CYCLES IN THE SUPERSINGULAR ℓ-ISOGENY GRAPH AND CORRESPONDING ENDOMORPHISMS

EFRAT BANK, CATALINA CAMACHO-NAVARRO, KIRSTEN EISENTRÄGER, TRAVIS MORRISON, AND JENNIFER PARK

Abstract. We study the problem of generating the endomorphism ring of a supersingular elliptic curve by two cycles in ℓ-isogeny graphs. We prove a necessary and sufficient condition for the two endomorphisms corresponding to two cycles to be linearly independent, expanding on the work by Kohel in his thesis. We also give a criterion under which the ring generated by two cycles is not a maximal order. We give some examples in which we compute cycles which generate the full endomorphism ring. The most difficult part of these computations is the calculation of the trace of these cycles. We show that a generalization of Schoof's algorithm can accomplish this computation efficiently.

1. Introduction

The currently used cryptosystems, such as RSA and systems based on Elliptic Curve Cryptography (ECC), are known to be broken by quantum computers. However, it is not known whether cryptosystems based on the hardness of computing endomorphism rings or isogenies between supersingular elliptic curves can be broken by quantum computers. Because of this, these systems have been studied intensely over the last few years, and the International Post-Quantum Cryptography Competition sponsored by NIST [NIS16] has further increased interest in studying the security of these systems. There is a submission under consideration [ACC+17] which is based on supersingular isogenies.

Cryptographic applications based on the hardness of computing isogenies between supersingular elliptic curves were first given in [CGL09]. In this paper, Charles, Goren, and Lauter constructed a hash function from the ℓ-isogeny graph of supersingular elliptic curves, and finding preimages for the hash function is connected to finding certain ℓ-power isogenies (for a small prime ℓ) between supersingular elliptic curves.

More recently, De Feo, Jao, and Plût [DFJP14] proposed post-quantum key-exchange and encryption schemes based on computing isogenies of supersingular elliptic curves. A signature scheme based on supersingular isogenies is given in [YAJ+17], and [GPS17] gives a signature scheme in which the secret key is a maximal order isomorphic to the endomorphism ring of a supersingular elliptic curve.

There are currently no subexponential classical or quantum attacks for these systems. However, under some heuristic assumptions, the quaternion analogue for the underlying hardness assumption of the hash function in [CGL09] was broken in [KLPT14], which suggests that a careful study of the isogenies and endomorphism rings of supersingular elliptic curves is necessary.

For a fixed q, [Cer04, LM04] list all isomorphism classes of supersingular elliptic curves over $\mathbb{F}_q$ along with their maximal orders in a quaternion algebra (which was improved in [CG14, §5.2]). In [McM14] McMurdy also computes explicit endomorphism rings for some supersingular elliptic curves. The problem of computing isogenies between supersingular

elliptic curves over p has been studied, both in the classical setting [DG16, Section 4] where the complexity of the algorithm is $\tilde{O}(p^{1/2})$, and in the quantum setting [BJS14], where the complexity is $\tilde{O}(p^{1/4})$. In fact, computing the endomorphism ring of a supersingular elliptic curve is deeply connected to computing isogenies between supersingular elliptic curves, as shown by [Koh96]. Heuristic arguments show that these two problems are equivalent [GPS17, KLPT14, EHL$^+$18].

In this paper, we work over finite fields $\mathbb{F}_q$ of characteristic p, and study the problem of generating the endomorphism ring of a supersingular elliptic curve E by two cycles in the *ℓ-isogeny graph* (Definition 2.1) of supersingular elliptic curves. Computing the endomorphism ring of a supersingular elliptic curve via ℓ-isogeny graphs was first studied by Kohel [Koh96, Theorem 75], who gave an approach for finding four linearly independent endomorphisms that generate a finite-index suborder of $\mathrm{End}(E)$ by finding cycles in the ℓ-isogeny graph. The running time of the probabilistic algorithm is $O(p^{1+\varepsilon})$. We demonstrate some obstructions to generating the full endomorphism ring with two cycles $\alpha, \beta \in \mathrm{End}(E)$.

Expanding on [Koh96], we prove in Theorem 4.10 the necessary and sufficient conditions for α and β to be linearly independent. We also prove sufficient conditions for when α and β generate a proper suborder of $\mathrm{End}(E)$ in Theorem 5.1, then compute some examples. In order to do this, we need to detect when the order generated by two cycles is isomorphic to another given order; in §3, we give a criterion that reduces this problem to computing traces of various endomorphisms. In the appendix we give a generalization of Schoof's algorithm [Sch85] (using the improvements from [SS15]) and show that the trace of an arbitrary endomorphism of norm ℓ^e can be computed in time polynomial in e, ℓ and $\log p$.

The paper is organized as follows: In §2 we review some definitions about elliptic curves and define isogeny graphs. In §3 we discuss some background on quaternion algebras, the Deuring correspondence, and we discuss how to compute the endomorphism ring of a supersingular elliptic curve from cycles in the supersingular ℓ-isogeny graph. In §4 we give a necessary and sufficient condition for two endomorphisms to be linearly independent, expanding on a result by Kohel [Koh96]. In §5 we give conditions under which two cycles α, β in the supersingular ℓ-isogeny graph generate a proper suborder of the endomorphism ring. In §6 we compute some examples, and in the Appendix we give the generalization of Schoof's algorithm.

Acknowledgments. We are deeply grateful to John Voight for several helpful discussions, and for providing us with some code that became a part of the code that generated the computational examples in Section 6. We also thank Sean Hallgren and Rachel Pries for helpful discussions. We thank Andrew Sutherland for many comments on an earlier version that led to a significant improvement in the running time analysis of the generalization of Schoof's algorithm, and for outlining the proof of Proposition 2.4. Finally, we thank the Women in Numbers 4 conference and BIRS, for enabling us to start this project in a productive environment. C.CN. was partially supported by Universidad de Costa Rica. K.E. was partially supported by National Science Foundation awards DMS-1056703 and CNS-1617802. T.M. was partially supported by National Science Foundation awards DMS-1056703 and CNS-1617802, and by funding from the Natural Sciences and Engineering Research Council of Canada, the Canada First Research Excellence Fund, CryptoWorks21, Public Works and Government Services Canada, and the Royal Bank of Canada.

2. Isogeny graphs

2.1. **Definitions and properties.** In this section, we recall several definitions and notation that are used throughout. We refer the reader to [Sil09] and [Koh96] for a detailed overview on some of the below. Let k be a field of characteristic $p > 3$.

By an elliptic curve E over a field k, we mean the projective curve with an affine model $E : y^2 = x^3 + Ax + B$ for some $A, B \in k$. The points of E are the points (x, y) satisfying the curve equation, together with the point at infinity. These points form an abelian group. The j-invariant of an elliptic curve given as above is $j(E) = \frac{256 \cdot 27 \cdot A^3}{4A^3 + 27B^2}$. Two elliptic curves E, E' defined over a field k have the same j-invariant if and only if they are isomorphic over the algebraic closure of k.

Let E_1 and E_2 be elliptic curves defined over k. An *isogeny* $\varphi : E_1 \to E_2$ defined over k is a non-constant rational map which is also a group homomorphism from $E_1(k)$ to $E_2(k)$ [Sil09, III.4]. The *degree* of an isogeny is its degree as a rational map. When the degree d of the isogeny φ is coprime to p, then φ is separable and every separable isogeny of degree $d > 1$ can be factored into a composition of isogenies of prime degrees such that the product of the degrees equals d. If $\psi : E_1 \to E_2$ is an isogeny of degree d, the *dual isogeny* of ψ is the unique isogeny $\widehat{\psi} : E_2 \to E_1$ satisfying $\widehat{\psi}\psi = [d]$, where $[d] : E_1 \to E_1$ is the multiplication-by-d map.

In this paper we will be interested in isogenies of ℓ-power degree, for ℓ a prime different from the characteristic of k. We can describe a separable isogeny from an elliptic curve E to some other elliptic curve via its kernel. Given an elliptic curve E and a finite subgroup H of E, there is a separable isogeny $\varphi : E \to E'$ having kernel H which is unique up to isomorphism (see [Sil09, III.4.12]). In this paper we will identify two isogenies if they have the same kernel. We can compute equations for the isogeny from its kernel by using Vélu's formula [Vél71].

An isogeny of an elliptic curve E to itself is called an endomorphism of E. If E is defined over some finite field $\mathbb{F}_q$, then the set of endomorphisms of E defined over $\overline{\mathbb{F}}_q$ together with the zero map form a ring under the operations addition and composition. It is called the *endomorphism ring* of E, and is denoted by $\mathrm{End}(E)$. It is isomorphic either to an order in a quadratic imaginary field or to an order in a quaternion algebra. In the first case we call E an *ordinary elliptic curve*. An elliptic curve whose endomorphism is isomorphic to an order in a quaternion algebra is called a *supersingular elliptic curve*. Every supersingular elliptic curve over a field of characteristic p has a model that is defined over $\mathbb{F}_{p^2}$ because the j-invariant of such a curve is in $\mathbb{F}_{p^2}$. Given $j \in \overline{\mathbb{F}}_q$ such that $j \neq 0, 1728$, we write $E(j)$ for the curve defined by the equation

$$y^2 + xy = x^3 - \frac{36}{j - 1728}x - \frac{1}{j - 1728}. \tag{2.1.1}$$

Such a curve can be put into a short Weierstrass equation $y^2 = x^3 + Ax + B$. We also write $E(0)$ and $E(1728)$ for the curves with equations $y^2 = x^3 + 1$ and $y^2 = x^3 + x$, respectively.

We borrow definitions from [Sut13, 2.3] to define the ℓ-isogeny graph of supersingular elliptic curves in characteristic p. Given a prime ℓ, the *modular polynomial* $\Phi_\ell(X, Y) \in \mathbb{Z}[X, Y]$ has the property that if $j, j' \in \mathbb{F}_q$ then $\Phi_\ell(j, j') = 0$ if and only if there are elliptic curves $E, E'/\mathbb{F}_q$ with j-invariants j and j', respectively, such that there is a separable isogeny $\phi : E \to E'$ of degree ℓ. When $j \neq 0, 1728$, $j, j' \in \mathbb{F}_q$, and E is ordinary, we can choose E' and ϕ such that ϕ is defined over $\mathbb{F}_q$ [Sch95, Proposition 6.1]. We state and prove a similar result for supersingular elliptic curves E in Corollary 2.5.

Definition 2.1. Let ℓ be a prime different from p. The *supersingular ℓ-isogeny graph in characteristic p* is the multigraph $G(p,\ell)$ whose vertex set is

$$V = V(G(p,\ell)) = \{j \in \mathbb{F}_{p^2} : E(j) \text{ is supersingular}\},$$

and the number of directed edges from j to j' is equal to multiplicity of j' as a root of $\Phi_\ell(j, Y)$. We can identify an edge between $E(j)$ and $E(j')$ with a cyclic isogeny $\phi : E(j) \to E(j')$ of degree ℓ. Such an isogeny is unique up to post-composing with an automorphism of $E(j')$. By the above discussion, we can label the edges of $G(p,\ell)$ which start at a given vertex $E(j)$ with the $\ell+1$ chosen isogenies whose kernels are the nontrivial cyclic subgroups of $E(j)[\ell]$.

Let E, E' be two supersingular elliptic curves defined over $\mathbb{F}_{p^2}$. For each prime $\ell \neq p$, E and E' are connected by a chain of isogenies of degree ℓ [Mes86]. By [Koh96, Theorem79], E and E' can be connected by m isogenies of degree ℓ (and hence by a single isogeny of degree ℓ^m), where $m = O(\log p)$. If ℓ is a fixed prime such that $\ell = O(\log p)$, then any ℓ-isogeny in the chain above can either be specified by rational maps or by giving the kernel of the isogeny, and both of these representations have size polynomial in $\log p$.

The theorem below summarizes several properties of the supersingular ℓ-isogeny graph mentioned above.

Theorem 2.2. Let $\ell \neq p$ be a prime, and let $G(p,\ell)$ be the supersingular ℓ-isogeny graph in characteristic p as in Definition 2.1.

(1) G is connected.
(2) G is $(\ell+1)$-regular as a directed graph.
(3) $\#V = \left[\frac{p}{12}\right] + \varepsilon_p$. Here,

$$\varepsilon_p \stackrel{\text{def}}{=} \begin{cases} 0, & p \equiv 1 \pmod{12} \\ 1, & p = 3 \\ 1, & p \equiv 5, 7 \pmod{12} \\ 2, & p \equiv 11 \pmod{12} \end{cases}$$

Remark 2.3. We have an exception to the $\ell+1$-regularity at the vertices and their neighbors corresponding to elliptic curves with $j = 0, 1728$, due to their extra automorphisms.

As $G(p,\ell)$ is connected, for any two supersingular elliptic curves E, E' defined over $\mathbb{F}_{p^2}$ there is an isogeny $\phi : E \to E'$ of degree ℓ^e for some e. In fact, we can take this isogeny to be defined over an extension of $\mathbb{F}_{p^2}$ of degree at most 6. If $E/\mathbb{F}_q$ is an elliptic curve and $n \geq 1$ is an integer, we denote the ring of endomorphisms of E which are defined over $\mathbb{F}_{q^n}$ by $\mathrm{End}_{\mathbb{F}_{q^n}}(E)$.

Proposition 2.4. *Let $E/\mathbb{F}_{p^2}$ be a supersingular elliptic curve. Then $\mathrm{End}_{\mathbb{F}_{p^{2d}}}(E) = \mathrm{End}(E)$, where $d = 1$ if $j(E) \neq 0, 1728$, $d = 1$ or $d = 3$ if $j(E) = 0$, and $d = 1$ or $d = 2$ if $j(E) = 1728$.*

Proof. First, we observe that for a supersingular elliptic curve $E/\mathbb{F}_q$, all endomorphisms of E are defined over $\mathbb{F}_q$ if and only if the Frobenius endomorphism $\pi : E \to E$ is equal to $[p^k]$ or $[-p^k]$ for some k. This follows from Theorem 4.1 of [Wat69], case (2). This is the case when q is an even power of p and the trace of Frobenius is $\pm 2\sqrt{q}$.

Now assume $E/\mathbb{F}_{p^2}$ is a supersingular elliptic curve and let $\pi : E \to E$ be the Frobenius endomorphism of E. Consider the multiplication-by-p map $[p] : E \to E$. By [Sil09, II.2.12], the map $[p]$ factors as

$$[p] = \alpha \circ \pi,$$

where α is an automorphism of E. The automorphism is defined over $\mathbb{F}_{p^2}$, since $[p]$ and π are defined over $\mathbb{F}_{p^2}$. Thus π and α commute. If $j(E) \neq 0, 1728$, then $\mathrm{Aut}(E) = \{[\pm 1]\}$ and thus $[p] = \pm\pi$. By the above observation, we have $\mathrm{End}_{\mathbb{F}_{p^2}}(E) = \mathrm{End}(E)$.

If $j(E) = 0$, then $\alpha^3 = [\pm 1]$. We also have

$$[p^3] = (\alpha \circ \pi)^3 = \alpha^3 \circ \pi^3,$$

so $\pi^3 = [\pm p^3]$. In this case, the Frobenius of the base change of E to $\mathbb{F}_{p^6}$ is π^3, and thus $\mathrm{End}_{\mathbb{F}_{p^6}}(E) = \mathrm{End}(E)$ again by the above observation. The proof of the case $j(E) = 1728$ is similar. □

Corollary 2.5. *If $E_0, E_1/\mathbb{F}_{p^2}$ are supersingular and if $\ell \neq p$, then $\mathrm{Hom}_{\mathbb{F}_{p^{2d}}}(E_0, E_1) = \mathrm{Hom}(E_0, E_1)$, where $d = 1, 2, 3,$ or 6. If $j(E_i) \neq 0, 1728$ for $i = 0, 1$, then we can take $d = 2$.*

Proof. First, we claim that for some $d' \in \{1, 2, 3, 6\}$, we have $\#E_0(\mathbb{F}_{p^{2d'}}) = \#E_1(\mathbb{F}_{p^{2d'}})$. This follows from the fact that all supersingular curves $E/\mathbb{F}_{p^2}$ will have the same number of points over an extension of $\mathbb{F}_{p^2}$ of degree $1, 2, 3$, or 6, which we now prove. The trace of Frobenius of a supersingular elliptic curve $E/\mathbb{F}_{p^2}$ is either $0, \pm p$ or $\pm 2p$, again by Proposition 4.1 of [Wat69]. By inspection, we see that if α, β are the roots of the characteristic polynomial of the (p^2-power) Frobenius endomorphism of E, then α and β are either $\pm p$, $\pm p(1 \pm \sqrt{-3})/2$, $\alpha = \beta = p$, or $\alpha = \beta = -p$. Thus for some $d' \in \{1, 2, 3, 6\}$, $\alpha^{d'} = \beta^{d'} = p^{d'}$. By [Sil09, V.2.3.1(a)],

$$\#E(\mathbb{F}_{p^{2d'}}) = p^{2d'} + 1 - \alpha^{d'} - \beta^{d'} = p^{2d'} + 1 - 2p^{d'}.$$

Thus we can choose $d' = 1, 2, 3$, or 6 such that the claim holds for E_0 and E_1.

Now let $\mathbb{F}_{p^{2d''}}/\mathbb{F}_{p^2}$ be an extension such that $\mathrm{End}_{\mathbb{F}_{p^{2d''}}}(E_i) = \mathrm{End}(E_i)$ for $i = 0, 1$. Let $d = \mathrm{lcm}\{d', d''\}$. By Proposition 2.4, $d \in \{1, 2, 3, 6\}$.

If $d > 1$, we base change E_i to $\mathbb{F}_{p^{2d}}$ and denote these curves again by E_i. For each $i = 0, 1$, let π_{E_i} be the p^{2d}-power Frobenius endomorphism for E_i; then by our choice of d' which divides d, either $\pi_{E_i} = [p^d] : E_i \to E_i$ or $\pi_{E_i} = [-p^d] : E_i \to E_i$ for $i = 0, 1$. Consequently, for any $\phi \in \mathrm{Hom}(E_0, E_1)$ it follows that

$$\phi \circ \pi_{E_0} = \pi_{E_1} \circ \phi.$$

Thus ϕ is defined over $\mathbb{F}_{p^{2d}}$. □

Remark 2.6. If $E_0, E_1/\mathbb{F}_{p^2}$ are supersingular and $j(E_i) \neq 0, 1728$ for $i = 0, 1$, then E_0 and E_1 are connected by a chain of ℓ-isogenies defined over $\mathbb{F}_{p^4}$.

3. Quaternion algebras, endomorphism rings, and cycles

3.1. **Quaternion algebras.** For $a, b \in \mathbb{Q}^\times$, let $H(a, b)$ denote the quaternion algebra over $\mathbb{Q}$ with basis $1, i, j, ij$ such that $i^2 = a$, $j^2 = b$ and $ij = -ji$. That is,

$$H(a, b) = \mathbb{Q} + \mathbb{Q}\,i + \mathbb{Q}\,j + \mathbb{Q}\,ij.$$

Every 4-dimensional central simple algebra over $\mathbb{Q}$ is isomorphic to $H(a, b)$ for some $a, b \in \mathbb{Q}$; for example, see [Voi, Proposition 7.6.1].

There is a *canonical involution* on $H(a, b)$ which sends an element $\alpha = a_1 + a_2 i + a_3 j + a_4 ij$ to $\overline{\alpha} := a_1 - a_2 i - a_3 j - a_4 ij$. Define the *reduced trace* of an element α as above to be

$$\mathrm{Trd}(\alpha) = \alpha + \overline{\alpha} = 2a_1,$$

and the *reduced norm* to be

$$\mathrm{Nrd}(\alpha) = \alpha\overline{\alpha} = a_1^2 - aa_2^2 - ba_3^2 + aba_4^2.$$

Definition 3.1. Let B be a quaternion algebra over $\mathbb{Q}$, and let p be a prime or ∞. Let $\mathbb{Q}_p$ be the p-adic rationals if p is finite, and let $\mathbb{Q}_\infty = \mathbb{R}$. We say that B is *split at* p if

$$B \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong M_2(\mathbb{Q}_p),$$

where $M_2(K)$ is the algebra of 2×2 matrices with coefficients in K. Otherwise B is said to be *ramified at* p.

Orders in quaternion algebras appear as endomorphism rings of some elliptic curves ([Deu41]):

Theorem 3.2 (Deuring Correspondence)**.** *Let E be an elliptic curve over $\mathbb{F}_p$ and suppose that the $\mathbb{Z}$-rank of* $\mathrm{End}(E)$ *is* 4*. Then $B := \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a quaternion algebra ramified exactly at p and ∞, denoted $B_{p,\infty}$, and* $\mathrm{End}(E)$ *is isomorphic to a maximal order in $B_{p,\infty}$.*

Under this isomorphism, taking the dual isogeny on $\mathrm{End}(E)$ corresponds to the canonical involution in the quaternion algebra, and thus the degrees and traces of endomorphisms correspond to reduced norms and reduced traces of elements in the quaternion algebra.

Lemma 3.3 ([Piz80], Proposition 5.1)**.** *$B_{p,\infty}$ can be explicitly given as*

(*i*) $B_{p,\infty} = \left(\frac{-1,-1}{\mathbb{Q}}\right)$ *if* $p = 2$*;*
(*ii*) $B_{p,\infty} = \left(\frac{-1,-p}{\mathbb{Q}}\right)$ *if* $p \equiv 3 \pmod 4$*;*
(*iii*) $B_{p,\infty} = \left(\frac{-2,-p}{\mathbb{Q}}\right)$ *if* $p \equiv 5 \pmod 8$ *and*
(*iv*) $B_{p,\infty} = \left(\frac{-p,-q}{\mathbb{Q}}\right)$ *if* $p \equiv 1 \mod 8$*, where* $q \equiv 3 \mod 4$ *is a prime such that q is not a square modulo p.*

The quaternion algebra $B_{p,\infty}$ is an inner product space with respect to the bilinear form

$$\langle x, y\rangle = \frac{\mathrm{Nrd}(x+y) - \mathrm{Nrd}(x) - \mathrm{Nrd}(y)}{2}.$$

The basis $\{1, i, j, ij\}$ is an orthogonal basis with respect to this inner product.

3.2. **Computing endomorphism rings from cycles in the ℓ-isogeny graphs.** Suppose we have an order in $\mathrm{End}(E)$ generated by two cycles in $G(p, \ell)$, which we embed as $\mathcal{O} \subseteq B_{p,\infty}$. Suppose we also have another order $\mathcal{O}' \subseteq B_{p,\infty}$. We want to check whether $\mathcal{O} \simeq \mathcal{O}'$ or not.

One can check this via using the fact that two orders are isomorphic if and only if they are conjugate; this follows from the Skolem-Noether theorem, see [Voi, Lemma 17.7.2], for example. One can do this by showing that as lattices in a quadratic space $\mathrm{End}(E)\otimes\mathbb{Q} \simeq B_{p,\infty}$, the two lattices are isometric under the quadratic form induced by Nrd. Thus, we can check whether $\mathcal{O} \simeq \mathcal{O}'$ by computing Gram matrices for a basis of each, and checking whether the matrices are conjugate by an orthogonal matrix. The following proposition, which is Corollary 4.4 in [Neb98], makes this remark explicit.

Proposition 3.4. *Two orders $\mathcal{O}, \mathcal{O}' \subseteq B_{p,\infty}$ are conjugate if and only if they are isometric as lattices with respect to the inner product induced by* Nrd*. In particular, for $m, n \in \{1, \ldots, 4\}$, let x_m, y_n be elements in the quaternion algebra $B_{p,\infty}$ such that $\mathcal{O}_1 = \langle x_1, x_2, x_3, x_4\rangle$ and*

$\mathcal{O}_2 = \langle y_1, y_2, y_3, y_4\rangle$ are orders in $B_{p,\infty}$. If $\mathrm{Trd}(x_m\overline{x_n}) = \mathrm{Trd}(y_m\overline{y_n})$ for $m, n \in \{1, 2, 3, 4\}$, then $\mathcal{O}_1 \cong \mathcal{O}_2$.

Proof. The first statement is [Neb98, Corollary 4.4]. The second statement follows then from the first: the map $x_m \to y_n$ extends linearly to an isometry of lattices in $B_{p,\infty}$. This implies that $\mathcal{O}_1$ and $\mathcal{O}_2$ are conjugate in $B_{p,\infty}$ and hence isomorphic as orders. □

Thus if we have two cycles in $G(p, \ell)$ passing through $E(j)$ which correspond to endomorphisms $\alpha, \beta \in \mathrm{End}(E(j))$, we can generate an order

$$\mathcal{O} = \langle 1, \alpha, \beta, \alpha\beta\rangle = \langle x_0, x_1, x_2, x_3\rangle \subseteq \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Also, suppose we have an order $\mathcal{O}' = \langle y_0, y_1, y_2, y_3\rangle \subseteq B_{p,\infty}$. Then we can check whether $\mathcal{O} \simeq \mathcal{O}'$ by comparing $\mathrm{tr}(x_m\widehat{x_n})$ and $\mathrm{Trd}(y_m\overline{y_n})$. This idea is used in our examples in §6. Additionally, we use this idea in Theorem 5.1 to produce a geometric obstruction to generating $\mathrm{End}(E(j))$ by two cycles in $G(p, \ell)$.

Lemma 3.5. *Let $\{a_1, \ldots, a_e\}$ be a cycle beginning and ending at a vertex $E(j)$. Then the endomorphism of $E(j)$ corresponding to this cycle has degree ℓ^e.*

Proof. Each edge a_k represents an ℓ-isogeny, which has degree ℓ. Composition of N isogenies of degree ℓ results in an isogeny of degree ℓ^N. □

Theorem 3.6. *Let $C = \{a_1, \ldots, a_e\}$ be a cycle in $G(p, \ell)$ beginning and ending at a vertex $E(j)$ corresponding to an endomorphism of $E(j)$. Then the (reduced) trace of C interpreted as an element of $\mathrm{End}(E(j))$ can be computed in time polynomial in ℓ, $\log p$, and e.*

Proof. This is proved in the appendix. □

In fact, some of the traces can be recognized immediately without resorting to the modification of Schoof's algorithm.

Lemma 3.7. *The cycles corresponding to the multiplication-by-ℓ^n map (n of the ℓ-isogenies followed by their dual isogenies in reverse order) have trace $2\ell^n$. Suppose $\phi : E \to E'$ is an isogeny and $\rho \in \mathrm{End}(E')$. Then $\mathrm{tr}(\hat{\phi} \circ \rho \circ \phi) = \deg(\phi) \cdot \mathrm{tr}(\rho)$.*

Proof. Let $\phi : E \to E'$ be an isogeny of supersingular elliptic curves. By Proposition 3.9 of [Wat69], the map

$$\begin{aligned} \iota \otimes \mathrm{id} : \mathrm{End}(E') \otimes \mathbb{Q} &\to \mathrm{End}(E) \otimes \mathbb{Q} \\ \rho \otimes 1 &\mapsto \widehat{\phi}\rho\phi \otimes \frac{1}{\deg(\phi)} \end{aligned}$$

is an isomorphism of quaternion algebras. It follows that $\mathrm{tr}(\widehat{\phi}\rho\phi) = \deg(\phi)\,\mathrm{tr}(\rho)$. □

4. A condition for linear independence

In this section, we prove a necessary and sufficient condition for two endomorphisms α and β to be linearly independent. To prove this we need the notion of a *cycle which has no backtracking*. We first show that this notion is equivalent to the corresponding endomorphism being primitive. Then, in Theorem 4.10, we characterize when two cycles with no backtracking are linearly independent. To do this we use the fact that if two endomorphisms are linearly dependent, then they generate a subring of a quadratic imaginary field, and in particular, they must commute. As a corollary, we obtain that two cycles through a vertex $E(j)$ that do not have the same vertex set must be linearly independent.

Definition 4.1. An isogeny $\phi : E \to E'$ is *primitive* if it does not factor through $[n] : E \to E$ for any natural number $n > 1$.

Remark 4.2. An isogeny $\phi : E \to E'$ is primitive if $\ker(\phi)$ does not contain $E[n]$ for any $n > 1$.

Definition 4.3. Suppose a_1, a_2 are edges in $G(p, \ell)$ whose chosen representatives are ℓ-isogenies $\phi : E(j) \to E(j')$, $\psi : E(j') \to E(j)$. We say that a_2 is dual to a_1 if $\hat{\phi} \in \mathrm{Aut}(E(j))\psi$. A cycle $\{a_1, \ldots, a_e\}$ in $G(p, \ell)$ *has no backtracking* if a_{i+1} is not dual to a_i for $i = 1, \ldots, e-1$.

Remark 4.4. Let $\{a_1, \ldots, a_e\}$ be a path in $G(p, \ell)$ and let $\phi_i : E(j_i) \to E(j_{i+1})$ be the chosen isogeny representing a_i for $i = 1, \ldots, e$. Suppose that a_{k+1} is dual to a_k for some $1 \leq k \leq e-1$. Then we claim that the isogeny

$$\phi = \phi_e \circ \cdots \circ \phi_1$$

will not be primitive. Since a_{k+1} is dual to a_k, there exists $\rho \in \mathrm{Aut}(E(j_k))$ such that $\phi_k = \widehat{\phi_{k+1}}\rho$. Then $\phi_{k+1} \circ \phi_k = [\ell]\rho$, so ϕ factors through $[\ell]$.

Our definition of a cycle with no backtracking is less restrictive than the notion of a simple cycle in [Koh96], which additionally requires that there are no repeated vertices in the cycle. Proposition 82 of [Koh96] shows that simple cycles in $G(p, \ell)$ through $E(j)$ give rise to primitive endomorphisms. We strengthen this result, proving in Lemma 4.6 below that cycles through $E(j)$ with no backtracking correspond exactly to primitive endomorphisms.

Given a path in $G(p, \ell)$ of length e between j and j', there is an isogeny $\phi : E(j) \to E(j')$ of degree ℓ^e obtained by composing the isogenies representing the edges in the path. If this path has no backtracking, the kernel of ϕ is a cyclic subgroup of order ℓ^e in $E(j)[\ell^e]$. Conversely, given an isogeny $\phi : E(j) \to E(j')$ with cyclic kernel of order ℓ^e, there is a corresponding path in $G(p, \ell)$.

Proposition 4.5. *Suppose that $\phi : E(j) \to E(j')$ is an isogeny with cyclic kernel of order ℓ^e. There is a unique path in $G(p, \ell)$ such that the factorization of ϕ into a chain of ℓ-isogenies corresponds to the edges in the path, and the path has no backtracking.*

Proof. The proof is by induction on e. If $e = 1$, there is a unique edge corresponding to the isogeny $\phi : E(j) \to E(j')$, because each edge starting at $E(j)$ corresponds to a unique cyclic subgroup of $E(j)[\ell]$. Now suppose that the kernel of $\phi : E(j) \to E(j')$ is generated by a point P of $E(j)$ of order ℓ^e. There is an edge in $G(p, \ell)$ from $E(j)$ to another vertex $E(j_1)$ which is labeled by $\phi_1 : E(j) \to E(j_1)$ and whose kernel is $\langle [\ell^{e-1}]P \rangle$. Then because $\phi([\ell^{e-1}]P) = 0$, we have a factorization $\phi := \psi \circ \phi_1$. Then $\psi : E(j_1) \to E(j')$ has degree ℓ^{e-1} and its kernel is cyclic of order ℓ^{e-1}, generated by $\phi_1(P)$. Then there is a path of length $e-1$ between $E(j_1)$ and $E(j')$ with no backtracking by the inductive hypothesis. By concatenating with the edge corresponding to ϕ_1, we have a path of length e between $E(j)$ and $E(j')$. Note that the first edge in the path for ψ cannot be dual to the edge for ϕ_1, because otherwise $E(j)[\ell] \subseteq \ker \phi$, which is cyclic by assumption. □

Given a path C in $G(p, \ell)$ starting at $E(j)$, the *isogeny corresponding to C* is the isogeny obtained by composing the isogenies representing the edges along the path. Conversely, given an isogeny $\phi : E(j) \to E(j')$ with cyclic kernel, the *path corresponding to ϕ* is the path constructed as above. We remark that it is the kernel of an isogeny which determines the path in $G(p, \ell)$, so two distinct primitive isogenies will determine the same path if they have the same kernel. This path is only unique because we fix an isogeny representing each edge.

Lemma 4.6. *Let $\{a_1, \ldots, a_e\}$ be a cycle in $G(p, \ell)$ through the vertex $E(j)$ with corresponding endomorphism $\alpha \in \mathrm{End}(E(j))$. If the cycle has no backtracking, then the corresponding endomorphism $\alpha \in \mathrm{End}(E(j))$ is primitive. Conversely, if $\alpha \in \mathrm{End}(E(j))$ is primitive and $\deg(\alpha) = \ell^e$ for some $e \in \mathbb{N}$, the cycle in $G(p, \ell)$ corresponding to α has no backtracking.*

Proof. The first statement is proved as Proposition 82 in [Koh96]. His proof does not use the assumption that there are no repeated vertices in the cycle. Now assume that $\alpha \in \mathrm{End}(E(j))$ is primitive and $\deg(\alpha) = \ell^e$. Then by Proposition 10 of [EHL+18], the kernel of α is cyclic, generated by $P \in E[\ell^e]$. By Proposition 4.5, the cycle in $G(p, \ell)$ corresponding to α has no backtracking.

□

Suppose $\alpha \in \mathrm{End}(E(j))$ is an endomorphism of degree ℓ^e. We wish to describe what information we can infer about the order $\mathbb{Z}[\alpha]$ of $\mathbb{Q}(\alpha)$ from the cycle corresponding to α in $G(p, \ell)$. We will show that we can detect when $\mathbb{Z}[\alpha]$ is maximal at a prime above ℓ.

Lemma 4.7. *Let $\alpha \in \mathrm{End}(E(j))$ be a primitive endomorphism corresponding to a cycle $\{a_1, \ldots, a_e\}$ in $G(p, \ell)$ which begins at $E(j)$. Then a_1 is dual to a_e if and only if $\mathrm{tr}(\alpha) \equiv 0 \pmod{\ell}$.*

Proof. The endomorphism α determines an endomorphism $A = \alpha|_{E[\ell]}$ of $E[\ell]$. If $\mathrm{tr}(\alpha) \equiv 0 \pmod{\ell}$, then the characteristic polynomial of A is x^2. Thus $E[\ell] \subseteq \ker(\alpha^2)$, so α^2 is not primitive. Lemma 4.6 implies that the cycle $\{a_1, \ldots, a_e, a_1, \ldots, a_e\}$ in $G(p, \ell)$ has backtracking, because the endomorphism corresponding to this cycle is α^2. We must have that a_1 is dual to a_e because α has no backtracking.

Conversely, assume a_1 is dual to a_e. Suppose that a_e is an edge from the vertex $E(j')$, and let $\phi_1 : E(j) \to E(j')$ be the isogeny corresponding to a_1 and let $\phi_e : E(j') \to E(j)$ be the isogeny corresponding to a_e. Then $\phi_e = \hat{\phi}_1 u$ for some $u \in \mathrm{Aut}(E(j))$. Thus $\alpha = \widehat{\phi_1} \alpha' \phi_1$, where α' is an endomorphism of $E(j')$. By Proposition 3.7, $\mathrm{tr}(\alpha) \equiv 0 \pmod{\ell}$. □

This lets us conclude the following.

Lemma 4.8. *Let $\{a_1, \ldots, a_e\}$ be a cycle in $G(p, \ell)$ with no backtracking and such that a_1 is not dual to a_e. Suppose a_1 is an edge originating from $E(j)$. In the case that the cycle is a self-loop a_1 at $E(j)$, we assume that a_1 is not dual to itself. Let $\alpha \in \mathrm{End}(E(j))$ be the endomorphism corresponding to the cycle. Then the conductor of the quadratic order $\mathbb{Z}[\alpha]$ in $\mathbb{Q}(\alpha)$ is coprime to ℓ.*

Proof. As α is primitive, it determines a quadratic imaginary extension $\mathbb{Q}(\alpha)$ of $\mathbb{Q}$. The discriminant of α is $\mathrm{tr}(\alpha)^2 - 4\ell^e$, which is coprime to ℓ by Lemma 4.7. Thus the conductor of $\mathbb{Z}[\alpha]$, which divides the square part of the discriminant of α, is also coprime to ℓ. □

Lemma 4.9. *Suppose that $\alpha \in \mathrm{End}(E(j))$ corresponds to a cycle $\{a_1, \ldots, a_e\}$ in $G(p, \ell)$ with no backtracking and such that a_1 is not dual to a_e. Let $K = \mathbb{Q}(\alpha)$. Then ℓ splits completely in $\mathcal{O}_K$ as $\ell\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$, and $\alpha\mathbb{Z}[\alpha] = (\mathfrak{p}_i \cap \mathbb{Z}[\alpha])^e$ for $i = 1$ or 2.*

Proof. Since a_1 is not dual to a_e, the conductor of $\mathbb{Z}[\alpha]$ is coprime to ℓ by Lemmas 4.7 and 4.8. Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ above ℓ. If ℓ ramifies in K, then the factorization $\alpha^2\mathcal{O}_K = \mathfrak{p}^{2e} = \ell^e\mathcal{O}_K$ implies that $\alpha^2\mathbb{Z}[\alpha] = \ell^e\mathbb{Z}[\alpha]$. But then $\alpha^2 = [\ell^e]\gamma$ for some $\gamma \in \mathbb{Z}[\alpha] \subseteq \mathrm{End}(E(j))$. On the other hand, α^2 must be primitive because the assumptions that α is primitive and a_e is not dual to a_1 imply that the cycle for α^2 has no backtracking. This implies that ℓ cannot ramify

in K. If ℓ is inert, it follows that e is even and $\alpha\mathbb{Z}[\alpha] = \ell^{e/2}\mathbb{Z}[\alpha]$, again contradicting the assumption that α is primitive.

We conclude that ℓ must split completely in K, so let $\ell\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ be the factorization of $\ell\mathcal{O}_K$. We now claim that the ideal $\alpha\mathcal{O}_K$ factors as $\alpha\mathcal{O}_K = \mathfrak{p}_1^e$ or $\alpha\mathcal{O}_K = \mathfrak{p}_2^e$.

If the claim does not hold, then $\alpha\mathcal{O}_K = \mathfrak{p}_1^r\mathfrak{p}_2^s$ with $r, s > 0$. Without loss of generality we may assume that $r > s$. Then $\alpha\mathcal{O}_K = (\mathfrak{p}_1\mathfrak{p}_2)^s(\mathfrak{p}_1)^{r-s} = (\ell)^s(\mathfrak{p}_1)^{r-s}$. Then in $\mathbb{Z}[\alpha]$, we have the factorization

$$\alpha\mathbb{Z}[\alpha] = (\ell)^s(\mathfrak{p}_1 \cap \mathbb{Z}[\alpha])^{r-s}.$$

This implies that $\alpha = [\ell]\gamma$ for some $\gamma \in \mathrm{End}(E(j))$, but by Lemma 4.6, this contradicts the assumption that α has no backtracking. □

Theorem 4.10. *Suppose that two cycles with no backtracking pass through $E(j)$ and that at least one cycle satisfies the hypotheses of Lemma 4.9. Denote the corresponding endomorphisms of $E(j)$ by α, β. Suppose further that α and β commute. Then there is a third cycle with no backtracking passing through $E(j)$ which corresponds to an endomorphism $\gamma \in \mathrm{End}(E(j))$ and two automorphisms $u, v \in \mathrm{Aut}(E(j))$ which commute with γ such that $\alpha = u\gamma^a$ and either $\beta = v\gamma^b$ or $\beta = v\widehat{\gamma^b}$. In particular, the cycle for α is just the cycle for γ repeated a times, and the cycle for β is the cycle for γ or $\widehat{\gamma}$ repeated b times.*

Proof. Assume that the cycle for α satisfies the assumption that its first edge is not dual to its last edge. Then the conductor of $\mathbb{Z}[\alpha]$ is coprime to ℓ. Since α and β commute, we must have $\beta \in \mathbb{Q}(\alpha)$. Let $\mathcal{O}$ be the order of $\mathbb{Q}(\alpha)$ whose conductor is the greatest common divisor of the conductors of $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$. Then $\mathcal{O} = \mathbb{Z}[\alpha] + \mathbb{Z}[\beta] \subseteq \mathrm{End}(E(j))$ and the conductor of $\mathcal{O}$ is coprime to ℓ. By Lemma 4.9, ℓ splits completely in K; let $\mathfrak{p}_1, \mathfrak{p}_2$ be the primes above ℓ. Then without loss of generality, we have the factorization $\alpha\mathcal{O} = (\mathfrak{p}_1 \cap \mathcal{O})^i$ of $\alpha\mathcal{O}$ into primes of $\mathcal{O}$ by the same argument as in Lemma 4.9.

Observe that since $\beta \in \mathcal{O}$, $\widehat{\beta} = \mathrm{tr}(\beta) - \beta \in \mathcal{O}$. After possibly exchanging β with its dual $\hat{\beta}$, we get with the same argument that $\beta\mathcal{O} = (\mathfrak{p}_1 \cap \mathcal{O})^j$. Now let $d = \gcd(i, j)$, which implies that there exist $m, n \in \mathbb{Z}$ such that $d = im + jn$ and hence

$$(\mathfrak{p}_1 \cap \mathcal{O})^d = (\mathfrak{p}_1 \cap \mathcal{O})^{im+jn} = \alpha^m\beta^n\mathcal{O}.$$

Set $\gamma = \alpha^m\beta^n \in K$. Then

$$\gamma\mathcal{O} = (\mathfrak{p}_1 \cap \mathcal{O})^d$$

implies $\gamma \in \mathcal{O}$ and that γ must be primitive. Filtering the kernel of γ yields a cycle. Write $i = da$ and $j = db$ for $a, b \in \mathrm{N}$. Then $\gamma^a\mathcal{O} = \alpha\mathcal{O}$, so there exists $u \in \mathcal{O}^* \subseteq \mathrm{Aut}(E(j))$ such that $\alpha = u\gamma^a$. We see that the cycle for α is just the cycle for γ repeated a times. Similarly, the cycle for β is the cycle for γ repeated b times. □

We can state a more general result about when two cycles can give rise to commuting endomorphisms.

Corollary 4.11. *Suppose that $P = \{a_1, \ldots, a_m\}$ is a path in $G(p, \ell)$ without backtracking between $E(j)$ and $E(j')$ which does not pass through $E(0)$ or $E(1728)$. Suppose that $C = \{a_{m+1}, \ldots, a_{m+e}\}$ is a cycle beginning at $E(j')$ satisfying the assumptions of Lemma 4.9. Let $\widehat{P}$ be a path $\{a_{m+e+1}, \ldots, a_{2m+e}\}$ without backtracking such that a_{m+1-k} is dual to a_{m+e+k} for $1 \leq k \leq m$. Let $\alpha \in \mathrm{End}(E(j))$ be the endomorphism corresponding to the cycle $\{a_1, \ldots, a_{2m+e}\}$, the concatenation of P, C, and $\widehat{P}$. Now let β be the endomorphism for another cycle in $G(p, \ell)$ without backtracking which starts at $E(j)$, and assume α and β commute. Then there exist*

automorphisms $u_1, u_2 \in \mathrm{Aut}(E(j))$, an ℓ-power isogeny $\phi : E(j) \to E(j')$, an endomorphism $\gamma \in \mathrm{End}(E(j'))$, automorphisms $v_1, v_2 \in \mathrm{Aut}(E(j'))$ which commute with γ, and positive integers a, b such that $\alpha = u_1 \circ \widehat{\phi} \circ v_1\gamma^a \circ \phi$ and $\beta = u_2 \circ \widehat{\phi} \circ v_2\gamma^b \circ \phi$ or $\beta = u_2 \circ \widehat{\phi} \circ v_2\widehat{\gamma}^b \circ \phi$.

Proof. Let $\alpha' \in \mathrm{End}(E(j'))$ be the endomorphism corresponding to C. Let the cycle for β be $\{a'_1, \ldots, a'_{e'}\}$. We can assume there is a positive integer n such that a'_k is dual to $a'_{e'-k+1}$ for $1 \le k \le n$, but a'_{n+1} is not dual to $a'_{e'-n}$. We can assume such an index exists because if not, a'_1 is not dual to $a'_{e'}$, and we could then apply the previous theorem to β. Write $f = e' - 2n$. Then we must have $f \ge 1$, because otherwise β will not be primitive. We then have two cases to consider: the cycle $\{a'_{n+1}, \ldots, a'_{n+f}\}$ satisfies the assumptions of Lemma 4.8, or $f = 1$ and a'_{n+1} is a self-loop which is dual to itself. We begin by considering the first case. We can assume that $m \le n$, because otherwise we could swap the roles of α and β.

We will proceed by induction on m. Assume first that $m = 1$. Let β' correspond to $\{a'_2, \ldots, a'_{2n+f-1}\}$. If the cycle $\{a_1, \ldots, a_{e+2}, a'_1, \ldots, a'_{2n+f}\}$ has backtracking, it follows that a'_1 is dual to a_{e+2}. As the path $P = \{a_1\}$ does not pass through $E(0)$ or $E(1728)$, it follows that $\phi_{e+2} = \widehat{\psi_1}$ or $\phi_{e+2} = \widehat{\psi_1} \circ [-1]$. Additionally, since a_1 is dual to a_{e+2}, $\phi_{e+2} = \widehat{\phi_1}$ or $\phi_{e+2} = \widehat{\phi_1} \circ [-1]$. In any case, the equality $\alpha\beta = \beta\alpha$ implies that $\alpha'\beta' = \beta'\alpha'$. We can now apply Theorem 4.10. If $m > 1$, the corollary follows by applying the same argument to α' and β'.

We will now show that $\beta\alpha$ cannot be primitive. Assume that $\beta\alpha$ is primitive. Then its kernel is cyclic and thus contains a unique subgroup H of order ℓ with $H \subset E(j)[\ell]$. Then $H = \ker(\phi_1)$. On the other hand, the equality $\alpha\beta = \beta\alpha$ implies that $H = \ker(\psi_1)$, so we conclude $\phi_1 = \psi_1$ (here we use that ϕ_1 and ψ_1 are fixed representatives of edges in $G(p, \ell)$). This contradicts the assumption that $\beta\alpha$ is primitive, since a_1 is dual to a_e and $a'_1 = a_1$.

Now we consider the case that $f = 1$; we will show that in this case, β does not commute with α. Consider first the case that the cycle for β is just $\{a'_1\}$, a single self-loop which is dual to itself. Then $a_1 = a'_1$ by the same argument as above, by considering whether $\alpha\beta$ is primitive or not. Then the path $\{a_2, \ldots, a_{2m+e-1}\}$ is also a cycle beginning at $E(j)$, and its corresponding endomorphism also commutes with β. By induction we conclude then that β also commutes with $\{a_{m+1}, \ldots, a_{m+e}\}$, which is impossible by Theorem 4.10.

If now, in the cycle for β, we have $n < m$, we can use induction to conclude that $a_k = a'_k$ for $1 \le k \le n$, and then reduce to the case that β is a single self-loop dual to itself.

Thus we conclude that $m \le n$. Again by using $\alpha\beta = \beta\alpha$, we find that $a_k = a'_k$ for $1 \le k \le m$, and we can reduce to the case of Theorem 4.10. □

Corollary 4.12. *Suppose that two cycles C_1 and C_2 through $E(j)$ have no backtracking and that C_1 passes through a vertex through which C_2 does not pass. Suppose also that one cycle does not contain a self-loop which is dual to itself. Further assume that neither cycle passes through $E(0)$ or $E(1728)$. Then the corresponding endomorphisms in $\mathrm{End}(E(j))$ are linearly independent.*

5. An obstruction to generating the full endomorphism ring

If C is a cycle in $G(p, \ell)$ which passes through $E(j_1)$ and $E(j_2)$, then we can view it as starting at $E(j_1)$ or $E(j_2)$ and thus it corresponds to an endomorphism $\alpha \in \mathrm{End}(E(j_1))$ or $\alpha' \in \mathrm{End}(E(j_2))$. This suggests the following: suppose we have two cycles which have a path between $E(j_1)$ and $E(j_2)$ in common. Then we can view them as endomorphisms of each vertex. These endomorphisms generate an order $\mathcal{O}$ contained in the intersection of

$\mathrm{End}(E(j_1))$ and $\frac{1}{\ell^e}\hat{\phi}\,\mathrm{End}(E(j_2))\phi$ where ϕ corresponds to the common path. These are two maximal orders inside of $\mathrm{End}(E(j_1)) \otimes \mathbb{Q}$ and thus the two cycles cannot generate a maximal order. However, this does not hold if $\mathrm{End}(E(j_1)) \simeq \mathrm{End}(E(j_2))$, i.e., j_1 is a Galois conjugate of j_2. This is formalized in the following theorem.

Theorem 5.1. *Suppose two cycles in $G(p,\ell)$ both contain the same path between two vertices $E(j_1)$ and $E(j_2)$. Let α and β be the corresponding endomorphisms of $E(j_1)$. If the path between $E(j_1)$ and $E(j_2)$ passes through additional vertices, or if $j_1^p \neq j_2$, then $\{1,\alpha,\beta,\alpha\beta\}$ is not a basis for $\mathrm{End}(E(j_1))$.*

Proof. We can assume that $j_1^p \neq j_2$, by replacing j_2 with an earlier vertex in the path if necessary. Let the path from $E(j_1)$ to $E(j_2)$ be correspond to the isogeny $\phi : E(j_1) \to E(j_2)$. By assumption, we can write $\alpha = \alpha_1\phi$ and write $\beta = \beta_1\phi$. Let $\alpha' = \phi\alpha_1$ and $\beta' = \phi\beta_1$ be the corresponding endomorphisms of $E(j_2)$. Assume towards contradiction that $\langle 1,\alpha,\beta,\alpha\beta\rangle = \mathrm{End}(E(j_1))$. Denote the lists

$$\{x_0,x_1,x_2,x_3\} = \{1,\alpha,\beta,\alpha\beta\}$$
$$\{y_0,y_1,y_2,y_3\} = \{1,\alpha',\beta',\alpha'\beta'\}.$$

We now show that $\mathrm{tr}(x_i\widehat{x_j}) = \mathrm{tr}(y_i\widehat{y_j})$ for $i,j = 0,\ldots,3$. Observe that $[\deg\phi](x_i\widehat{x_j}) = \widehat{\phi}y_i\widehat{y_j}\phi$, so

$$\deg(\phi)\,\mathrm{tr}(x_i\widehat{x_j}) = \mathrm{tr}(\widehat{\phi}y_i\widehat{y_j}\phi).$$

On the other hand, we use Lemma 3.7 to compute

$$\mathrm{tr}(\widehat{\phi}y_i\widehat{y_j}\phi) = \deg(\phi)\,\mathrm{tr}(y_i\widehat{y_j}).$$

This implies that the embedding

$$\mathrm{End}(E(j_2)) \hookrightarrow \mathrm{End}(E(j_1)) \otimes \mathbb{Q}$$
$$\rho \mapsto \widehat{\phi}\rho\phi \otimes \frac{1}{\deg\phi}$$

maps $\langle 1,\alpha',\beta',\alpha'\beta'\rangle$ to an order isomorphic to $\mathrm{End}(E(j_1))$ by [Neb98, Corollary 4.4]. But this violates Deuring's correspondence. □

One might conjecture that two cycles in $G(p,\ell)$ which only intersect at one vertex $E(j)$ generate $\mathrm{End}(E(j))$, but the example in the following section shows this might not be true. In particular, there is an example of two cycles which generate an order $\mathcal{O}$ which is not maximal, but there is a unique maximal order containing $\mathcal{O}$.

6. Examples

We used the software package Magma to perform most of the computations required to compute the endomorphism rings of supersingular elliptic curves in characteristic p with $p \in \{31,101,103\}$. In all cases we worked with the 2-isogeny graph. We started with the supersingular j-invariants and found models for the elliptic curves $E(j)$ as in Equation 2.1.1 that we transformed into ones of the form $y^2 = x^3 + ax + b$ for some $A,B \in \mathbb{F}_{p^2}$. Then for every $E(j)$ we computed the 2-torsion points to generate its 2-isogenies, as in Section 2.1. By Theorem 3.2 and Lemma 3.3 we know that $\mathrm{End}(E(j))$ corresponds to a maximal order in $B_{p,\infty}$.

For each vertex corresponding to $E(j)$, we select cycles in the 2-isogeny graph that satisfy the conditions of Theorem 4.10 and compute their traces and norms. Then we find elements of $B_{p,\infty}$ with these traces and norms and verify that they generate a maximal order.

Example 6.1 ($p = 31$)**.** Let $p = 31$. The unique quaternion algebra ramified at p and ∞ is

$$B_{31,\infty} = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij,$$

where $i^2 = -1$ and $j^2 = -31$.

There are three j-invariants corresponding to isomorphism classes of supersingular elliptic curves over $\mathbb{F}_{p^2}$, namely 2, 4 and 23. Figure 1 shows the 2-isogeny graph with labeled edges.

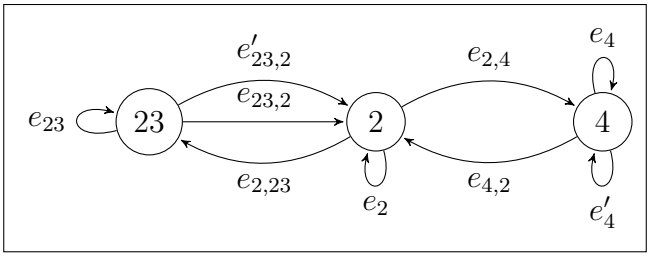

FIGURE 1. 2-isogeny graph for $p = 31$.

Table 1 contains, for each vertex, two cycles that correspond to elements that generate a maximal order in $B_{b,\infty}$. Hence these two cycles must generate the full endomorphism ring.

Vertex	**Cycle**	**Trace**	**Norm**
2	e_2	0	2
	$e_{2,4}e_4e_{4,2}$	2	8
4	e_4	1	2
	$e_{4,2}e_2e_{2,4}$	0	8
23	e_{23}	2	2
	$e_{23,2}e_2e_{2,23}$	-1	8

TABLE 1

With this data we are able to generate the maximal orders that correspond to each endomorphism ring:

$$\mathrm{End}(E(23)) \cong \left\langle 1, -i, -\frac{1}{2}i + \frac{1}{2}ij, \frac{1}{2} - \frac{1}{2}j \right\rangle,$$

$$\mathrm{End}(E(2)) \cong \left\langle 1, \frac{1}{4}i\frac{1}{4}ij, 2i, \frac{1}{2} - \frac{1}{2}j \right\rangle,$$

$$\mathrm{End}(E(4)) \cong \left\langle 1, \frac{1}{2} + \frac{1}{6}i + \frac{1}{6}j - \frac{1}{6}ij, \frac{5}{6}i + \frac{1}{3}j + \frac{1}{6}ij, -\frac{13}{6}i + \frac{1}{3}j + \frac{1}{6}ij \right\rangle.$$

Example 6.2 ($p = 103$)**.** Let $p = 103$. The unique quaternion algebra ramified at p and ∞ is

$$B_{103,\infty} = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij,$$

where $i^2 = -1$ and $j^2 = -103$.

The supersingular j-invariants over $\mathbb{F}_{p^2}$ are $23, 24, 69, 34, 80$, and four defined over $\mathbb{F}_{p^2} - \mathbb{F}_p$: α, β and their conjugates. Figure 2 shows the 2-isogeny graph.

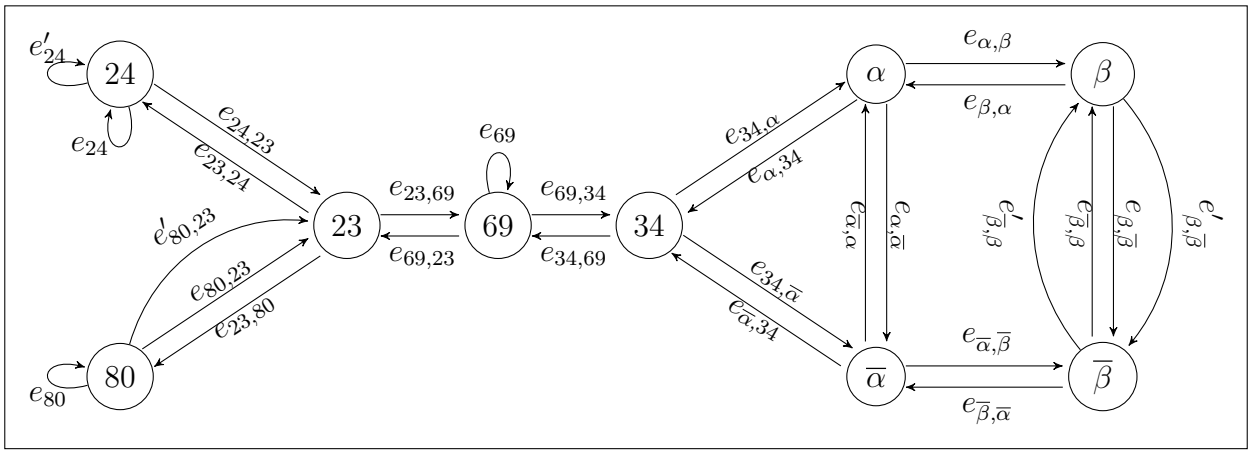

FIGURE 2. 2-isogeny graph for $p = 103$.

After several computations, we were able to find generators for the maximal orders corresponding to all the endomorphism rings of supersingular curves $E(j)$ where $j \in \mathbb{F}_{103^2}$. Table 2 contains, for each such vertex two cycles that correspond to elements that generate the maximal order.

Vertex	**Cycle**	**Trace**	**Norm**
34	$e_{34,\overline{\alpha}}e_{\overline{\alpha},\alpha}e_{\alpha,34}$	-3	8
	$e_{34,69}e_{69}e_{69,34}$	0	8
69	e_{69}	0	2
	$e_{69,34}e_{34,\alpha}e_{\alpha,\overline{\alpha}}e_{\overline{\alpha},34}e_{34,69}$	-6	32
23	$e_{23,24}e_{24}e_{24,23}$	2	8
	$e_{23,80}e_{80}e_{80,23}$	-4	8
80	e_{80}	2	2
	$e_{80,23}e_{23,69}e_{69}e_{69,23}e_{23,80}$	0	32
24	e_{24}	-1	2
	$e_{24,23}e_{23,69}e_{69}e_{69,23}e_{23,24}$	0	32

TABLE 2

In the case of the vertex α, we found an example of two cycles that do not share an additional vertex but that do not generate a maximal order. For instance, the cycles

$$e_{\alpha,\beta}e'_{\beta,\overline{\beta}}e'_{\overline{\beta},\beta}e_{\beta,\alpha}$$

$$e_{\alpha,34}e_{34,69}e_{69}e_{69,34}e_{34,\alpha}$$

generate the order $\mathcal{O} = \left\langle 1, -\frac{1}{2} + \frac{17}{6}i - \frac{1}{6}j + \frac{1}{6}ij, -\frac{5}{2}i + \frac{1}{2}ij, -\frac{1}{2} - \frac{22}{3}i - \frac{11}{6}j - \frac{2}{3}ij \right\rangle$ and there is a unique maximal order containing it, hence this corresponds to $\mathrm{End}(E(\alpha)) \cong \mathrm{End}(E(\overline{\alpha}))$.

Finally, there is only one maximal order remaining in $B_{103,\infty}$, which by Theorem 3.2 is isomorphic to the endomorphism rings of $E(\beta)$ and $E(\overline{\beta})$.

The endomorphism rings are then isomorphic to the following maximal orders:

$$\begin{aligned}
\mathrm{End}(E(80)) &\cong \left\langle 1, i, \frac{1}{2}i + \frac{1}{2}ij, \frac{1}{2} + \frac{1}{2}j \right\rangle, \\
\mathrm{End}(E(23)) &\cong \left\langle 1, 2i, \frac{3}{4}i + \frac{1}{4}ij, \frac{1}{2} - \frac{1}{2j} \right\rangle, \\
\mathrm{End}(E(34)) &\cong \left\langle 1, \frac{17}{14}i + \frac{1}{14}ij\frac{15}{7}i - \frac{2}{7}ij, \frac{1}{2} - \frac{1}{2}j \right\rangle, \\
\mathrm{End}(E(69)) &\cong \left\langle 1, \frac{1}{2} + \frac{1}{7}i + \frac{3}{14}j, \frac{1}{2} - \frac{16}{7}i + \frac{1}{14}j, \frac{1}{2} - \frac{17}{14}i - \frac{1}{14}j - \frac{1}{2}ij \right\rangle, \\
\mathrm{End}(E(24)) &\cong \left\langle 1, \frac{1}{2} + \frac{3}{8}i + \frac{1}{8}ij, \frac{1}{2} - \frac{29}{8}i + \frac{1}{8}ij, -\frac{13}{8}i + \frac{1}{2}j + \frac{1}{8}ij \right\rangle. \\
\mathrm{End}(E(\alpha)) &\cong \left\langle -1, -\frac{1}{2} + \frac{1}{6}i - \frac{1}{6}j - \frac{1}{6}ij, 3i, \frac{5}{6}i - \frac{1}{3}j + \frac{1}{6}ij \right\rangle, \\
\mathrm{End}(E(\beta)) &\cong \left\langle 1, \frac{1}{2} + \frac{13}{10}i + \frac{1}{10}j - \frac{1}{10}ij, -\frac{12}{5}i + \frac{1}{5}j - \frac{1}{5}ij, \frac{1}{2} - \frac{3}{5}i + \frac{3}{10}j + \frac{1}{5}ij \right\rangle.
\end{aligned}$$

Example 6.3 ($p = 101$)**.** Let $p = 101$. The unique quaternion algebra ramified at p and ∞ is

$$B_{101,\infty} = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij,$$

where $i^2 = -2$ and $j^2 = -101$.

The supersingular j-invariants over $\mathbb{F}_{101^2}$ are $64, 0, 21, 57, 3, 59, 66$, and two additional ones, which we denote by α and $\overline{\alpha}$, are defined over $\mathbb{F}_{p^2} - \mathbb{F}_p$. Figure 3 shows the 2-isogeny graph.

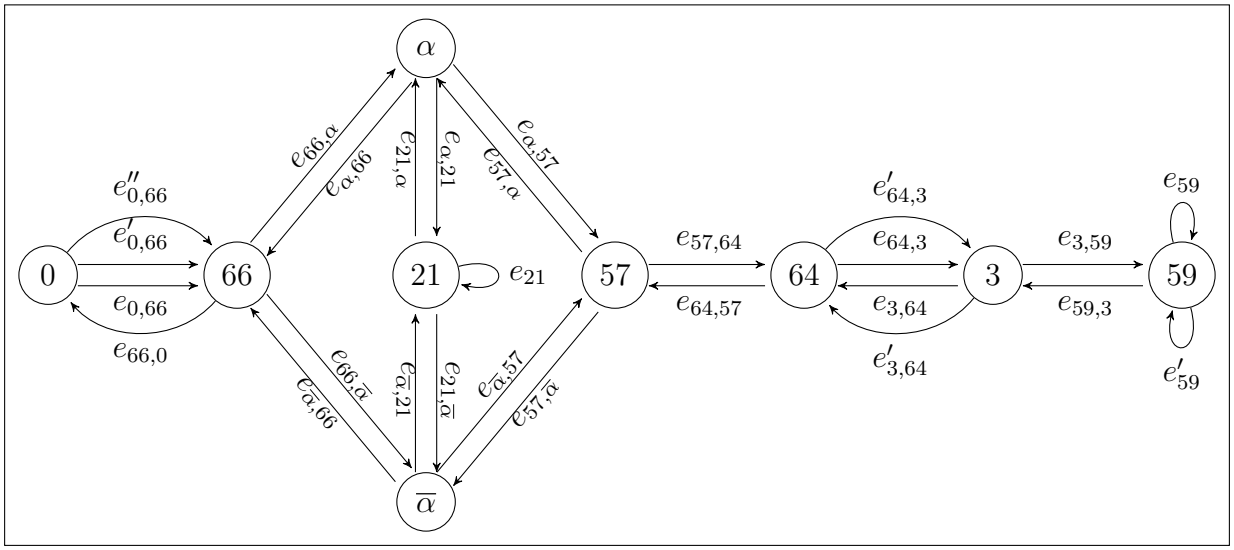

FIGURE 3. 2-isogeny graph for $p = 101$.

It was possible to find two cycles that generate the maximal order corresponding to $\mathrm{End}(E(j))$ where $j \in \{3, 59, 64, 66\}$. Table 3 contains the data for these cycles.

Vertex	**Cycle**	**Trace**	**Norm**
3	$e_{3,59}e_{59}e_{59,3}$	2	8
	$e_{3,64}e'_{64,3}$	-1	4
59	e_{59}	-1	2
	$e_{59,3}e_{3,64}e_{64,3}e_{3,59}$	-8	16
64	$e_{64,57}e_{57,\alpha}e_{\alpha,66}e_{66,\overline{\alpha}}e_{\overline{\alpha},57}e_{57,64}$	10	64
	$e_{64,3}e'_{3,64}$	-1	4
66	$e_{66,0}e_{0,66}$	2	4
	$e_{66,\alpha}e_{\alpha,57}e_{57,\overline{\alpha}}e_{\overline{\alpha},66}$	5	16

TABLE 3

For the vertices $21, 57, \alpha$ no two cycles were found that generate the full endomorphism ring. However, in each of these cases we were able to to generate an order from two cycles which happened to be contained in a unique maximal order. These cycles are listed in Table 4.

Vertex	**Cycle**	**Trace**	**Norm**
21	e_{21}	0	2
	$e_{21,\alpha}e_{\alpha,66}e_{66,0}e'_{0,66}e_{66,\alpha}e_{\alpha,21}$	-8	64
57	$e_{57,64}e_{64,3}e_{3,59}e_{59}e_{59,3}e_{3,64}e_{64,57}$	-8	128
	$e_{57,\alpha}e_{\alpha,66}e_{66,\overline{\alpha}}e_{\overline{\alpha},37}$	-5	16
α	$e_{\alpha,21}e_{21}e_{21,\overline{\alpha}}e_{\overline{\alpha},57}e_{57,\alpha}$	5	32
	$e_{\alpha,66}e_{66,0}e'_{0,66}e_{66,\alpha}$	4	16

TABLE 4

By Theorem 5.1, no two cycles through $j = 0$ generate a maximal order, but it is possible to determine which one corresponds to the endomorphism ring of $E(0)$ once we ruled out the other seven. The endomorphism rings are then isomorphic to the following maximal orders:

$$\begin{aligned}
\mathrm{End}(E(3)) &\cong \left\langle 1, \frac{1}{2} - \frac{13}{12}i + \frac{1}{12}ij, \frac{5}{6}i + \frac{1}{6}ij, \frac{5}{12}i - \frac{1}{2}j + \frac{1}{12}ij \right\rangle, \\
\mathrm{End}(E(59)) &\cong \left\langle 1, \frac{1}{2} + \frac{5}{12}i - \frac{1}{12}ij, -\frac{13}{6}i - \frac{1}{6}ij, -\frac{13}{12}i + \frac{1}{2}j - \frac{1}{12}ij \right\rangle, \\
\mathrm{End}(E(64)) &\cong \left\langle -1, -\frac{1}{2} - \frac{3}{5}i - \frac{1}{10}j + \frac{1}{10}ij, -\frac{1}{2} - \frac{21}{20}i + \frac{1}{5}j + \frac{1}{20}ij, \right. \\
&\qquad \left. -\frac{67}{20}i - 1/10j - 3/20ij \right\rangle, \\
\mathrm{End}(E(66)) &\cong \left\langle 1, \frac{7}{10}i - \frac{1}{10}ij, \frac{1}{2} - \frac{29}{20}i - \frac{3}{20}ij, \frac{7}{20}i - \frac{1}{2}j - \frac{1}{20}ij \right\rangle, \\
\mathrm{End}(E(21)) &\cong \left\langle -1, i, -\frac{1}{2} + \frac{1}{4}i - \frac{1}{4}ij, -\frac{1}{2} + \frac{1}{2}i - \frac{1}{2}j \right\rangle, \\
\mathrm{End}(E(57)) &\cong \left\langle 1, \frac{1}{2} - \frac{13}{28}i + \frac{1}{7}j + \frac{1}{28}ij, -\frac{53}{28}i - \frac{1}{14}j + \frac{3}{28}ij, \frac{1}{2} - \frac{11}{4}i - \frac{1}{4}ij \right\rangle, \\
\mathrm{End}(E(0)) &\cong \left\langle -1, -\frac{1}{2} + \frac{7}{20}i + \frac{1}{20}ij, -\frac{1}{2} + \frac{9}{5}i + \frac{1}{2}j - \frac{1}{10}ij, -\frac{29}{20}i + \frac{1}{2}j + \frac{3}{20}ij \right\rangle, \\
\mathrm{End}(E(\alpha)) &\cong \mathrm{End}(E(\overline{\alpha})) \cong \left\langle -1, 2i, -\frac{1}{2} + \frac{3}{8}i + \frac{1}{4}j - \frac{1}{8}ij, -\frac{7}{8}i + \frac{1}{4}j + \frac{1}{8}ij \right\rangle.
\end{aligned}$$

References

[ACC+17] Reza Azarderakhsh, Matthew Campagna, Craig Costello, Luca De Feo, Basil Hess, Amir Jalali, David Jao, Brian Koziel, Brian LaMacchia, Patrick Longa, Michael Naehrig, Joost Renes, Vladimir Soukharev, and David Urbanik. Supersingular isogeny key encapsulation. Submission to the NIST Post-Quantum Standardization project, 2017. `https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions`.

[BJS14] Jean-François Biasse, David Jao, and Anirudh Sankar. A quantum algorithm for computing isogenies between supersingular elliptic curves. In *Progress in cryptology—INDOCRYPT 2014*, volume 8885 of *Lecture Notes in Comput. Sci.*, pages 428–442. Springer, Cham, 2014.

[BMSS08] A. Bostan, F. Morain, B. Salvy, and É. Schost. Fast algorithms for computing isogenies between elliptic curves. *Math. Comp.*, 77(263):1755–1778, 2008.

[Cer04] J. M. Cerviño. Supersingular elliptic curves and maximal quaternionic orders. In *Mathematisches Institut, Georg-August-Universität Göttingen: Seminars Summer Term 2004*, pages 53–60. Universitätsdrucke Göttingen, Göttingen, 2004.

[CG14] Ilya Chevyrev and Steven D. Galbraith. Constructing supersingular elliptic curves with a given endomorphism ring. *LMS J. Comput. Math.*, 17(suppl. A):71–91, 2014.

[CGL09] Denis X. Charles, Eyal Z. Goren, and Kristin Lauter. Cryptographic hash functions from expander graphs. *J. Cryptology*, 22(1):93–113, 2009.

[Deu41] Max Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hansischen Univ.*, 14:197–272, 1941.

[DFJP14] Luca De Feo, David Jao, and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *J. Math. Cryptol.*, 8(3):209–247, 2014.

[DG16] Christina Delfs and Steven D. Galbraith. Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$. *Des. Codes Cryptogr.*, 78(2):425–440, 2016.

[EHL+18] Kirsten Eisenträger, Sean Hallgren, Kristin Lauter, Travis Morrison, and Christophe Petit. Supersingular isogeny graphs and endomorphism rings: reductions and solutions. *Eurocrypt 2018, LNCS 10822*, pages 329–368, 2018.

[GPS17] Steven D. Galbraith, Christophe Petit, and Javier Silva. Identification protocols and signature schemes based on supersingular isogeny problems. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology – ASIACRYPT 2017*, pages 3–33, Cham, 2017. Springer International Publishing.

[KLPT14] David Kohel, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol. On the quaternion l-isogeny path problem. *LMS Journal of Computation and Mathematics*, 17:418–432, 2014.

[Koh96] David Kohel. *Endomorphism rings of elliptic curves over finite fields*. PhD thesis, University of California, Berkeley, 1996.

[LM04] Kristin Lauter and Ken McMurdy. Explicit generators of endomorphism rings of supersingular elliptic curves. Preprint, 2004.

[McM14] Ken McMurdy. Explicit representation of the endomorphism rings of supersingular elliptic curves. `https://phobos.ramapo.edu/~kmcmurdy/research/McMurdy-ssEndoRings.pdf`, 2014.

[Mes86] J.-F. Mestre. La méthode des graphes. Exemples et applications. In *Proceedings of the international conference on class numbers and fundamental units of algebraic number fields (Katata, 1986)*, pages 217–242. Nagoya Univ., Nagoya, 1986.

[Neb98] Gabriele Nebe. Finite quaternionic matrix groups. *Represent. Theory*, 2:106–223, 1998.

[NIS16] NIST. Post-quantum cryptography, 2016. `csrc.nist.gov/Projects/Post-Quantum-Cryptography`; accessed 30-September-2017.

[Piz80] Arnold Pizer. An algorithm for computing modular forms on $\Gamma_0(N)$. *J. Algebra*, 64(2):340–390, 1980.

[Sch85] René Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp.*, 44(170):483–494, 1985.

[Sch95] René Schoof. Counting points on elliptic curves over finite fields. *J. Théor. Nombres Bordeaux*, 7(1):219–254, 1995. Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993).

[Sil09] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer New York, 2009.

[SS15] Igor E. Shparlinski and Andrew V. Sutherland. On the distribution of Atkin and Elkies primes for reductions of elliptic curves on average. *LMS J. Comput. Math.*, 18(1):308–322, 2015.

[Sut13] Andrew V. Sutherland. Isogeny volcanoes. In *ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium*, volume 1 of *Open Book Ser.*, pages 507–530. Math. Sci. Publ., Berkeley, CA, 2013.

[Vél71] Jacques Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris Sér. A-B*, 273:A238–A241, 1971.

[Voi] John Voight. *Quaternion Algebras*. v.0.9.12, March 29, 2018.

[Wat69] William C. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. (4)*, 2:521–560, 1969.

[YAJ+17] Youngho Yoo, Reza Azarderakhsh, Amir Jalali, David Jao, and Vladimir Soukharev. A post-quantum digital signature scheme based on supersingular isogenies. In *Financial Cryptography and Data Security - 21st International Conference, FC 2017, Sliema, Malta, April 3-7, 2017, Revised Selected Papers*, pages 163–181, 2017.

Appendix A. Modified Schoof's algorithm for traces of arbitrary endomorphisms

Let E be an elliptic curve over a finite field $\mathbb{F}_q$ of characteristic $p \neq 2, 3$. The Frobenius endomorphism $\phi \in \mathrm{End}_{\mathbb{F}_q}(E)$ takes any point $(x, y) \in E(\mathbb{F}_q)$ to (x^q, y^q); it satisfies the relation in $\mathrm{End}_{\mathbb{F}_q}(E)$, given by

$$\phi^2 - t\phi + q = 0.$$

Here, t is called the trace of the Frobenius endomorphism, and it is related to the number of $\mathbb{F}_q$-points on E via the relation

$$\#E(\mathbb{F}_q) = q + 1 - t.$$

Schoof's algorithm [Sch85] computes the trace of the Frobenius endomorphism in $O(\log^9 q)$ elementary operations (bit operations). This algorithm has been improved in [SS15] to be completed in $O(\log^5 q \log\log q)$ operations.

Let E be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$. Here we outline a modification of Schoof's algorithm that computes the trace of any endomorphism $\alpha \in \mathrm{End}_{\mathbb{F}_q}(E)$ that corresponds to a cycle in the ℓ-isogeny graph, where $\ell \neq p$ is a prime. That is, we assume that we are given a cycle of length e in the ℓ-isogeny graph; this path can be represented as a chain of e isogenies of degree ℓ, $\phi_k : E_k \to E_{k+1}$ for $k = 0, \ldots, e-1$. Here $E_0, \ldots, E_e$ are elliptic curves in short Weierstrass form, defined over $\mathbb{F}_{p^2}$, and $E_0 = E_e$. We assume the isogenies are specified by their rational maps. We remark that if this cycle is instead represented by a sequence of ℓ-isogenous elliptic curves, then one can compute a corresponding sequence of ℓ-isogenies in $\tilde{O}(n^2)$ time by Theorem 2 of [BMSS08], where $n = \max\{\lceil \log p \rceil, \ell, e\}$. In the context we are interested in (where p is of cryptographic size, $\ell = O(\log p)$, and we assume $e = O(\log p)$), we observe that finding a cycle in $G(p, \ell)$ could require time exponential in $\log p$, so we may as well assume that we are given the isogenies.

More precisely then, we assume that the input to our algorithm is a cycle of isogenies, each given explicitly as in Proposition 4.1 of [BMSS08] which we record here.

Proposition A.1. *Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve. Then every (normalized) ℓ-isogeny $\psi : E \to E'$ can be written as*

$$\psi(x, y) = \left(\frac{N(x)}{D(x)}, y \left(\frac{N(x)}{D(x)} \right)' \right),$$

where

$$D(x) = \prod_{P \in \ker \psi \setminus \{0\}} (x - x_P)$$

and we define $N(x)$ by the relation

$$\frac{N(x)}{D(x)} = \ell x - \sigma - (3x^2 + A)\frac{D'(x)}{D(x)} - 2(x^3 + Ax + B)\left(\frac{D'(x)}{D(x)} \right)'.$$

Here, σ is the coefficient of $x^{\ell-1}$ in $D(x)$, the sum of the abscissas of the nonzero points of the kernel of ψ.

Proof. This is Proposition 4.1 of [BMSS08]. □

By Corollary 2.5, if E is defined over $\mathbb{F}_{p^2}$ we can take these isogenies to be defined over an extension of degree at most degree 6 of $\mathbb{F}_{p^2}$. If $\ell = O(\log p)$ and the path has length $e = O(\log p)$, which are the parameters that are most interesting, we will show that the trace of this endomorphism can be computed in $\tilde{O}(\log^7 p)$ time by using a modified version of Schoof's algorithm, where we use $f(n) = \tilde{O}(g(n))$ to mean that there exists k such that $f(n) = O(g(n) \log^k n)$.

The naïve computation of the composition of the e isogenies via Vélu's formula yields a formula for the ℓ^e-isogeny that requires at least $O(\ell^e)$ elementary operations; in order to cut down on the number of elementary operations required to compute the explicit formula

for the isogeny, we note that the explicit isogeny formula is simpler on the set of m-torsion points for any m, by taking the quotient modulo the division polynomials. Thus, ℓ^e-isogenies on $E[m]$ can be computed much more quickly, and this is sufficient information to which one can apply Schoof's idea. We remark that the algorithm will correctly compute the trace of an endomorphism of an ordinary curve $E/\mathbb{F}_q$, but unlike in the supersingular case and without further assumptions on the cycle, not all of the isogenies are defined over $\mathbb{F}_q$ (or an extension of $\mathbb{F}_q$ of bounded degree).

A.1. **Complexity of computing endomorphisms on m-torsion.** Let $f_k(X)$ denote the k-th division polynomial of E. It is the polynomial whose roots are the x-coordinates of the nonzero elements of the k-torsion subgroup of E. When k is coprime to p, the degree of f_k is $(k^2-1)/2$. The division polynomials can be defined recursively and the complexity of computing them is analyzed in [SS15].

Let $M(n)$ denote the number of elementary operations required to multiply two n-bit integers. If we choose to multiply two n-bit integers via long multiplication, then $M(n) = O(n^2)$; if we multiply two numbers using the Fast Fourier Transform (FFT), then $M(n) = O(n \log n \log\log n)$.

Proposition A.2. *Given a natural number $m > 1$, the division polynomials $f_1, \ldots, f_m$ can be computed in $O(mM(m^2 \log q))$ time.*

Proof. Using the recursive relations defining the division polynomials, f_k can be computed in $O(M(k^2 \log q))$ time by using a double-and-add method. Thus $f_1, \ldots, f_m$ can be computed in $O(mM(m^2 \log q))$ time; see [SS15, Section 5.1]. □

We continue to work over $\mathbb{F}_q$; typically we will work over an extension of $\mathbb{F}_{p^2}$ of degree at most 6.

Given an ℓ-isogeny $\psi : E \to E'$ as well as a prime $m \neq 2, p$, we are interested in the explicit formula for the induced isogeny on the m-torsion points $\psi_m : E[m] \to E'[m]$. If E is defined by the equation $y^2 = x^3 + ax + b$, and $f_m(x)$ is the m-th division polynomial for E, then $E[m] = \operatorname{Spec} \mathbb{F}_q[x,y]/I$, where $I = \langle f_m(x), y^2 - (x^3 + ax + b)\rangle$. Thus we may reduce the coordinates of the explicit formula for the isogeny ψ given by $(x,y) \mapsto (X(x,y), Y(x,y))$ modulo the ideal I, and the resulting map ψ_m agrees with ψ on $E[m]$. Let $d = \max m, \ell$.

Proposition A.3. *Keeping the notation of the discussion in the above paragraph, $\deg \psi_m = O(d)$, and ψ_m can be computed in $O(M(d^2 \log q) \log d)$ elementary operations.*

Proof. First we observe that by Proposition A.1, the rational functions which define ψ have degree $O(\ell)$. Next, reduce modulo $f_m(x)$, so that the degree of the resulting expression is bounded by $\deg f_m = O(m^2)$. Then by [SS15, Lemma 9, p. 315], it takes $O(M(d^2 \log q) \log d)$ elementary operations to compute the reduction of the isogeny formula modulo f_m.

□

A.2. **Computing the trace on m-torsion points.** To compute the trace of an endomorphism $\psi \in \operatorname{End}(E)$, where ψ appears as a cycle of length e in the supersingular ℓ-isogeny graph in characteristic p, we will compute $\operatorname{tr}(\psi) \pmod m$ for several primes m and then recover the trace using the Chinese remainder theorem, as in Schoof's algorithm.

The endomorphism ψ satisfies the equation $x^2 - \operatorname{tr}(\psi)x + \operatorname{norm}(\psi)$. There is a simple relationship between $\operatorname{tr}(\psi)$ and $\operatorname{norm}(\psi)$:

Lemma A.4. *Let $\psi \in \operatorname{End}(E)$. Then $|\operatorname{tr}(\psi)| \leq 2\operatorname{norm}(\psi)$.*

Proof. If ψ is multiplication by some integer, then its characteristic polynomial is $x^2 \pm 2nx + n^2$, with $n \in \mathbb{N}$. Then $|\operatorname{tr}(\psi)| = 2n$, $\operatorname{norm}(\psi) = n^2$, and the statement of the lemma holds.

If ψ is not multiplication by an integer, then $\mathbb{Z}[\psi]$ is an order in the ring of integers $\mathcal{O}_K$ for some quadratic imaginary number field K. Hence we can fix an embedding $\iota : \mathbb{Z}[\psi] \hookrightarrow \mathcal{O}_K$. Since $\iota(\psi)$ is imaginary, its characteristic polynomial $x^2 - \operatorname{tr}(\psi)x + \operatorname{norm}(\psi)$ must have discriminant < 0, so $|\operatorname{tr}(\psi)| \leq 2\sqrt{\operatorname{norm}(\psi)}$. □

As in Schoof's algorithm, we begin by looking for a bound L such that

$$N := \prod_{\substack{m \leq L \text{ prime} \\ m \neq 2,p}} m > 2\operatorname{norm}(\psi) = 2\ell^e, \tag{A.2.1}$$

where the last equality follows from the fact that the cycle corresponding to ψ in the isogeny graph has length e, so $\operatorname{norm}(\psi) = \ell^e$. By the Prime Number Theorem, we can take $L = O(\log p)$ and there are $O(\log p / \log\log p)$ many primes less than L.

Let m be a prime. Any $\psi \in \operatorname{End}(E)$ induces an endomorphism $\psi_m \in \operatorname{End}(E[m])$; if ψ_m has characteristic polynomial $x^2 - t_m x + n_m$, then $t_m \equiv \operatorname{tr}(\psi) \pmod{m}$. After computing $t \pmod{m}$ for each $m < L$, we can compute $t \pmod{N}$ using the Chinese Remainder Theorem. The bound in Lemma A.4 then lets us compute the value of $\operatorname{tr}(\psi)$. Now, fix one such prime m.

A.2.1. *Computation of* $\operatorname{tr}(\psi_m)$. Let $t_m \equiv \operatorname{tr}(\psi) \bmod m$. Then the relation $\psi_m^2 - t_m\psi_m + n_m = 0$ holds in $\operatorname{End}(E[m]) := \operatorname{End}(E)/(m)$. Here, $n_m \equiv \operatorname{norm}(\psi_m) = \ell^e \bmod m$, with $0 \leq n_m < m$.

Furthermore, one has an explicit formula for $\psi_m : E[m] \to E[m]$ by reducing the explicit coordinates for ψ modulo the ideal I (using the notation in the discussion before Proposition A.3), with $\deg \psi_m = O(m^2)$. Using the addition formulas for E, we can compute the explicit formula for $\psi_m^2 + n_m$, and reduce it modulo I. The main modification to Schoof's algorithm, as it is described in [SS15, 5.1], is to replace the Frobenius endomorphism on $E[m]$ with ψ_m. Having computed $\psi_m^2 + n_m$ and ψ_m, for τ with $0 \leq \tau \leq m-1$ we compute $\tau\psi_m$ until

$$\psi_m^2 + n_m = \tau\psi_m$$

in $\operatorname{End}(E[m])$. Then $\tau = t_m$. Having computed t_m for sufficiently many primes, we recover $\operatorname{tr}\psi$ using the Chinese remainder theorem.

A.2.2. *Complexity analysis for computing the trace.*

Proposition A.5. *Let $E/\mathbb{F}_q$ be a supersingular elliptic curve. Let ψ be an isogeny of E of degree ℓ^e, specified as a chain $\phi_1, \ldots, \phi_e$ of ℓ-isogenies, whose explicit formulas are given. The explicit formula for ψ_m can be computed in $O(edM(d\log q)\log d)$ time, where $d \in \max\{\ell, m^2\}$.*

Proof. The expression for ψ_m can be computed by computing $(\phi_k)_m$ for $k = 1, \ldots, e$, composing the rational maps, and reducing modulo I at each step. The calculation of $f \circ g \bmod h$, where $f, g, h \in \mathbb{F}_q[x]$ are polynomials of degree at most d, takes $O(dM(d\log q))$ elementary operations using the naïve approach. Thus, computing e of these compositions, reducing modulo f_m at each step, takes $O(edM(d\log q)\log q)$ time. □

We now wish to compute the trace of an endomorphism of E corresponding to a cycle in $G(p,\ell)$. Since the diameter of $G(p,\ell)$ is $O(\log p)$, we are interested in computing the trace of a cycle of length $e = O(\log p)$ in $G(p,\ell)$. We are also interested in the case where ℓ is a small

prime, so we will take $\ell = O(\log p)$. The resulting generalization of Schoof's algorithm runs in time polynomial in $\log p$.

Theorem A.6. *Let $p > 3$ be a prime and let ψ be an endomorphism of a supersingular elliptic curve $E/\mathbb{F}_{p^2}$ given as a chain of ℓ-isogenies,*

$$\psi = \phi_e \circ \cdots \circ \phi_1,$$

where each ϕ_k is specified by its rational functions and is defined over $\mathbb{F}_q$. We can take $\mathbb{F}_q$ to be an extension of $\mathbb{F}_{p^2}$ of degree at most 6. Let $n = \lceil \log p \rceil$ and assume $e, \ell = O(n)$. Then the modified version of Schoof's algorithm computes $\operatorname{tr}\psi$ in $\tilde{O}(n^7)$ time.

Proof. We follow the steps in our modification of Schoof's algorithm. Since $\operatorname{norm}\psi = \ell^e$, we first choose a bound $L = O(\log \ell^e)$.

We can compute ψ_m in time $\tilde{O}(n^6)$ time by Proposition A.5. For a prime $m < L$, we compute $\operatorname{tr}\psi_m$, the trace of the induced isogeny ψ_m on $E[m]$, by reducing by the m-division polynomial f_m whenever possible.

Having computed ψ_m and ψ_m^2, with the same argument as in the proof of Theorem 10 of [SS15], we can compute t_m in $O((m + \log q)(M(m^2 \log q)))$ time. This is because once ψ_m and ψ_m^2 are computed, the algorithm proceeds the same way as Schoof's original algorithm. We must repeat this $L = O(\log p) = O(n)$ times.

Once we compute $\operatorname{tr}\psi_m$ for each prime $m \neq p$ less than L, we compute $\operatorname{tr}\psi$ using the Chinese Remainder Theorem. This step is dominated by the previous computations. Thus we have a total run time of $\tilde{O}(n^7)$. □

Department of Mathematics, University of Michigan, Ann Arbor, MI, USA
E-mail address: ebank@umich.edu
URL: http://www-personal.umich.edu/~ebank/

Department of Mathematics, Colorado State University, Fort Collins, CO, 80523, USA
E-mail address: camacho@math.colostate.edu

Department of Mathematics, The Pennsylvania State University, University, Park, PA 16802, USA
E-mail address: eisentra@math.psu.edu
URL: http://www.personal.psu.edu/kxe8/

Institute for Quantum Computing, The University of Waterloo, Waterloo, ON
E-mail address: travis.morrison@uwaterloo.ca

Department of Mathematics, University of Michigan, Ann Arbor, MI, USA
E-mail address: jmypark@umich.edu
URL: http://www-personal.umich.edu/~jmypark/