathbb{F}_q$ $(q = p^n)$ is an order in a 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. We give a brief description of the Eisenträger-Lauter algorithm [5] which computes the endomorphism ring of J. 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

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

with a, b, c, d, n some integers such that a, b, c, d have no common factor with n (n is the smallest integer such that $n\alpha \in \mathbb{Z}[\pi]$). The LLL algorithm computes a sequence a, b, c, d, n such that α can be written as in Equation 2. In order to check whether α is an endomorphism or not, Eisenträger and Lauter [5] use the following result.

Lemma 1. *Let A be an abelian variety defined over a field k and n an integer coprime to the characteristic of k. Let $\alpha : A \to A$ be an endomorphism of A. Then $A[n] \subset Ker\ \alpha$ if and only if there is another endomorphism β of A such that $\alpha = n \cdot \beta$.*

Using Lemma 1, 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 [6, Lemma 3.3]). Since $[\mathbb{Z}[\pi] : \mathbb{Z}[\pi,\bar{\pi}]$ 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. For a fixed prime ℓ, Freeman and Lauter prove the following result, which allows computing a bound for the degree of the smallest extension field over which the ℓ-torsion points are defined.

Proposition 1. *[6, Prop. 6.2] Let J be the Jacobian of a genus 2 curve over $\mathbb{F}_q$ and suppose that $End(J)$ is isomorphic to the ring of integers $\mathcal{O}_K$ of the primitive quartic CM field K. Let $\ell \neq q$ be a prime number, and suppose $\mathbb{F}_{p^r}$ is the smallest field over which the points of $J[\ell]$ are defined. If ℓ is unramified in K, then r divides one of the following:*

(a) $\ell - 1$, if ℓ splits completely in K;
(b) $\ell^2 - 1$, if ℓ splits into two or three ideals in K;
(c) $\ell^3 - \ell^2 + \ell - 1$, if ℓ is inert in K.

If ℓ ramifies in K, then r divides one of the following:

(a) $\ell^3 - \ell^2$, if there is a prime over ℓ of ramification degree 3, or if ℓ is totally ramified in K and $\ell \leq 3$.
(b) $\ell^2 - \ell$, in all other cases where ℓ factors into four prime ideals in K (counting multiplicities).
(c) $\ell^3 - \ell$, if ℓ factors into two or three prime ideals in K (counting multiplicities).

Once we computed the extension field over which the ℓ-torsion is defined, the ℓ^d-torsion will be computed using the following result [6].

Proposition 2. *[6, Prop. 6.3] Let A be an ordinary abelian variety defined over a finite field $\mathbb{F}_q$ and let ℓ be a prime number not equal to the characteristic of $\mathbb{F}_q$. Let d be a positive integer. If the ℓ-torsion points of A are defined over $\mathbb{F}_q$, then the ℓ^d-torsion points are defined over $\mathbb{F}_{q^{\ell^{d-1}}}$.*

3 Background on the Tate pairing

Consider now H a smooth irreducible genus 2 curve defined over a finite field $\mathbb{F}_q$, with $q = p^r$, whose equation is

$$y^2 + h(x)y = f(x), \tag{3}$$

with $h, f \in \mathbb{F}_q[x]$, $\deg h \leq 2$, f monic and $\deg f = 5, 6$. Let J be the jacobian of H and denote by $\bar{\mathbb{F}}_q$ the algebraic closure of $\mathbb{F}_q$ and by $G_{\bar{\mathbb{F}}_q/\mathbb{F}_q} = \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ the Galois group. Let $m \in \mathbb{N}$ and consider $J[m]$ the subgroup of m-torsion, i.e. the points of order m. We denote by $\mu_m \subset \bar{\mathbb{F}}_q$ the group of m-th roots of unity. The m-Weil pairing

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

is a bilinear, non-degenerate map and it commutes with the action of G. If $\lambda : A \to \hat{A}$ is a polarization, then we define the Weil pairing as

$$\begin{aligned} W_m^\lambda : J[m] \times J[m] &\to \mu_m \\ (P, Q) &\to W_m(P, \lambda(Q)). \end{aligned}$$

Given a subgroup $G \subset J[m]$, we say that G is *isotropic* with respect to the Weil pairing if the Weil pairing restricted to $G \times G$ is trivial. It is *maximal isotropic* if it is isotropic and it is not properly contained in any other such subgroup. We denote by $H^i(G_{\bar{\mathbb{F}}_q/\mathbb{F}_q}, J)$ the i-th Galois cohomology group, for $i \geq 0$.

Consider the exact sequence $0 \to J[m] \to J(\bar{\mathbb{F}}_q) \to J(\bar{\mathbb{F}}_q) \to 0$. Then by taking Galois cohomology we get the connecting morphism

$$\begin{aligned} \delta : J(\mathbb{F}_q)/mJ(\mathbb{F}_q) = H^0(G_{\bar{\mathbb{F}}_q/\mathbb{F}_q}, J)/mH^0(G_{\bar{\mathbb{F}}_q/\mathbb{F}_q}, J) &\to H^1(G_{\bar{\mathbb{F}}_q/\mathbb{F}_q}, J[m]) \\ P &\to F_P, \end{aligned}$$

where the map F_P is defined as follows

$$\begin{aligned} F_P : G_{\bar{\mathbb{F}}_q/\mathbb{F}_q} &\to J(\bar{\mathbb{F}}_q)[m] \\ \sigma &\to \sigma(\bar{P}) - \bar{P}, \end{aligned}$$

where $\bar{P}$ is any point such that $m\bar{P} = P$. Using the connecting morphism and the Weil pairing, we define the m-Tate pairing as follows

$$\begin{aligned} t_m : J(\mathbb{F}_q)/mJ(\mathbb{F}_q) \times \hat{J}[m](\mathbb{F}_q) &\to H^1(G, \mu_m) \\ (P, Q) &\to [\sigma \to W_m(F_P(\sigma), Q)]. \end{aligned}$$

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

$$\begin{aligned} t_m^\lambda : J(\mathbb{F}_q)/mJ(\mathbb{F}_q) \times J[m](\mathbb{F}_q) &\to \mathbb{F}_q^*/\mathbb{F}_q^{*m} \\ (P, Q) &\to t_m(P, \lambda(Q)). \end{aligned}$$

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 [11] describes a version of the Tate pairing on Jacobian varieties. More precisely, suppose we have $m|\#J(\mathbb{F}_q)$ and denote by k the *embedding degree with respect to* m, i.e. the smallest integer $k \geq 0$ such that $m|q^k - 1$. Let $D_1 \in J(\mathbb{F}_{q^k})$ and $D_2 \in J[m](\mathbb{F}_{q^k})$ 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 Tate pairing of the divisor classes D_1 and D_2 is computed as

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

Moreover, in computational applications, it is convenient to work with a unique value of the pairing. Given that $\mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^m \simeq \mu_m$, we use the *reduced Tate pairing*, given by

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

The function $f_{m,D_2}(D_1)$ is computed using Miller's algorithm [12] in $O(\log m)$ operations in $\mathbb{F}_{q^k}$. Since $H^1(G_{\bar{\mathbb{F}}_{q^k}/\mathbb{F}_{q^k}}, \mu_m) \simeq \mu_m$ by Hilbert's 90 theorem, it follows that there is an isomorphism $H^1(G_{\bar{\mathbb{F}}_{q^k}/\mathbb{F}_{q^k}}, \mu_m) \simeq H^1(\mathrm{Gal}(\mathbb{F}_{q^{km}}/\mathbb{F}_{q^k}), \mu_m)$. Since $H^1(Gal(\mathbb{F}_{q^{km}}/\mathbb{F}_{q^k}), \mu_m) \simeq \mu_m$, we may compute the Tate pairing as

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

where π is the Frobenius of the finite field $\mathbb{F}_{q^k}$.

4 Pairings and endomorphism ring computation

In this section we relate some properties of the Tate pairing to the isomorphism class of the endomorphism ring of the Jacobian. Let ℓ be a prime odd number. We give a method to check whether the endomorphism ring is locally maximal at ℓ (i.e. the index $[\mathcal{O}_K : \mathcal{O}]$ is not divisible by ℓ) by computing a certain number of pairings.

Let H be a genus 2 smooth irreducible curve defined over a finite field $\mathbb{F}_q$, J its jacobian and suppose that $J[\ell^n] \subseteq J(\mathbb{F}_q)$ and that $J[\ell^{n+1}] \not\subseteq J(\mathbb{F}_q)$.

Lemma 2. *The reduced Tate pairing defined as*

$$T_{\ell^n} : J[\ell^n] \times J[\ell^n] \to \mu_{\ell^n}$$

is k_ℓ-antisymmetric, i.e. $T_{\ell^n}(\bar{D}_1, \bar{D}_2)T_{\ell^n}(\bar{D}_2, \bar{D}_1) \in \mu_{\ell^{k_\ell}}$, for all $\bar{D}_1, \bar{D}_2 \in J[\ell^n]$.

Proof. Indeed, assume that there are $\bar{D}_1, \bar{D}_2 \in J[\ell^n]$ such that $T_{\ell^n}(\bar{D}_1, \bar{D}_2)T_{\ell^n}(D_2, \bar{D}_1) \in \mu_{\ell^n} \backslash \mu_{\ell^{k_\ell}}$. We denote by $G = \langle \bar{D}_1, \bar{D}_2 \rangle$ and by $r > k_\ell$ the largest integer such that $T_{\ell^n}(\bar{D}_1, \bar{D}_2)T_{\ell^n}(\bar{D}_2, \bar{D}_1)$ is an ℓ^r-th primitive root of unity. Then the polynomial

$$\mathcal{P}(a, b) = \log T_{\ell^n}(\bar{D}_1, \bar{D}_1)a^2 + \log(T_{\ell^n}(\bar{D}_1, \bar{D}_2)T_{\ell^n}(\bar{D}_2, \bar{D}_1))ab + \log T_{\ell^n}(\bar{D}_2, \bar{D}_2)b^2,$$

where the log function is computed with respect to some fixed ℓ^n-th root of unity, is zero mod ℓ^{n-r-1} and non-zero mod ℓ^{n-r}. Dividing by ℓ^{n-r-1}, we may view $\mathcal{P}$ as a polynomial in $\mathbb{F}_\ell[a, b]$. Since $\mathcal{P}$ is a quadratic non-zero polynomial, it has at most two roots. These correspond to two divisor classes in G, with r-degenerate self-pairing. Hence, there is at least one divisor $\bar{D} \in G$ such that $T_{\ell^n}(\bar{D}, \bar{D})$ is a ℓ^r-th root of unity. Since there is at least one maximal isotropic subgroup $W \in \mathcal{W}$ with respect to the Weil pairing such that $\bar{D} \in W$, this contradicts the definition of k_ℓ.

Let $\mathcal{O}$ be an order of K and let $\theta \in \mathcal{O}$. We define

$$v_{\ell,\mathcal{O}}(\theta) := \max_{m \geq 0}\{m : \theta \in \mathbb{Z} + \ell^m \mathcal{O}\}.$$

We denote by $1, \delta, \gamma, \eta$ a $\mathbb{Z}$-basis of $\mathcal{O}$ and and we write $\theta = a_1 + a_2\delta + a_3\gamma + a_4\eta$. Then we compute $v_{\ell,\mathcal{O}}$ as

$$v_{\ell,\mathcal{O}}(\theta) = v_\ell(\gcd(a_2, a_3, a_4)). \tag{4}$$

Note that the value of $v_{\ell,\mathcal{O}}(\theta)$ is independent of the choice of the basis. We say that θ is divisible by $t \in \mathbb{Z}$ if we have $\theta \in t\mathcal{O}$. We say that θ is exactly divisible by ℓ^n if it is divisible by ℓ^n and it is not divisible by ℓ^{n+1}. The following lemma gives a criterion to check whether an order is locally maximal at ℓ or not.

Lemma 3. *Let $K := \mathbb{Q}(\eta)$ be a quartic CM field, with $\eta = i\sqrt{a + b\frac{-1+\sqrt{d}}{2}}$, if $d \equiv 1 \bmod 4$ and $\eta = i\sqrt{a + b\sqrt{d}}$, if $d \equiv 2, 3 \bmod 4$. We assume that $a, b, d \in \mathbb{Z}$ and that d and $a^2 - b^2d$ are square free. Assume that $K_0 = \mathbb{Q}(\sqrt{d})$ has class* *number 1. Let $\ell > 2$ a prime number that does not divide $lcm(a, b, d)$. Let $\mathcal{O}_K$ be the maximal order of K and $\mathcal{O}$ an order such that $[\mathcal{O}_K : \mathcal{O}]$ is divisible by ℓ. Let $\pi \in \mathcal{O}$ such that $N_{K/K_0}(\pi) \in \mathbb{Z}$ is not divisible by ℓ and that $v_{\ell,\mathcal{O}_K}(\pi) > 0$. We suppose that $\pi = a_1 + a_2\frac{-1+\sqrt{d}}{2} + (a_3 + a_4\frac{-1+\sqrt{d}}{2})\eta$, if $d \equiv 1 \bmod 4$ and $\pi = a_1+a_2\sqrt{d}+(a_3+a_4\sqrt{d})\eta$, if $d \equiv 2, 3 \bmod 4$. If $\max(v_\ell(\frac{a_3-a_4}{\ell}), v_\ell(\frac{a_3-\ell a_4}{\ell^2})) < \min(v_\ell(a_3), v_\ell(a_4))$, then $v_{\ell,\mathcal{O}}(\pi) < v_{\ell,\mathcal{O}_K}(\pi)$.*

Proof. We denote by $\mathcal{O}_1 = \mathcal{O}_{K_0} + \mathcal{O}_{K_0}\eta$. Since $\ell > 2$, it suffices to show that $v_{\ell,\mathcal{O}\cap\mathcal{O}_1}(\pi) < v_{\ell,\mathcal{O}_1}(\pi)$. We will therefore assume, without restricting the generality, that $\mathcal{O} \subset \mathcal{O}_1$. Let $\delta = \frac{-1+\sqrt{d}}{2}$ if $d \equiv 1 \bmod 4$ and $\delta = \sqrt{d}$, if $d \equiv 2, 3 \bmod 4$ and let $\gamma := \delta\eta$. Then $1, \delta, \gamma, \eta$ is a basis for $\mathcal{O}_1$. We write $\pi = a_1+a_2\delta+a_3\gamma+a_4\eta$. By writing down the norm condition for $d \equiv 2, 3 \bmod 4$

$$\left(a_1 + a_2\sqrt{d} + (a_3 + a_4\sqrt{d})i\sqrt{a + b\sqrt{d}}\right)\left(a_1 + a_2\sqrt{d} - (a_3 + a_4\sqrt{d})i\sqrt{a + b\sqrt{d}}\right) \in \mathbb{Z},$$

we get that

$$2a_1a_2 + a_3^2b + a_4^2bd + 2aa_3a_4 = 0. \quad (5)$$

Similarly, for $d \equiv 1 \bmod 4$, we have

$$-\frac{a_2^2}{2} + a_1a_2 - \frac{aa_4^2}{2} + a_3a_4(a - b) + \frac{a_3^2b}{2} + \frac{a_4^2(1 + d)b}{8} - \frac{a_4^2(2a - b)}{4} = 0. \quad (6)$$

Since $\ell \nmid a_1$, equations (5) and (4) imply that $v_\ell(a_2) > \min(v_\ell(a_3), v_\ell(a_4))$. Since there is always an order $\mathcal{O}'$ such that $\mathcal{O} \subset \mathcal{O}' \subset \mathcal{O}_1$ such that $[\mathcal{O}_1 : \mathcal{O}']$ is a power of ℓ, it suffices to prove the lemma in the case $[\mathcal{O}_1 : \mathcal{O}]$ is a power of ℓ. For the order $\mathcal{O}$, we choose $\{1, \delta', \gamma', \eta'\}$ a HNF basis with respect to $\{1, \delta, \gamma, \eta\}$. We denote by $(a_{i,j})_{1\le i,j\le 4}$ the corresponding transformation matrix. Then $[\mathcal{O}_1 : \mathcal{O}] = \prod_{1\le i\le 4} a_{i,i}$. Note that neither η nor γ are in $\mathcal{O}$. Otherwise, $\mathcal{O}$ is the maximal order. Indeed, assume $\eta \in \mathcal{O}$. Since ℓ divides neither a nor b, it follows that $\delta \in \mathcal{O}$. This implies that $\mathcal{O}$ is $\mathcal{O}_1$. We consider the decomposition of π over the basis $\{1, \delta', \gamma', \eta'\}$

$$\pi = a_1' + a_2'\delta' + a_3'\gamma' + a_4'\eta', a_i' \in \mathbb{Z}.$$

Since $\eta \notin \mathcal{O}$, we know that a_{44} is ℓ. If a_{33} is divisible by ℓ, then $v_\ell(a_3') < v_\ell(a_3)$. If $a_{34} = 1$, then $a_4' = -(a_3 - \ell a_4)/\ell^2$. If $a_{34} = 0$, then $a_4' = a_4/\ell$. If $a_{33} = 1$, it follows that $a_{34} = 1$ (otherwise we would have $\gamma \in \mathcal{O}$). Then $a_3' = a_3$ and $a_4' = -(a_3 - a_4)/\ell$. We conclude that $v_{\ell,\mathcal{O}}(\pi) < v_{\ell,\mathcal{O}_K}(\pi)$.

Since we know that $J[\ell^n]$ is $\mathbb{F}_q$-rational, while $J[\ell^{n+1}]$ is not, Lemma 1 implies that $\pi - 1$ is exactly divisible by ℓ^n. Moreover, the Frobenius matrix on the Tate module is the identity matrix $I_4 \bmod \ell^n$. In following lemma, we compute the matrix of the Frobenius on the Tate module.

Lemma 4. *Let J be a abelian surface defined over a finite field $\mathbb{F}_q$ and π the Frobenius endomorphism. Then the largest integer m such that the matrix of the Frobenius endomorphism on the ℓ-Tate module is of the form*

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

is $v_{\ell,\mathcal{O}}(\pi)$, where $\mathcal{O}$ is the endomorphism ring of J.

Proof. Let m be the largest integer such that the matrix of the Frobenius on $J[\ell^m]$ has the form given in Equation (7). Let $\mathcal{O}$ be the endomorphism ring of J. We denote by $\{1, \delta, \gamma, \eta\}$ the $\mathbb{Z}$-basis of $\mathcal{O}$ and by $\pi = a_1 + a_2\delta + a_3\gamma + a_4\eta$ the decomposition of π over this basis. It is obvious that $m \geq v_\ell(\gcd(a_2, a_3, a_4))$. For the converse, we note that $\pi - \lambda$ kills the ℓ^m-torsion, hence we may write $\pi - \lambda = \ell^m\alpha$, with $\alpha \in \mathrm{End}(J)$. We write down the decomposition of α over the basis $\{1, \delta, \gamma, \eta\}$ and conclude that $\ell^m | \gcd(a_2, a_3, a_4)$. Hence $m \leq v_\ell(\gcd(a_2, a_3, a_4))$. We conclude that $m = v_\ell(\gcd(a_2, a_3, a_4))$, hence $m = v_{\ell,\mathcal{O}}(\pi)$ by (4).

Using Galois cohomology, Schmoyer [13] computes the matrix of the Frobenius on the Tate module, up to a certain precision, if the self-pairings of the Tate pairing are degenerate. We use a similar approach and show that the precision up to which the Frobenius acts on the Tate module as a multiple of the identity is $2n - k_\ell$. Consequently, we recover information on the conductor of the endomorphism ring of J by computing k_ℓ. For $m \in \mathbb{Z}$, we will use a *symplectic basis* of $J[\ell^m]$, i.e. a basis such that the matrix associated to the ℓ^m-Weil pairing is

$$\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} \bmod \ell^m. \tag{8}$$

Proposition 3. *Let H be a hyperelliptic smooth irreducible curve defined over a finite field $\mathbb{F}_q$, and J its jacobian. Suppose that the Frobenius endomorphism π is such that $\pi - 1$ is exactly divisible by ℓ^n, for $\ell \geq 3$ prime. Then if $v_{\ell,End(J)}(\pi) < 2n$, we have*

$$v_{\ell,End(J)}(\pi) = 2n - k_\ell. \tag{9}$$

Proof. Let $\{Q_1, Q_2, Q_{-1}, Q_{-2}\}$ a symplectic basis for the ℓ^{2n}-torsion (whose matrix is given by Equation (8)) and let $\pi(Q_g) = \sum_{h=-2}^{2} a_{h,g}Q_h$, with $(a_{h,g})_{h,g\in\{-2,-1,1,2\}}$ in $\mathbb{Z}$. By bilinearity, we have that

$$\begin{aligned} T_{\ell^n}(\ell^n Q_i, \ell^n Q_j) = W_{\ell^{2n}}(Q_i, \pi(Q_j) - Q_j) &= W_{\ell^{2n}}(Q_i, \sum_{\substack{h=-2 \\ h\neq 0}}^{2} a_{h,j}Q_h - Q_j) \\ &= W_{\ell^{2n}}(Q_i, Q_j)^{a_{j,j}-1} \prod_{\substack{h=-2 \\ h\neq 0,j}}^{2} W_{\ell^{2n}}(Q_i, Q_h)^{a_{h,j}}. \end{aligned}$$

If $j \neq -i$, we have that $T_{\ell^n}(\ell^n Q_i, \ell^n Q_j) \in \mu_{\ell^{k_\ell}}$. It follows that

$$a_{-i,j} \equiv 0 \pmod{\ell^{2n-k_\ell}}, \tag{10}$$

for $i \neq -j$. If $j = -i$, then $T_{\ell^n}(\ell^n Q_i, \ell^n Q_j) = W_{\ell^{2n}}(Q_i, Q_j)^{a_{j,j}-1}$. Since the Tate pairing is k_ℓ-antisymmetric we get

$$a_{i,i} \equiv a_{-i,-i} \pmod{\ell^{2n-k_\ell}}.$$

It remains to prove that $a_{i,i} \equiv a_{j,j}$, for $i, j \in \{-2,-1,1,2\}$. Note that by Galois invariance, we have $W_{\ell^{2n}}(\pi(Q_i), \pi(Q_j)) = \pi(W_{\ell^{2n}}(Q_i, Q_j)) = W_{\ell^{2n}}(Q_i, Q_j)^q$. For $i = -j$ we have

$$W_{\ell^{2n}}(\pi(Q_i), \pi(Q_{-i})) = W_{\ell^{2n}}\Big(\sum_{\substack{h=-2\\h\neq 0}}^{2} a_{h,i}Q_h, \sum_{\substack{g=-2\\g\neq 0}}^{2} a_{g,-i}Q_g\Big)$$

$$= \prod_{\substack{h=-2\\h\neq 0}}^{2}\prod_{\substack{g=-2\\g\neq 0}}^{2} W_{\ell^{2n}}(a_{h,i}Q_h, a_{g,-i}Q_g) = W_{\ell^{2n}}(Q_i, Q_{-i})^{a_{i,i}a_{-i,-i}} \prod_{\substack{h=-2\\h\neq 0,i}}^{2} W_{\ell^{2n}}(a_{h,i}Q_h, a_{-i,-i}Q_{-i})$$

$$\cdot \prod_{\substack{g=-2\\g\neq 0,-i}}^{2} W_{\ell^{2n}}(a_{i,i}Q_i, a_{g,-i}Q_g) \prod_{\substack{s=-2\\s\neq 0,i}}^{2}\prod_{\substack{t=-2\\t\neq 0,-i}}^{2} W_{\ell^{2n}}(Q_s, Q_t)^{a_{s,i}a_{t,-i}}$$

Since $\{Q_1, Q_2, Q_{-1}, Q_{-2}\}$ is a symplectic basis and that $a_{h,g} \equiv 0 \pmod{\ell^n}$, for $h \neq -g$, then

$$W_{\ell^{2n}}(\pi(Q_i), \pi(Q_{-i})) = W_{\ell^{2n}}^{a_{i,i}a_{-i,-i}}(Q_i, Q_{-i}).$$

Since $a_{i,i} \equiv a_{-i,-i} \pmod{\ell^{2n-k_\ell}}$, it follows that

$$a_{i,i}^2 \equiv q \text{ for all } i \in \{-2,-1,1,2\}.$$

Since $a_{i,i} \equiv 1 \pmod{\ell^n}$, it follows that $a_{i,i} \equiv b \pmod{\ell^{2n-k_\ell}}$, for some $b \in \mathbb{Z}$. By Lemma 4, we have $2n - k_\ell \leq v_{\ell,\mathrm{End}J}(\pi)$. For the converse, let $k = 2n - v_{\ell,\mathrm{End}J}(\pi)$ and R, S be two points in $J[\ell^n]$ such that $W_\ell(R,S) = 1$. It suffices to show that $T_{\ell^n}(R,S)$ is k-degenerate. We write $\pi - 1 = a_1 + a_2\alpha + a_3\beta + a_4\theta$, where $1, \alpha, \beta, \theta$ form a $\mathbb{Z}$-basis of $\mathrm{End}(J)$. We take $\bar{S}$ such that $S = \ell^n \bar{S}$ and we get

$$\begin{aligned} T_{\ell^n}(R,S) &= W_{\ell^n}(R, (\pi-1)(\bar{S})) = \\ &= W_{\ell^n}(R,S)^{\frac{a_1}{\ell^n}} W_{\ell^n}\Big(R, \big(\frac{a_2}{\ell^{2n-k}}\delta + \frac{a_3}{\ell^{2n-k}}\gamma + \frac{a_4}{\ell^{2n-k}}\eta\big)(S)\Big)^{\ell^{n-k}}. \end{aligned}$$

Since $W_\ell(R,S) = 1$ and $v_\ell(\gcd(a_2,a_3,a_4)) = \ell^{2n-k}$, we have $T_{\ell^n}(R,S) \in \mu_{\ell^k}$. Hence $k \geq k_\ell$. This concludes the proof.

Proposition 3 gives a method to compute to compute $v_{\ell,\mathrm{End}J}(\pi)$ using pairings. Together with Lemma 3, this gives a criterion to check whether the endomorphism ring of a jacobian is locally maximal at ℓ.

Theorem 2. *Let H be a smooth irreducible genus 2 curve defined over a finite field $\mathbb{F}_q$ and J its jacobian. Suppose that the Frobenius endomorphism π is exactly divisible by ℓ^n, $n \in \mathbb{Z}$ and that the conditions in Lemma 3 are satisfied. Then if $v_{\ell,\mathcal{O}_K}(\pi) < 2n$, End$(J)$ is a locally maximal order at ℓ if and only if k_ℓ equals $2n - v_{\ell,\mathcal{O}_K}(\pi)$.*

Proof. By Proposition 3, k_ℓ equals $2n - v_{\ell^n,\mathcal{O}}(\pi)$, where $\mathcal{O} \simeq \mathrm{End}(J)$. By Lemma 3, the value of $v_{\ell^n,\mathcal{O}_K}(\pi)$ uniquely characterizes orders which are locally maximal at ℓ.

Remark 1. Let $\pi = 1+a_1+a_2\delta+a_3\gamma+a_4\eta$ be the decomposition of the Frobenius over a $\mathbb{Z}$-basis of $\mathcal{O}_K$. We deduce that $k_\ell > 0$ if and only if $v_\ell(\gcd(a_2, a_3, a_4)) < 2v_\ell(\gcd(a_1, a_2, a_3, a_4))$.

We conclude this section by giving in Algorithm 1 a computational method which verifies whether the jacobian J of a genus 2 curve has locally maximal endomorphism ring. If $k_\ell = 0$, the algorithm aborts. By Lemma 4, computing k_ℓ is equivalent to computing the greatest power of ℓ dividing all coefficients $a_{i,j}$, with $i \neq j$ of the matrix of the Frobenius on the Tate module. Equation 10 shows that in order to compute the ℓ-adic valuation of these coefficients, it suffices to determine all the values $T_{\ell^n}(Q_i, Q_j)$, for $i \neq j$.

5 Application to horizontal isogeny computation

In this section, we are interested in computing *horizontal* isogenies, i.e. isogenies between Jacobians having the same endomorphism ring. Note that if $I : J_1 \to J_2$ is an isogeny such that J_1 has maximal endomorphism ring at ℓ, we distinguish two cases: either End(J_2) is locally maximal at ℓ, or End$(J_2) \subset$ End(J_1). In the last case we say that the isogeny is *descending*.

Over the complex numbers, horizontal isogenies are given in terms of the action of the Shimura class group [14]. Let Φ be a CM-type and let A be an abelian surface over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$, given by $A = \mathbb{C}^2/\Phi(I^{-1})$, where I is an ideal of $\mathcal{O}_K$. The surface is principally polarized if there is a purely imaginary $\xi \in \mathcal{O}_K$ with $\mathrm{Im}(\Phi_i(\xi)) > 0$, for $i \in \{1, 2\}$, and such that $\xi\mathfrak{D}_K = I\bar{I}$ (where $\mathfrak{D}_K$ is the different $\{\alpha \in \mathcal{O}_K : \mathrm{Tr}_{K/\mathbb{Q}}(\alpha\mathcal{O}_K) \subset \mathbb{Z}\}$). Computing horizontal isogenies is usually done by using the action of the Shimura class group [14]. This group, that we denote by $\mathfrak{C}(K)$, is defined as

$$\{(\mathfrak{a}, \alpha) | \mathfrak{a} \text{ is a fractional } \mathcal{O}_K\text{-ideal with } \mathfrak{a}\bar{\mathfrak{a}} = (\alpha) \text{ with } \alpha \in K_0 \text{ totally positive}\}/\sim,$$

where $(\mathfrak{a}, \alpha) \sim (\mathfrak{b}, \beta)$ if and only if there exists $u \in K^*$ with $\mathfrak{b} = u\mathfrak{a}$ and $\beta = u\bar{u}\alpha$. The action of $(\mathfrak{a}, \alpha) \in \mathfrak{C}(K)$ on an principally polarized abelian surface given by (I, ξ) is given by the ideal $(\mathfrak{a}I, \alpha\xi)$. This action is transitive and free [14, §14.6].

If the norm of $\mathfrak{a}$ is coprime to the discriminant of $\mathbb{Z}[\pi, \bar{\pi}]$, the kernel of the horizontal isogeny corresponding to $\mathfrak{a}$ is a subgroup of the ℓ-torsion invariant under the Frobenius endomorphism. Hence in order to compute the kernel, we

Algorithm 1 Checking whether the endomorphism ring is locally maximal

INPUT: A jacobian J of a genus 2 curve defined over $\mathbb{F}_q$ such that $J[\ell^n] \subset J(\mathbb{F}_q)$, the Frobenius π, a symplectic basis $(Q_1, Q_2, Q_{-1}, Q_{-2})$ for $J[\ell^n]$

OUTPUT: The algorithm outputs true if $\mathrm{End}(J)$ is maximal at ℓ.

for all $i, j \in \{1, 2, -1, -2\}$ **do**
  if $i \neq -j$ **then**
    Compute $t_{i,j} \leftarrow T_{\ell^n}(Q_i, Q_j)$,
  else
    $t_{i,j} \leftarrow T_{\ell^n}(Q_i, Q_j) T_{\ell^n}(Q_j, Q_i)$
  end if
end for
Let Count $\leftarrow 0$ and check $\leftarrow -1$.
while check $\neq$ Count **do**
  check $\leftarrow$ Count
  for all $i, j \in \{1, 2, -1, -2\}$ **do**
    if $t_{i,j} \neq 1$ **then**
      Let $t_{i,j} = t_{i,j}^{\ell}$
      check $\leftarrow -1$
    end if
  end for
  if check $\neq$ Count **then**
    Count $=$ Count $+ 1$
  end if
end while
$k_\ell \leftarrow n -$ Count
if Count $= 0$ **then**
  abort
end if
if $k_\ell = 2n - v_{\ell,\mathcal{O}_K}(\pi)$ **then**
  return true
else
  return false
end if

need to compute the matrix of the Frobenius for some basis of the ℓ-torsion and then determine subspaces which are invariant by this matrix (see [2, Algorithm VI.3.4]). We show that, when a Jacobian with locally maximal order at ℓ is given, kernels of (ℓ, ℓ)-horizontal isogenies are subgroups on which the Tate pairing is degenerate. This result holds for any $\ell > 2$ and is independent of the value of the discriminant of $\mathbb{Z}[\pi, \bar{\pi}]$. The resulting algorithm, whose complexity is analysed in Section 6, computes kernels of horizontal isogenies with only a few pairing computations.

We state the following lemma for jacobians of genus 2 curves over finite fields, which are the framework for this paper. We note that the result holds for abelian varieties in general.

Lemma 5. *(a) Let J_1, J_2 be jacobians of genus 2 smooth irreducible curves defined over a finite field $\mathbb{F}_q$ and $I : J_1 \to J_2$ an isogeny defined over $\mathbb{F}_q$ which* *splits multiplication by d. Let $\lambda : J_1 \to \hat{J}_1$ be a principal polarization. Then for $P \in J_1(K)$, $Q \in J_1[m](K)$ we have*

$$T_m^{\lambda_I}(I(P), I(Q)) = T_m^{\lambda}(P, Q)^d,$$

where $\lambda_I : J_2 \to \hat{J}_2$ is the principal polarization such that $I \circ \lambda_I \circ \check{I} = d \circ \lambda$.

(b) Let J_1, J_2 be jacobians of genus 2 smooth irreducible curves defined over $\mathbb{F}_q$ and $I : J_1 \to J_2$ an isogeny defined over $\mathbb{F}_q$ which splits multiplication by m. Let $P \in J_1(K)$, $Q \in J_1[mm'](K)$ such that $I(Q)$ is a m'-torsion point.

$$T_{m'}^{\lambda_I}(I(P), I(Q)) = T_{mm'}^{\lambda}(P, Q)^m,$$

where λ_I is a principal polarization of J_2 such that $I \circ \lambda_I \circ \check{I} = m \circ \lambda$.

Proof. (a) It is easy to check that $\delta(I(P)) = I(\delta(P))$. Hence for $\sigma \in G_K$ we have

$$W_m(F_{I(P)}(\sigma), I(Q)) = W_m(I(F_P(\sigma)), I(Q)).$$

By using [10, Proposition 13.2.b]

$$W_m^{\lambda_I}(I(F_P(\sigma)), I(Q)) = W_m^{\check{I} \circ \lambda_I \circ I}(F_P(\sigma), Q).$$

(b) The proof is immediate by using (a) and the fact that $T_{mm'}(I(P), I(Q)) = T_{m'}(I(P), I(Q))$.

Lemma 6. *Let $H/\mathbb{F}_q$ be a smooth irreducible curve and D_1, D_2 are two elements of $J(\mathbb{F}_q)$ of order ℓ^n, $n \geq 1$. Let $\bar{D}_1, \bar{D}_2 \in J(\mathbb{F}_q)$ such that $\ell\bar{D}_1 = D_1$ and $\ell\bar{D}_2 = D_2$. Then we have*

(a) If $\bar{D}_1, \bar{D}_2 \in J(\mathbb{F}_q)$, then

$$T_{\ell^{n+1}}(\bar{D}_1, \bar{D}_2)^{\ell^2} = T_{\ell^n}(D_1, D_2).$$

(b) Suppose $\ell \geq 3$. If $\bar{D}_1 \in J(\bar{\mathbb{F}}_q) \backslash J(\mathbb{F}_q)$, then

$$T_{\ell^{n+1}}(\bar{D}_1, \bar{D}_2)^{\ell} = T_{\ell^n}(D_1, D_2).$$

Proof. The proof is similar to to the one of [8, Lemma 4.6]. For completeness, we detail it in Appendice 9.

We may now prove Theorem 1.

Proof of Theorem 1. We assume that $k_\ell \geq 2$. Otherwise, we use Lemma 6 and work over an extension field of $\mathbb{F}_q$. We denote by $I : J \to J'$ the isogeny of kernel G. Let k'_ℓ be the k_ℓ corresponding to J'.
1) Suppose that $\bar{G}$ is such that the Tate pairing is non-degenerate over $\bar{G} \times \bar{G}$. Then by applying Lemma 5 we have

$$T_{\ell^{n-1}}(I(P_1), I(P_2)) \in \mu_{\ell^{k_\ell - 1}} \backslash \mu_{\ell^{k_\ell - 2}},$$

for $P_1, P_2 \in \bar{G}$. If $J'[\ell^n]$ is not defined over $\mathbb{F}_q$, then its endomorphism ring cannot be maximal at ℓ, hence the isogeny is descending. Assume then that $J'[\ell^n]$ is defined over $\mathbb{F}_q$. Let $\bar{P}_1, \bar{P}_2 \in J'[\ell^n]$ be such that $I(P_1) = \ell\bar{P}_1$, $I(P_2) = \ell\bar{P}_2$. Then $T_{\ell^n}(\bar{P}_1, \bar{P}_2) \in \mu_{\ell^{k_\ell+1}} \backslash \mu_{\ell^{k_\ell}}$. We denote by $G' =< \bar{P}_1, \bar{P}_2 >$. The subgroup G' may be chosen such that it is maximal isotropic with respect to the ℓ^n-Weil pairing. It follows that $k'_\ell \geq k_\ell + 1$. By Theorem 2, we deduce that the endomorphism ring of J' is not locally maximal at ℓ, hence the isogeny is descending.
2) Suppose now that the Tate pairing is degenerate over $\bar{G} \times \bar{G}$. We distinguish two cases.
Case 1. Suppose that $J'[\ell^n]$ is defined over $\mathbb{F}_q$. With the same notations as above, we get that $T_{\ell^n}(\bar{P}_1, \bar{P}_2) \in \mu_{\ell^{k_\ell}}$. Let $L \subset J'[\ell^n]$ be a subgroup of rank 2 maximal isotropic with respect to the Weil pairing and consider $Q_1, Q_2 \in L \backslash G'$. Then $\ell^{n-1}Q_1, \ell^{n-1}Q_2 \in Ker\ I^\dagger$. Since $T_{\ell^{n-1}}(I^\dagger(Q_1), I^\dagger(Q_2)) \in \mu_{\ell^{k_\ell-2}}$, it follows that $T_{\ell^n}(Q_1, Q_2) \in \mu_{\ell^{k_\ell-1}}$. Hence $k'_\ell \leq k_\ell$. By Theorem 2, we conclude that the endomorphism ring of J' is locally maximal at ℓ.
Case 2. Suppose that $J'[\ell^n]$ is not defined over $\mathbb{F}_q$. Hence I is descending. We have

$$T_{\ell^{n-1}}(I(P_1), I(P_2)) \in \mu_{\ell^{k_\ell-2}}.$$

Let $L \subset J'[\ell^{n-1}]$ be a subgroup of rank 2 such that $\ell^{n-2}L$ is maximal isotropic with respect to the Weil pairing and consider $Q_1, Q_2 \in L \backslash G'$. Then $\ell^{n-2}Q_1, \ell^{n-2}Q_2 \in Ker\ I^\dagger$. Since $T_{\ell^{n-1}}(I^\dagger(Q_1), I^\dagger(Q_2)) \in \mu_{\ell^{k_\ell-4}}$, it follows that $T_{\ell^{n-1}}(Q_1, Q_2) \in \mu_{\ell^{k_\ell-3}}$. Hence $v_{\ell,\mathrm{End}J'}(\pi) = v_{\ell,\mathrm{End}J}(\pi)$ which contradicts the hypothesis that I is descending.

Let $G \in \mathcal{W}$. By an argument similar to the one in Lemma 2, in order to determine the largest integer k such that $T_{\ell^n} : G \times G \to \mu_{\ell^k}$ is surjective, it suffices to determine the largest k such that all the self-pairings $T_{\ell^n}(P, P)$, with $P \in G$, are ℓ^k-th roots of unity. Let G and G' in $\mathcal{W}$ such that $\ell^{n-1}G = \ell^{n-1}G'$. First note that $P' \in G'$ can be written as $P' = P + L$, with $P \in G$ and $L \in J[\ell^{n-1}]$. Then by bilinearity

$$T_{\ell^n}(P', P') = T_{\ell^n}(P, P)(T_{\ell^n}(P, L)T_{\ell^n}(L, P))T_{\ell^n}(L, L).$$

By Lemma 2 and given that $L \in J[\ell^{n-1}]$, we have that $T_{\ell^n}(P', P')$ is a ℓ^{k_ℓ}-th primitive root of unity if and only if $T_{\ell^n}(P, P)$ is a ℓ^{k_ℓ}-th primitive root of unity. This implies that in order to compute k_ℓ it suffices to compute pairings over a set of representatives of $\mathcal{W}$ modulo the equivalence relation $G \sim G'$ if and only if $\ell^{n-1}G = \ell^{n-1}G'$.

Consequently, in order to find all kernels of horizontal isogenies we search, among subgroups $G \in \mathcal{W}$ (modulo the ℓ^{n-1}-torsion), those for which the Tate pairing restricted to $G \times G$ maps to $\mu_{\ell^{k_{\ell,J}-1}}$. If $\{Q_1, Q_2, Q_{-1}, Q_{-2}\}$ is a symplectic basis for $J[\ell^n]$, then a subgroup of rank 2 generated by $\lambda_1 Q_1 + \lambda_{-1}Q_{-1} + \lambda_2 Q_2 + \lambda_{-2}Q_{-2}$ and $\lambda'_1 Q_1 + \lambda'_{-1}Q_{-1} + \lambda'_2 Q_2 + \lambda'_{-2}Q_{-2}$, with $\lambda_i, \lambda'_j \in \mathbb{F}_\ell$, $i, j \in \{-2, -1, 1, 2\}$, is maximal isotropic with respect to the Weil pairing if the following equation is satisfied

$$\lambda_1\lambda'_{-1} - \lambda_{-1}\lambda'_1 + \lambda_2\lambda'_{-2} - \lambda_{-2}\lambda_2 = 0. \tag{11}$$

Moreover, this subgroup has degenerate Tate pairing if the following equations are satisfied

$$\sum_{i,j\in\{1,2,-1,-2\}} \lambda_i\lambda_j \log T_{\ell^n}(Q_i, Q_j) = 0 \bmod \ell^{n-k_\ell+1} \tag{12}$$

$$\sum_{i,j\in\{1,2,-1,-2\}} \lambda_i\lambda'_j \log T_{\ell^n}(Q_i, Q_j) = 0 \bmod \ell^{n-k_\ell+1} \tag{13}$$

$$\sum_{i,j\in\{1,2,-1,-2\}} \lambda'_i\lambda'_j \log T_{\ell^n}(Q_i, Q_j) = 0 \bmod \ell^{n-k_\ell+1} \tag{14}$$

Example 1. We consider the jacobian of the hyperelliptic curve

$$y^2 = 5x^5 + 4x^4 + 98x^2 + 7x + 2,$$

defined over the finite field $\mathbb{F}_{127}$. The jacobian has maximal endomorphism ring at 5 and $[\mathrm{End}J : \mathbb{Z}[\pi, \bar{\pi}]] = 50$. The ideal (5) decomposes as $5 = \mathfrak{a}_1\mathfrak{a}_2$ in $\mathcal{O}_K$. Hence there are two horizontal isogenies, which correspond to ideals $\mathfrak{a}_1$ and $\mathfrak{a}_2$ under the Shimura class group action. The 5-torsion is defined over an extension field of degree 8 of the field $\mathbb{F}_{127}$, that we denote $\mathbb{F}_{127}(t)$. Our computations with MAGMA found two subgroups of $J[5]$, maximal isotropic with respect to the Weil pairing and with degenerate 5-Tate pairing. For lack of space, we give here the Mumford coordinates of the generators of one of these subgroups.

$$\begin{aligned}
&(x^2 + (74t^7 + 25t^6 + 6t^5 + 110t^4 + 96t^3 + 75t^2 + 29t + 20)x \\
&+39t^7 + 62t^6 + 77t^5 + 47t^4 + 9t^3 + 62t^2 + 97t + 15, \\
&(116t^7 + 61t^6 + 13t^5 + 38t^4 + 70t^3 + 109t^2 + 62t + 71)x + 98t^7 \\
&+77t^6 + 17t^5 + 76t^4 + 81t^3 + 5t^2 + 36t + 33) \\
&(x^2 + (66t^7 + 89t^6 + 50t^5 + 124t^4 + 91t^3 + 102t^2 + 100t + 52)x \\
&+119t^7 + 14t^6 + 126t^5 + 42t^4 + 42t^3 + 85t^2 + 12t + 77, \\
&(92t^7 + 90t^6 + 94t^5 + 57t^4 + 59t^3 + 24t^2 + 72t + 11)x \\
&+103t^7 + 16t^6 + 7t^5 + 111t^4 + 95t^3 + 79t^2 + 45t + 34)
\end{aligned}$$

6 Complexity analysis

In this section, we evaluate the complexity of Algorithm 1 and compare its performance to that of the Freeman-Lauter algorithm. Note that for a fixed $\ell > 2$, both algorithms perform computations in extension fields over which the ℓ^d-torsion, for a certain ℓ^d dividing $[\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]]$, is rational.

Checking locally maximal endomorphism rings. In Freeman and Lauter's algorithm, in order to check if $\mathrm{End}(J)$ is locally maximal at ℓ, for $\ell > 2$, it suffices to check that $\sqrt{d}$ and η are endomorphisms of J (see [5, Lemma 6]). If

$\pi = c_1 + c_2\sqrt{d} + (c_3 + c_4\sqrt{d})\eta$[1] then we have

$$2c_2\sqrt{d} = \pi + \bar{\pi} - 2c_1 \qquad (15)$$

$$(4c_2(c_3^2 - c_4^2 d))\eta = (2c_2c_3 - c_4(\pi + \bar{\pi} - 2c_1))(\pi - \bar{\pi}). \qquad (16)$$

Moreover, Eisenträger and Lauter show that the index is $[\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]] = 2^s c_2(c_3^2 - c_4^2 d)$, for some $s \in \mathbb{N}$. Hence, for a fixed $\ell > 2$ dividing the index $[\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]]$, we need to consider an extension field over which $J[\ell^u]$ is defined, where u is the ℓ-adic valuation of the index. Meanwhile, Algorithm 1 performs computations over the smallest extension field containing the ℓ-torsion points. The degree of this extension field is smaller than ℓ^3, by Proposition 1.

Notation. We denote by r the degree of the smallest extension field $\mathbb{F}_{q^r}$ such that the ℓ-torsion is $\mathbb{F}_{q^r}$-rational.

We suppose that $\pi^r - 1$ is exactly divisible by ℓ^n. First, we need to compute a basis for the ℓ^n-torsion. We assume that the zeta function of $J/\mathbb{F}_{q^r}$ and the factorization $\#J(\mathbb{F}_{q^r}) = \ell^s m$ are known in advance. We denote by $M(r)$ the cost of multiplication in an extension field of degree r. In order to compute the generators of $J[\ell^n]$, we use an algorithm implemented in AVIsogenies [3], which needs $O(M(r)(r \log q + \ell^n))$ operations in $\mathbb{F}_q$. We then compute a symplectic basis of $J[\ell^n]$, by using an algorithm similar to Gram–Schmidt orthogonalization. In order to compute k_ℓ, we use the values of the Tate pairing $T_{\ell^n}(Q_i, Q_j)$ for $i, j \in \{1, -1, 2, -2\}$. Computing the Tate pairing costs $O(M(r)(n \log \ell + r \log q))$ 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. We conclude that the cost of Algorithm 1 is $O(M(r)(r \log q + +\ell^n + n \log \ell))$. 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 ℓ^u-torsion, whose degree is $r\ell^{u-r}$ (by Proposition 2). The costs of the two algorithms are given in Table 1.

Table 1. Cost for checking locally maximal endomorphism rings at ℓ

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

Computing horizontal isogenies. Both classical algorithms and our algorithm need to compute first a basis for the ℓ-torsion. As stated before, this costs $O(rM(r) \log q)$. The classical algorithm (see [2, Algorithm VI.3.4]) computes

[1] Note that we cannot always write π in this form, but if this is not case, we can always replace π by $2^s\pi$, for some $s \in \mathbb{Z}$.

subspaces which are invariant under the action of Frobenius. More precisely, this algorithm needs to compute the matrix of the Frobenius endomorphism (in $O(\ell^2)$ operations in $\mathbb{F}_{q^r}$ using a baby-step giant-step approach). We conclude that the overall complexity of this algorithm is $O(M(r)(r \log q + \ell^2))$. The method described in Section 5 computes a symplectic basis of the ℓ^n-torsion and solves a system of 4 homogenous equations of degree 2, with coefficients in $\mathbb{F}_\ell$. The cost of solving this system is polynomial in ℓ and thus negligible (ℓ is small). Our method for horizontal isogeny computation has the same cost as Algorithm 1.

7 Conclusion

For an ordinary jacobian defined over a finite field, we have described a relation between its endomorphism ring and some properties of the ℓ-Tate pairing. We deduced an efficient criterion for checking whether the jacobian is locally maximal at ℓ and an algorithm computing kernels of horizontal (ℓ, ℓ)-isogenies.

8 Acknowledgements

This work was supported by the Direction Générale de l'Armement through the AMIGA project under contract 2010.60.055 and by the French Agence Nationale de la Recherche through the CHIC project. The author thanks David Gruenewald and John Boxall for helpful discussions and is particularly indebted to Ben Smith for valuable comments and proofreading of previous versions of this manuscript.

References

1. J. Belding, R. Broker, A. Enge, and K. Lauter. Computing Hilbert class polynomials. In A.J. van der Poorten and A. Stein, editors, *Algorithmic Number Theory Symposium-ANTS VIII*, volume 5011 of *Lecture Notes in Computer Science*, pages 282–295. Springer Verlag, 2008.
2. G. Bisson. *Endomorphism rings in cryptography.* PhD thesis, Institut National Polytechnique de Lorraine, 2011.
3. G. Bisson, R. Cosset, and D. Robert. Avisogenies. http://avisogenies.gforge.inria.fr/.
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. 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.
6. D. Freeman and K. Lauter. Computing endomorphism rings of jacobians of genus 2 curves. In *Symposium on Algebraic Geometry and its Applications, Tahiti*, 2006.
7. P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenhaler, and A. Weng. The 2-adic CM method for genus 2 curves with applications in cryptography. In Xuejia Lai and Kefei Chen, editors, *ASIACRYPT06*, volume 4284 of *Lecture Notes in Computer Science*, pages 114–129. Springer, 2006.

8. 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.
9. S. Ionica and A. Joux. Pairing the volcano. *Mathematics of Computation*, 82:581–603, 2013.
10. J.S.Milne. Abelian varieties. http://www.jmilne.org/math/CourseNotes/av.html.
11. S. Lichtenbaum. Duality theorems for curves over p-adic fields. *Invent.Math.7*, pages 120–136, 1969.
12. V. Miller. The Weil pairing, and its efficient calculation. *Journal of Cryptology*, 17(4):235–261, September 2004.
13. S.L. Schmoyer. The Triviality and Nontriviality of Tate-Lichtenbaum Self-Pairings on Jacobians of curves, 2006. http://www-users.math.umd.edu/ schmoyer/.
14. G. Shimura. *Abelian varieties with complex multiplication and modular functions.* Princeton Mathematical Series. Princeton University Press, 1998.
15. Andrew Sutherland. Computing Hilbert Class Polynomials with the CRT. http://arxiv.org/abs/0903.2785, 2009.
16. A. Weng. Constructing hyperelliptic curves of genus 2 suitable for crpytography. *Math. Comp.*, 72:435–458, 2003.

9 Appendix A

We detail the proof of Lemma 6.

Proof. (a) We can easily check that

$$f_{\ell^{n+1},\bar{D}_2} = (f_{\ell,\bar{D}_2})^{\ell^n} \cdot f_{\ell^n,D_2}.$$

Note that these functions are $\mathbb{F}_q$-rational. By evaluating them at D_1 and raising to the power $(q-1)/\ell^n$, we obtain the desired equality. (b) Since $\mathrm{div}\,(f_{\ell^{n+1},D_2}) = \mathrm{div}\,(f^{\ell}_{\ell^n,D_2})$, we have $T^{\ell}_{\ell^{n+1}}(\bar{D}_1,\bar{D}_2) = T^{(\mathbb{F}_{q^\ell})}_{\ell^n}(\bar{D}_1, D_2)$, where $T^{(\mathbb{F}_{q^\ell})}_{\ell^n}$ is the ℓ^n-Tate pairing defined over $\mathbb{F}_{q^\ell}$. We only need to show that

$$T^{(\mathbb{F}_{q^\ell})}_{\ell^n}(\bar{D}_1, D_2) = T_{\ell^n}(D_1, D_2)$$

Note that we have $\pi(\bar{D}_1) = \bar{D}_1 + D_\ell$, where D_ℓ is a point of order ℓ. This implies that

$$\bar{D}_1 + \pi(\bar{D}_1) + \pi^2(\bar{D}_1) + \ldots + \pi^{\ell-1}(\bar{D}_1) \sim \ell\bar{D}_1 \sim D_1.$$

Hence we get

$$\begin{aligned} T^{(\mathbb{F}_{q^\ell})}_{\ell^n}(\bar{D}_1, D_2) &= f_{\ell^n,D_2}(\bar{D}_1)^{\frac{(1+q+\ldots+q^{\ell-1})(q-1)}{\ell^n}} \\ &= f_{\ell^n,D_2}(\bar{D}_1 + \pi(\bar{D}_1) + \ldots + \pi^{\ell-1}(\bar{D}_1))^{\frac{(q-1)}{\ell^n}}. \end{aligned}$$

By applying Weil's reciprocity law, we obtain

$$T^{(\mathbb{F}_{q^\ell})}_{\ell^n}(\bar{D}_1, D_2) = f_{\ell^n,D_2}(D_1)^{\frac{(q-1)}{\ell^n}} f(D_2)^{q-1},$$

where f is such that $\mathrm{div}(f) = (\bar{D}_1) + (\pi(\bar{D}_1)) + \ldots + (\pi(\bar{D}_1)) - D_1$ and that $\mathrm{supp}(f) \cap \mathrm{supp}(D_2) = \emptyset$. Note that f is $\mathbb{F}_q$-rational, so $f(D_2)^{q-1} = 1$. This concludes the proof.