Computing supersingular endomorphism rings using inseparable endomorphisms

Jenny Fuselier[1], Annamaria Iezzi[2, 3], Mark Kozek[4], Travis Morrison[5], and Changningphaabi Namoijam[6]

[1]Department of Mathematical Sciences, High Point University, High Point, NC 27268, USA
[2]Dipartimento di Matematica e Applicazioni "Renato Caccioppoli", Università degli Studi di Napoli Federico II, I-80126 Napoli, Italy
[3]Laboratoire GAATI, Université de la Polynésie française, 98702 Faaa, French Polynesia
[4]Department of Mathematics & Computer Science, Whittier College, Whittier, CA 90601, USA
[5]Department of Mathematics, Virginia Tech, Blacksburg, VA 24060 USA
[6]Department of Mathematics, Colby College, Waterville, ME 04901, USA

Abstract

We give an algorithm for computing inseparable endomorphisms of a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$, which, conditional on GRH, runs in expected $O(\sqrt{p}(\log p)^2(\log\log p)^3)$ time. With two calls to this algorithm, we compute a Bass suborder of $\mathrm{End}(E)$, improving on the results of Eisenträger, Hallgren, Leonardi, Morrison, and Park [EHL$^+$] who only gave a heuristic algorithm for computing a Bass suborder. We further improve on the results of [EHL$^+$] by removing the heuristics involved in an algorithm for recovering $\mathrm{End}(E)$ from a Bass suborder. We conclude with an argument that $O(1)$ endomorphisms generated by our algorithm along with negligible overhead suffice to compute $\mathrm{End}(E)$, conditional on a heuristic assumption about the distribution of the discriminants of these endomorphisms.

1 Introduction

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$, where q is a power of a prime p. If E is ordinary, in order to compute the geometric endomorphism ring $\mathrm{End}(E)$ of E, one must determine the index $[\mathrm{End}(E) : \mathbb{Z}[\pi_E]]$ where $\mathbb{Z}[\pi_E]$ is the order generated by the Frobenius endomorphism π_E of E. This problem has been well-studied, and there exist algorithms for computing the endomorphism ring of an ordinary elliptic curve, such as Bisson and Sutherland [BS11], which run in expected subexponential time, conditional on reasonable heuristics including the Generalized Riemann Hypothesis (GRH).

When E is supersingular, however, its endomorphism algebra $\mathrm{End}^0(E) \coloneqq \mathrm{End}(E) \otimes \mathbb{Q}$ is a quaternion algebra, and $\mathrm{End}(E)$ is a maximal order of $\mathrm{End}^0(E)$. In this case, there is no canonical imaginary quadratic order which embeds in $\mathrm{End}(E)$. Even worse, if we have a suborder $\Lambda \subseteq \mathrm{End}(E)$, there can be exponentially (in $\log(\mathrm{disc}(\Lambda))$) many pairwise non-isomorphic maximal orders which contain Λ. This stands in contrast to the ordinary case where we have a canonical embedding of a finite-index suborder and there is a unique maximal order containing both this suborder and $\mathrm{End}(E)$: the maximal order is the ring of integers of the imaginary quadratic number field $\mathbb{Q}(\pi_E) \cong \mathrm{End}^0(E)$.

This suggests that computing the endomorphism ring of a supersingular elliptic curve is a hard problem, and this assumption is central to the security of isogeny-based cryptography. Indeed, the problems of path-finding in supersingular isogeny graphs and of computing supersingular endomorphism rings are equivalent, assuming GRH (see Eisenträger, Hallgren, Lauter, Morrison, and Petit [EHL$^+$18] and Wesoloswki [Wes22]). The first algorithm for computing a suborder of $\mathrm{End}(E)$ is due to Kohel [Koh96] and runs in time $O(p^{1+\epsilon})$ for any $\epsilon > 0$. Eisenträger, Hallgren, Leonardi, Morrison, and Park [EHL$^+$] give a $O(p^{1/2+\epsilon})$ algorithm for computing a Bass suborder of $\mathrm{End}(E)$, conditional on heuristics including GRH. They also discuss how to find $\mathrm{End}(E)$ among the maximal overorders of a Bass suborder $\Lambda \subseteq \mathrm{End}(E)$.

In this paper, we give an algorithm, Algorithm 1, for computing inseparable endomorphisms of E. We prove Theorem 4.3, which states that with two calls to Algorithm 1, we provably compute a Bass suborder of $\mathrm{End}(E)$. Under GRH, Algorithm 1 runs in expected time $O(p^{1/2+\epsilon})$. From a theoretical viewpoint, it

suffices to compute a Bass suborder of $\mathrm{End}(E)$: building on ideas in [EHL$^+$], in Section 5 we show that $\mathrm{End}(E)$ can be recovered from a Bass suborder Λ and the time required to find $\mathrm{End}(E)$ among the maximal overorders of Λ is dominated by the time required to compute Λ.

Another approach to computing the endomorphism ring of a supersingular elliptic curve is to compute several endomorphisms until finding a generating set. Suppose we have an algorithm which generates a random endomorphism of a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$. A simple question arises: what is the expected number of calls to that algorithm before finding a set of endomorphisms which generate $\mathrm{End}(E)$ as an order? In [GPS17], Galbraith, Petit, and Silva give a heuristic argument that this expectation is $O(\log p)$. Our work suggests that this estimate is pessimistic: the expected number of calls is bounded by a constant, assuming a reasonable heuristic on the distribution of the discriminants of random endomorphisms. We focus on computing $\mathrm{End}(E)$ with endomorphisms output by Algorithm 1.

First, no collection of inseparable endomorphisms could generate $\mathrm{End}(E)$: if P denotes the 2-sided ideal of inseparable endomorphisms of E, then the endomorphisms produced by Algorithm 1 belong to P. We show in Proposition 3.1 that $\mathbb{Z} + P$ is the unique suborder of $\mathrm{End}(P)$ of index p, and the only maximal order containing $\mathbb{Z} + P$ is $\mathrm{End}(E)$. In Section 6, we show that the expected number of calls to Algorithm 1 before finding a generating set for $\mathbb{Z} + P$ is bounded by a positive constant that is not dependent on either p or E, assuming Heuristic 6.1 which concerns the distribution of discriminants of endomorphisms produced by Algorithm 1. Finally, with a basis for $\mathbb{Z} + P$, one can efficiently compute a basis of $\mathrm{End}(E)$ using algorithms due to Voight [Voi13]. In conclusion, we prove that two calls to Algorithm 1 produce a Bass order unconditionally, and $O(1)$ calls to Algorithm 1 along with negligible overhead produce $\mathrm{End}(E)$ assuming Heuristic 6.1.

The paper is organized as follows. In Section 2, we review the mathematical background of the paper and fix our notation. In Section 3, we study the properties of the suborder $\mathbb{Z} + P \subseteq \mathrm{End}(E)$, where P is the ideal of inseparable endomorphisms of E. We also define inseparable reflections, building on the definition of (d, ϵ)-structures of Chenu and Smith [CS21], and study the structure of quadratic orders generated by inseparable reflections. In Section 4, we study quaternionic orders generated by inseparable reflections, determining when they generate Gorenstein (Proposition 4.1) and Bass (Theorem 4.3) orders in $\mathrm{End}(E)$. Section 5 concerns an algorithm that, given a supersingular elliptic curve $E/\mathbb{F}_{p^2}$, computes a $\mathbb{Z}$-basis of $\mathrm{End}(E)$. First, we analyze Algorithm 1, which computes inseparable endomorphisms of E. Next, we use Algorithm 1 in Algorithm 2 to compute a Bass suborder of $\mathrm{End}(E)$. Algorithm 3 uses Algorithm 2, along with the algorithms of [EHL$^+$18, EHL$^+$, Wes22] to compute a basis for $\mathrm{End}(E)$. Finally, in Section 6, we outline a heuristic algorithm to compute $\mathrm{End}(E)$ in which we first find enough inseparable reflections to generate $\mathbb{Z} + P$. Heuristically, the expectation of the number of such inseparable reflections is bounded by a constant, independent of p, and in practice, this expectation appears to be bounded by 4.

Acknowledgements

We thank Heidi Goodson, Christelle Vincent, and Mckenzie West for organizing the first edition of *Rethinking Number Theory* in 2020, where this project began, and the American Institute of Mathematics for their additional support. We also thank John Voight for several helpful discussions.

The second author was partially supported by the European Union - FSE-REACT-EU, PON Research and Innovation 2014-2020 DM1062/2021 contract number 18-I-15358-2. The fourth author was partially supported by the Commonwealth Cyber Initiative. The fifth author was partially supported by MoST Grant 110-2811-M-007-517.

2 Background and notation

In this section we fix our notation and recall some definitions and facts about elliptic curves and quaternion algebras. We refer the reader to Silverman [Sil09, Chapters III and V] and Voight [Voi21] for details.

2.1 Elliptic curves

Let q be a positive power of a prime $p > 3$, and let E be an elliptic curve defined over the finite field $\mathbb{F}_q$. Since isomorphic elliptic curves have isomorphic endomorphism rings, we may always assume that E is defined by

a short Weierstrass affine form $E : y^2 = x^3 + ax + b$, with $a, b \in \mathbb{F}_q$, such that $4a^3 + 27b^2 \neq 0$. We define the elliptic curve $E^{(p)} : y^2 = x^3 + a^p x + b^p$, and let π denote the p-power Frobenius isogeny $\pi \colon E \to E^{(p)}$ defined by $\pi(x, y) = (x^p, y^p)$. We use the same notation π for every such Frobenius isogeny, independent of the choice of the starting elliptic curve. We let π_E denote the Frobenius endomorphism which sends $(x, y) \mapsto (x^q, y^q)$. For an integer n, we denote by $E[n]$ the *n-torsion subgroup* of E, consisting of points of E of order dividing n. The elliptic curve E is *supersingular* if and only if $E[p] = \{0\}$. For elliptic curves E, E' defined over $\mathbb{F}_q$, we use the notation $\mathrm{Hom}(E, E')$ for the set of isogenies from E to E' defined over $\mathbb{F}_q$ together with the zero map. If $L/\mathbb{F}_q$ is an algebraic extension, we let E_L denote the base change of E from $\mathbb{F}_q$ to L and let $\mathrm{Hom}_L(E, E') \coloneqq \mathrm{Hom}(E_L, E'_L)$. Finally we call $\mathrm{End}(E) \coloneqq \mathrm{Hom}_{\overline{\mathbb{F}_q}}(E, E)$ the *endomorphism ring of E* and $\mathrm{End}^0(E) \coloneqq \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ the *endomorphism algebra of E*. When E is a supersingular elliptic curve defined over $\mathbb{F}_q$, E has a model defined over $\mathbb{F}_{p^2}$ since its j-invariant is in $\mathbb{F}_{p^2}$. Moreover, we can choose a model of E so that all of its isogenies are defined over $\mathbb{F}_{p^2}$ as well: indeed we can choose a model so that the trace of π_E of E is $2p$, in which case $\pi_E = [p]$, the multiplication-by-p map. If $\psi \colon E \to E'$ is an isogeny between any two such models of elliptic curves E and E', then $\psi\pi_E = \pi_{E'}\psi$ and so ψ is defined over $\mathbb{F}_{p^2}$ as desired.

In this paper, we focus on supersingular elliptic curves over $\mathbb{F}_{p^2}$, although some of the results are stated for elliptic curves over $\mathbb{F}_q$. If $E/\mathbb{F}_{p^2}$ is a supersingular elliptic curve, then $\mathrm{End}^0(E)$ is isomorphic to the definite quaternion algebra $B_{p,\infty}$ over $\mathbb{Q}$ ramified exactly at p and ∞, and $\mathrm{End}(E)$ is a maximal order in $\mathrm{End}^0(E)$. Therefore, computing $\mathrm{End}(E)$ entails finding a basis of a maximal order $\mathcal{O}$ in $B_{p,\infty}$ such that $\mathrm{End}(E) \cong \mathcal{O}$.

2.1.1 Isogeny graphs

Let $\ell \geq 1$ be an integer, and let k be a field whose characteristic is coprime to ℓ. The ℓth classical modular polynomial $\Phi_\ell(X, Y) \in \mathbb{Z}[X, Y]$ parameterizes $\overline{k}$-isomorphism classes of elliptic curves connected by an ℓ-isogeny with cyclic kernel. Now let p and ℓ be distinct primes. The *supersingular ℓ-isogeny graph* is defined as follows. The vertex set of $G(p, \ell)$ is $V = V(p) = \{E_i\}_{1 \leq i \leq n}$, a complete set of representatives of isomorphism classes of supersingular elliptic curves over $\mathbb{F}_{p^2}$. The arrows in $G(p, \ell)$ from E_i to E_j are a complete set of representatives of equivalence classes of ℓ-isogenies $E_i \to E_j$, where two ℓ-isogenies $\phi, \psi \colon E_i \to E_j$ are equivalent if $\phi = u\psi$ for some automorphism $u \in \mathrm{Aut}(E_j)$. This graph is finite with constant out-degree equal to $\ell+1$. Moreover, $G(p, \ell)$ is a *Ramanujan graph*: the magnitude of the second largest eigenvalue of the adjacency matrix of $G(p, \ell)$ is bounded by $2\sqrt{\ell}$. This implies that the random walk in $G(p, \ell)$ mixes rapidly, a fact that we exploit in our algorithms for computing endomorphisms of supersingular elliptic curves.

2.2 Quaternion algebras

Let F be a field. A quaternion algebra B over F is a central simple F-algebra of dimension 4. Let $a, b \in F^\times$, and let $H(a, b) \coloneqq F \oplus Fi \oplus Fj \oplus Fij$ be the F-algebra with F-basis $\{1, i, j, ij\}$ subject to the multiplication rules $i^2 = a$, $j^2 = b$, and $ij = -ji$. Then, $H(a, b)$ is a quaternion algebra. Moreover, assuming the characteristic of F is not 2, for any quaternion algebra B over F, there exist $a, b \in F$ such that B is isomorphic to $H(a, b)$.

2.2.1 The canonical involution, reduced trace, and reduced norm

Let $B = H(a, b)$ be a quaternion algebra over F with basis $\{1, i, j, ij\}$. The *standard involution* of B is the F-linear map $\bar{\cdot} \colon B \to B$ such that if $\alpha = w + xi + yj + zij \in B$, then $\bar{\alpha} = w - xi - yj - zij$. Note that it satisfies $\bar{1} = 1$, $\bar{\bar{\alpha}} = \alpha$, and $\overline{\alpha\beta} = \bar{\beta}\bar{\alpha}$ for every $\alpha, \beta \in B$. We define the *reduced trace* of $\alpha \in B$ to be $\mathrm{Trd}\,\alpha \coloneqq \alpha + \bar{\alpha}$ and the *reduced norm of α* to be $\mathrm{Nrd}\,\alpha \coloneqq \alpha\bar{\alpha}$. Both $\mathrm{Trd}\,\alpha$ and $\mathrm{Nrd}\,\alpha$ are in F for any $\alpha \in B$. Note that α and $\bar{\alpha}$ are roots of their characteristic polynomial $x^2 - (\mathrm{Trd}\,\alpha)x + \mathrm{Nrd}\,\alpha$.

The reduced trace defines a pairing $\langle \cdot, \cdot \rangle \colon B \times B \to F$ defined by $(\alpha, \beta) \mapsto \mathrm{Trd}(\alpha\bar{\beta})$. The corresponding quadratic form $Q : B \to F$ is defined by $Q(\alpha) = \mathrm{Nrd}(\alpha)$, for $\alpha \in B$. Now, let $\mathcal{B} = \{e_1, e_2, e_3, e_4\}$ be a basis of B. We define the *Gram matrix of Q* with respect to the basis $\mathcal{B}$ as the matrix

$$G = \left(\langle e_i, e_j \rangle\right)_{1 \leq i,j \leq 4} = \left(\mathrm{Trd}(e_i\bar{e_j})\right)_{1 \leq i,j \leq 4}.$$

Then, for $\alpha = x_1e_1 + x_2e_2 + x_3e_3 + x_4e_4$ and $\beta = y_1e_1 + y_2e_2 + y_3e_3 + y_4e_4$, with $x_i, y_i \in F$, we have

$$\langle \alpha, \beta \rangle = \mathrm{Trd}(\alpha\bar{\beta}) = xGy^t,$$

where $x = (x_1, x_2, x_3, x_4)$ and $y = (y_1, y_2, y_3, y_4)$.

2.2.2 Completions, splitting, and ramification

Let $\mathbb{Q}_v$ denote the completion at a place v of $\mathbb{Q}$. Here, $\mathbb{Q}_v = \mathbb{Q}_p$ for some prime p if v is a finite place, and $\mathbb{Q}_v = \mathbb{R}$ if v is the infinite place. If B is a quaternion algebra over $\mathbb{Q}$, then $B \otimes \mathbb{Q}_v$ is a quaternion algebra over $\mathbb{Q}_v$. A quaternion algebra over $\mathbb{Q}_v$ is either the unique division algebra of dimension 4 over $\mathbb{Q}_v$ or is isomorphic to $M_2(\mathbb{Q}_v)$. If $B \otimes \mathbb{Q}_v \simeq M_2(\mathbb{Q}_v)$, we say that B is *split at* v. If $B \otimes \mathbb{Q}_v$ is a division algebra, we say that B is *ramified at* v. The set of places of $\mathbb{Q}$ where B is ramified is a finite set of even cardinality. If B is not ramified at any place, then $B \simeq M_2(\mathbb{Q})$. The *discriminant* $\mathrm{disc}(B)$ *of* B is the product of all primes p at which B is ramified.

A $\mathbb{Z}$*-lattice* $I \subseteq \mathcal{O}$ is a finitely generated $\mathbb{Z}$-submodule of B such that $\mathbb{Q}I = B$. A $\mathbb{Z}$*-order* $\mathcal{O} \subseteq B$ is a $\mathbb{Z}$-lattice in B which is also a subring. Analogously, one defines a $\mathbb{Z}_p$-order in the quaternion algebra $B \otimes \mathbb{Q}_p$. Given a lattice I in B, the *left order* of I is $\mathcal{O}_L(I) \coloneqq \{\alpha \in B : \alpha I \subseteq I\}$, and we similarly define its right order $\mathcal{O}_R(I) \coloneqq \{\alpha \in B : I\alpha \subseteq I\}$. A lattice $I \subseteq B$ is a *left fractional* $\mathcal{O}$*-ideal* if $\mathcal{O} \subseteq \mathcal{O}_L(I)$. For a left ideal I of an order $\mathcal{O}$, define the *reduced norm* $\mathrm{Nrd}(I)$ *of* I to be $\gcd(\{\mathrm{Nrd}(\alpha) : \alpha \in I\})$.

An order $\mathcal{O} \subseteq B$ is *maximal* if it is not properly contained in any other order. There can exist distinct maximal orders in B which can even be non-isomorphic.

The situation is a little simpler for $B \otimes \mathbb{Q}_p$. Indeed, if B is split at p, there are infinitely many maximal orders in $B \otimes \mathbb{Q}_p$, but they are all conjugate to $M_2(\mathbb{Z}_p)$. If $B \otimes \mathbb{Q}_p$ is a division algebra, then one can extend the valuation on $\mathbb{Q}_p$ to $B \otimes \mathbb{Q}_p$, and the unique maximal order is the valuation ring. A $\mathbb{Z}$-order $\mathcal{O} \subseteq B$ is maximal if and only if $\mathcal{O} \otimes \mathbb{Q}_p$ is a maximal $\mathbb{Z}_p$-order in $B \otimes \mathbb{Q}_p$ for every prime p [Voi21, Lemma 10.4.3]. Thus, maximality of an order in B is a local property.

We can define the notion of discriminant also for an order $\mathcal{O} \subseteq B$. Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be a $\mathbb{Z}$-basis of $\mathcal{O}$, then the *discriminant* $\mathrm{disc}(\mathcal{O})$ is defined as

$$\mathrm{disc}(\mathcal{O}) \coloneqq \det(\langle \alpha_i, \alpha_j \rangle)_{1 \le i,j \le 4} = \det(\mathrm{Trd}(\alpha_i\bar{\alpha_j}))_{1 \le i,j \le 4} \in \mathbb{Z}.$$

It is possible to show that $\mathrm{disc}(\mathcal{O})$ is always a square, so we define the *reduced discriminant* $\mathrm{discrd}(\mathcal{O})$ of $\mathcal{O}$ to be the positive integer satisfying $\mathrm{discrd}(\mathcal{O})^2 = \mathrm{disc}(\mathcal{O})$. A $\mathbb{Z}$-order $\mathcal{O}$ is maximal in B if and only if $\mathrm{discrd}(\mathcal{O}) = \mathrm{disc}(B)$ [Voi21, Theorem 15.5.5]. Moreover, if $\mathcal{O} \subseteq \mathcal{O}'$, then $\mathrm{discrd}(\mathcal{O}) = [\mathcal{O}' \colon \mathcal{O}]\,\mathrm{discrd}(\mathcal{O}')$, where $[\mathcal{O}' \colon \mathcal{O}]$ denotes the index of $\mathcal{O}$ in $\mathcal{O}'$ as abelian groups [Voi21, Lemma 15.2.15].

We recall some of the properties of orders in a quaternion algebra B over $\mathbb{Q}$. We say that a $\mathbb{Z}$-order $\mathcal{O} \subset B$ is *Gorenstein* if every left ideal I of $\mathcal{O}$ satisfying $\mathcal{O}_L(I) = \mathcal{O}$ is invertible. The order $\mathcal{O}$ is *Bass* if every superorder $\mathcal{O}' \supseteq \mathcal{O}$ is Gorenstein. We are interested in Bass orders because, by [EHL$^+$, Proposition 5.2], one can efficiently enumerate the maximal superorders containing a given Bass order $\mathcal{O}$, and bound the number of these maximal superorders with a quantity growing subexponentially in the size of $\mathcal{O}$.[1] An order $\mathcal{O}$ is Bass if and only if it is *basic*, meaning $\mathcal{O}$ contains a maximal order in a commutative subalgebra of B, and being basic is a local property [Voi21, Proposition 24.5.10]: this fact was originally proved by Eichler [Eic36, Satz 8] for quaternion algebras over $\mathbb{Q}$, and generalized in [CSV21]. This allows us to prove an order is Bass by producing, for each prime ℓ, an imaginary quadratic order R in $\mathcal{O}$ whose conductor is coprime to ℓ.

3 Inseparable endomorphisms

Let E be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$ and let $\alpha \in \mathrm{End}(E)$. We say that α is *inseparable* if $\alpha = \pi \circ \phi$, where $\phi \in \mathrm{Hom}(E, E^{(p)})$. The set of inseparable endomorphisms $P \coloneqq \pi\,\mathrm{Hom}(E, E^{(p)})$ is a 2-sided ideal of $\mathrm{End}(E)$ and we refer to it as the *ideal of inseparable endomorphisms of* E.

In this section, we first study the arithmetic properties of $\mathbb{Z} + P \subseteq \mathrm{End}(E)$. Then in Subsection 3.2, we focus our attention on a particular kind of inseparable endomorphisms that we call *inseparable reflections*.

[1] Actually, this is proven in [EHL$^+$] under the additional assumption that $\mathcal{O}$ is hereditary (i.e. its reduced discriminant is squarefree), but this assumption is not necessary; see the proof of Theorem 4.3.

3.1 Properties of $\mathbb{Z} + P$

For completeness, we present the results of this subsection in the more general setting where B is a quaternion algebra over $\mathbb{Q}$ ramified at a prime p, $\mathcal{O}$ is a maximal order in B, and P is the unique 2-sided ideal in $\mathcal{O}$ of reduced norm p.

Proposition 3.1. *Let B be a quaternion algebra over $\mathbb{Q}$ ramified at a prime p. Let $\mathcal{O}$ be a maximal order in B and let P be the 2-sided ideal in $\mathcal{O}$ of reduced norm p. Then $\mathbb{Z} + P$ is a suborder of $\mathcal{O}$ of index p, and $\mathcal{O}$ is the unique maximal order of B containing $\mathbb{Z} + P$.*

Proof. We begin by showing that $\mathbb{Z} + P$ is an order. First, it is a lattice since it is finitely generated and $B = P\mathbb{Q} \subseteq (\mathbb{Z} + P)\mathbb{Q}$. Second, since P is an ideal, $\mathbb{Z} + P$ is closed under multiplication and contains $1 \in B$ so $\mathbb{Z} + P$ is a subring of B. Therefore $\mathbb{Z} + P$ is a suborder of $\mathcal{O}$.

We now calculate the index of $\mathbb{Z} + P$ in $\mathcal{O}$. Let $D = \operatorname{disc}(B)$. Since P is invertible (as it is an integral ideal of a maximal order, see [Voi21, Proposition 16.1.2]), by [Voi21, Proposition 16.7.7(iv)], we conclude $[\mathcal{O} : P] = \operatorname{Nrd}(P)^2 = p^2$. Since $\mathbb{Z} \cap P \simeq p\mathbb{Z}$ by [Voi21, 18.2.7(b)], as $\mathbb{Z}$-modules we have $(\mathbb{Z} + P)/P \simeq \mathbb{Z}/(\mathbb{Z} \cap P) \simeq \mathbb{Z}/p\mathbb{Z}$. Therefore, $[\mathbb{Z} + P : P] = p$. By multiplicativity of the index, we have $[\mathcal{O} : \mathbb{Z} + P] = p$, and so [Voi21, Lemma 15.2.15] implies

$$\operatorname{disc}(\mathbb{Z} + P) = [\mathcal{O} : \mathbb{Z} + P]^2 \operatorname{disc}(\mathcal{O}) = p^2 D^2 = (pD)^2.$$

Now we show that $\mathcal{O}$ is the only maximal order containing $\mathbb{Z} + P$. First, an order Λ in B is maximal at a prime $\ell \neq p$ if and only if $v_\ell(\operatorname{discrd}(\Lambda)) = v_\ell(D)$: this is because a maximal order in $M_2(\mathbb{Q}_\ell)$ has reduced discriminant equal to $\mathbb{Z}_\ell$ [Voi21, Lemma 15.5.3], and a maximal order in the division quaternion algebra over $\mathbb{Q}_\ell$ has reduced discriminant equal to $\ell\mathbb{Z}_\ell$ [Voi21, Example 15.5.4]. Since the reduced discriminant of $\mathbb{Z} + P$ is pD, we have $v_\ell(\operatorname{discrd}(\mathbb{Z} + P)) = v_\ell(p) + v_\ell(D) = v_\ell(D)$, and so the order $\mathbb{Z} + P$ is maximal at any prime $\ell \neq p$. Since B is ramified at p, by [Voi21, Lemmas 10.4.3, 13.3.4], $\mathcal{O} \otimes \mathbb{Z}_p$ is the unique maximal order of $B \otimes \mathbb{Q}_p$ and contains $(\mathbb{Z} + P) \otimes \mathbb{Z}_p$. We see that, for every prime ℓ, $\mathcal{O} \otimes \mathbb{Z}_\ell$ is the unique maximal $\mathbb{Z}_\ell$-order containing $(\mathbb{Z}+P)\otimes\mathbb{Z}_\ell$, so by [Voi21, Corollary 9.4.7, Theorem 9.4.9, Lemma 9.5.3], $\mathcal{O}$ is the unique maximal order containing $\mathbb{Z} + P$. □

Remark 3.2. The order $\mathbb{Z}+P$ is Bass, as its reduced discriminant is pD and thus cubefree [Voi21, Exercise 24.6.7(a)]. It is not Eichler [Voi21, Definition 23.4.1], since it fails to be Eichler at p (it is not maximal at p, and the only Eichler order in a local division quaternion algebra is the unique maximal order). It is not hereditary [Voi21, Definition 21.4.1], since its reduced discriminant is divisible by p^2 and is therefore not square-free [Voi21, Lemma 23.3.18]. However, the order $\mathbb{Z} + P$ is residually ramified at p since $(\mathbb{Z} + P)/P \simeq \mathbb{Z}/p\mathbb{Z}$ (see [Voi21, 24.3.2] for a definition of *residually ramified*). Finally, the order $\mathbb{Z} + P$ is the *order of level* p^2 in its unique maximal super-order (see [Piz80, Definition 3.5]).

Remark 3.3. Let $E/\mathbb{F}_{p^2}$ be a supersingular elliptic curve. To compute a basis of $\operatorname{End}(E)$, one can first compute a basis of $\mathbb{Z} + P \subseteq \operatorname{End}(E)$ and then use Algorithms 7.9 and 3.12 in [Voi13] to recover a basis of the unique maximal order $\mathcal{O}$ containing $\mathbb{Z} + P$. Proposition 3.1 implies $\mathcal{O} = \operatorname{End}(E)$.

3.2 Inseparable reflections

We now define, inside the ideal of inseparable endomorphisms of E, the *inseparable reflections*. These are inseparable endomorphisms whose construction is based on a symmetry of the supersingular ℓ-isogeny graph $G(p, \ell)$ given by the Galois involution (see Subsection 3.2.2 for a formal definition).

3.2.1 The Galois involution of $G(p, \ell)$

Let $\sigma_p \colon \mathbb{F}_{p^2} \to \mathbb{F}_{p^2}$ be the p-power Frobenius automorphism such that $\sigma_p(\alpha) = \alpha^p$, for $\alpha \in \mathbb{F}_{p^2}$. The Galois group $\operatorname{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p) = \langle \sigma_p \rangle$ acts on the set of elliptic curves defined over $\mathbb{F}_{p^2}$ sending E to $E^{(p)}$. Note that $(E^{(p)})^{(p)} = E$, so σ_p defines an involution. Moreover, notice that that $E^{(p)} = E$ if and only if E is defined over $\mathbb{F}_p$.

Similarly we can define an action of $\operatorname{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ on separable isogenies defined over $\mathbb{F}_{p^2}$. Given a rational function $f \in \mathbb{F}_{p^2}(x, y)$, let $f^{(p)}$ denote the rational function obtained by raising the coefficients of f to the

p-th power. Given a separable isogeny $\phi\colon E_1 \to E_2$ defined over $\mathbb{F}_{p^2}$, let us choose representative coordinate functions $f, g \in \mathbb{F}_{p^2}(E_1)$, defined on $E_1 - \ker\phi$, so that $\phi(x,y) = (f(x,y), g(x,y))$. Therefore, σ_p maps ϕ to the isogeny $\phi^{(p)}\colon E_1^{(p)} \to E_2^{(p)}$ such that $\phi^{(p)}(x,y) = (f^{(p)}(x,y), g^{(p)}(x,y))$. It is easy to see that the kernel of $\phi^{(p)}$ is $\pi(\ker\phi)$. Moreover, we have $(\phi^{(p)})^{(p)} = \phi$.

Lemma 3.4. *Let E_1, E_2, and E_3 be elliptic curves defined over $\mathbb{F}_{p^2}$, and let $\phi_1 : E_1 \to E_2$ and $\phi_2 : E_2 \to E_3$ be separable isogenies defined over $\mathbb{F}_{p^2}$. The following hold.*

(a) $(\phi_2 \circ \phi_1)^{(p)} = \phi_2^{(p)} \circ \phi_1^{(p)}$.

(b) $\phi_1^{(p)} \circ \pi = \pi \circ \phi_1$.

(c) $(\widehat{\phi_1^{(p)}})^{(p)} = \widehat{\phi_1}$. *Equivalently,* $\widehat{\phi_1}^{(p)} = \widehat{\phi_1^{(p)}}$.

Proof. Part (a) follows from the calculation that for functions $f, g, h \in \mathbb{F}_{p^2}(x,y)$, we have

$$(f(g(x,y), h(x,y)))^{(p)} = f^{(p)}(g^{(p)}(x,y), h^{(p)}(x,y)).$$

Next, we prove (b). Let us choose representative coordinate functions f, g so that $\phi_1(x,y) = (f(x,y), g(x,y))$. Then, $\phi_1^{(p)}(x,y) = (f^{(p)}(x,y), g^{(p)}(x,y))$. This implies

$$\begin{aligned}(\phi_1^{(p)} \circ \pi)(x,y) &= \phi_1^{(p)}(x^p, y^p)\\ &= (f^{(p)}(x^p, y^p), g^{(p)}(x^p, y^p))\\ &= ((f(x,y))^p, (g(x,y))^p)\\ &= (\pi \circ \phi_1)(x,y).\end{aligned}$$

We now prove (c). We compute

$$\begin{aligned}(\widehat{\phi_1^{(p)}})^{(p)} \circ \phi_1 &= (\widehat{\phi_1^{(p)}})^{(p)} \circ (\phi_1^{(p)})^{(p)} = ((\widehat{\phi_1^{(p)}}) \circ \phi_1^{(p)})^{(p)}\\ &= ([\deg \phi_1^{(p)}]_{E_1^{(p)}})^{(p)} = ([\deg \phi_1]_{E_1^{(p)}})^{(p)}\\ &= [\deg \phi_1]_{E_1},\end{aligned}$$

where the first equality follows since ϕ_1 is defined over $\mathbb{F}_{p^2}$, in the second equality we used part (a), and the fourth one we used $\deg \phi_1 = \deg \phi_1^{(p)}$. The last equality follows from the fact that coordinate functions for the multiplication-by-m map on a curve E is determined by $\psi_{E,m}$, the mth division polynomial of E [Sil09, Exercise 3.7], along with the observation that the recursive definition of $\psi_{E,m}$ implies $\psi_{E,m}^{(p)} = \psi_{E^{(p)},m}$. Therefore $\widehat{\phi_1} = (\widehat{\phi_1^{(p)}})^{(p)}$. □

Because every $\overline{\mathbb{F}_p}$-isomorphism class of supersingular elliptic curves contains a model defined over $\mathbb{F}_{p^2}$ such that all the isogenies are also defined over $\mathbb{F}_{p^2}$, the Frobenius automorphism $\sigma_p \in \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ induces an automorphism of order 2 of $G(p,\ell)$. In particular, for every ℓ-isogeny $\phi : E \to E'$ there is the ℓ-isogeny $\phi^{(p)} : E^{(p)} \to E'^{(p)}$. The fixed vertices of this automorphism correspond to supersingular curves defined over $\mathbb{F}_p$, and following the terminology of [ACNL+23], this action can be visualized as a reflection of $G(p,\ell)$ over the *spine* consisting of curves defined over $\mathbb{F}_p$. Going forward, in order to lighten the notation, we write $\psi\phi$, instead of $\psi \circ \phi$, for the composition of two (or more) isogenies.

3.2.2 Arithmetic properties of inseparable reflections

In order to define inseparable reflections we introduce the concept of (d,ϵ)-structures, defined by Chenu and Smith in [CS21].

Definition 3.5. Let d be a positive integer coprime to p. A (d,ϵ)-*structure* is a pair (E,ψ) where E is an elliptic curve defined over $\mathbb{F}_{p^2}$ and $\psi\colon E \to E^{(p)}$ is a degree d-isogeny satisfying $\psi^{(p)} = \epsilon\widehat{\psi}$ with $\epsilon \in \{\pm 1\}$. We say (E,d) is *supersingular* if E is supersingular.

A (d, ϵ)-structure (E, ψ) yields an endomorphism $\mu = \pi\psi$ of E, which Chenu and Smith call its *associated endomorphism*. When d is square-free, a supersingular (d, ϵ)-structure (E, ψ) yields an associated endomorphism $\mu = \pi\psi$ of E such that $\mathbb{Z}[\mu] \simeq \mathbb{Z}[\sqrt{-dp}]$, [CS21, Proposition 2]. In fact, this holds for arbitrary d coprime to p, assuming $p > 3$.

Proposition 3.6. *Let d be an integer coprime to a prime $p > 3$, and let (E, ψ) be a (d, ϵ)-structure. If $\mu = \pi\psi$ is the associated endomorphism of E, then $\mu^2 = [-dp]$ and $\pi_E = -\epsilon p$.*

Proof. The argument is similar to those in Propositions 1 and 2 of [CS21]. First, since (E, ψ) is a (d, ϵ) structure, we have $\psi^{(p)} = \epsilon\widehat{\psi}$. Therefore,

$$\mu^2 = \pi\psi\pi\psi = \pi\pi\psi^{(p)}\psi = \pi_E\epsilon\widehat{\psi}\psi = \epsilon d\pi_E.$$

Let $x^2 - ax + dp$ be the characteristic polynomial of μ. We now show $a = 0$. Suppose toward a contradiction that a is nonzero. We have $a\mu = \mu^2 + dp = \epsilon d\pi_E + dp$. Taking traces, we have

$$a^2 = \operatorname{Trd}(a\mu) = \operatorname{Trd}(\epsilon d\pi_E + dp) = \epsilon d \operatorname{Trd}\pi_E + 2dp.$$

We first observe this implies $d|a^2$. Since E is supersingular, we have $p|\operatorname{Trd}\pi_E$, so we conclude $p|a^2$, and since p is prime, $p^2|a^2$ as well. Since p and d are coprime, dp^2 divides a^2. Since we assume a is nonzero, we obtain $dp^2 \leq a^2$. On the other hand, $\mathbb{Z}[\mu]$ must have non-positive discriminant, so $a^2 - 4dp < 0$. Thus

$$dp^2 \leq a^2 \leq 4dp,$$

which implies $p < 4$. This is our desired contradiction, so we conclude $a = 0$ and $\mu^2 = -dp$. Finally, we have $0 = \epsilon d \operatorname{Trd}\pi_E + 2dp$, which implies $\operatorname{Trd}\pi_E = -2\epsilon p$. This implies $\pi_E = -\epsilon p$. □

We now discuss a construction of a (d, ϵ)-structure for d which is not necessarily squarefree.

Proposition 3.7. *Let E_1 be a supersingular elliptic curve. If $\phi\colon E_1 \to E_2$ is a d_1-isogeny and (E_2, ψ) is a (d, ϵ)-structure, then $(E_1, \widehat{\phi^{(p)}}\psi\phi)$ is a $(d_1^2 d, \epsilon)$-structure.*

Proof. We must show $(\widehat{\phi^{(p)}}\psi\phi)^{(p)} = \epsilon\widehat{\widehat{\phi^{(p)}}\psi\phi}$:

$$\begin{aligned}
(\widehat{\phi^{(p)}}\psi\phi)^{(p)} &= (\widehat{\phi^{(p)}})^{(p)}\psi^{(p)}\phi^{(p)} && \text{by Lemma 3.4, part (a)} \\
&= \widehat{\phi}\psi^{(p)}\phi^{(p)} && \text{by Lemma 3.4 part (c)} \\
&= \widehat{\phi}\epsilon\widehat{\psi}\phi^{(p)} && (E, \psi) \text{ is a } (d, \epsilon) - \text{structure} \\
&= \epsilon\widehat{\widehat{\phi^{(p)}}\psi\phi}.
\end{aligned}$$

□

Below, we define a special type of associated endomorphism to a (d, ϵ)-structure. We call these endomorphisms *inseparable reflections* since they arise from paths in isogeny graphs whose image under the Frobenius involution is the same path, traversed in the opposite direction.

Definition 3.8. Let p be a prime, and let d_1, d be coprime integers, with d square-free, which are both coprime to p. An *inseparable reflection* of degree $d_1^2 dp$ of a supersingular elliptic curve E_1 defined over $\mathbb{F}_{p^2}$ is an endomorphism

$$\alpha = \pi\widehat{\phi^{(p)}}\psi\phi$$

such that $\phi\colon E_1 \to E_2$ is a cyclic d_1-isogeny, (E_2, ψ) is a (d, ϵ)-structure, and ϕ does not factor nontrivially through an isogeny $\phi'\colon E_1 \to E_2'$ such that E_2' has a (d, ϵ)-structure (E_2', ψ').

We now study the arithmetic of orders generated by inseparable reflections. First, we determine the imaginary quadratic order generated by a single inseparable reflection, then we study orders generated by two or more inseparable reflections. In particular, we give sufficient conditions for when two inseparable reflections do not commute and hence generate a quaternionic suborder of $\operatorname{End}(E)$. The following proposition follows immediately from Propositions 3.6 and 3.7.

Proposition 3.9. *Let E be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$, and let $\alpha = \pi\widehat{\phi^{(p)}}\psi\phi$ be an inseparable reflection of degree $d_1^2 dp$. Then $\alpha^2 = [-d_1^2 dp]$ and in particular α has trace zero.*

We show in Lemma 3.11 that the kernel of an inseparable reflection is cyclic. For this, we need the following lemma.

Lemma 3.10. *Let E_1, E_2, and E_3 be elliptic curves defined over $\mathbb{F}_q$ and let $\phi_1 \colon E_1 \to E_2$ and $\phi_2 \colon E_2 \to E_3$ be separable, cyclic isogenies. Then $\ker(\phi_2\phi_1)$ is cyclic if and only if $\ker\widehat{\phi_1} \cap \ker\phi_2$ is trivial.*

Proof. If $\ker\widehat{\phi_1} \cap \ker\phi_2 = G$ is nontrivial, let $\tau \colon E_2 \to E'$ be a separable isogeny with kernel G, where E' is an elliptic curve defined over $\mathbb{F}_q$. Then, both $\widehat{\phi_1}$ and ϕ_2 factor through τ: there exist isogenies ψ_1, ψ_2 such that $\widehat{\phi_1} = \psi_1\tau$ and $\phi_2 = \psi_2\tau$.

$$\begin{array}{ccccc} E_1 & \xrightarrow{\phi_1} & E_2 & \xrightarrow{\phi_2} & E_3 \\ & \nwarrow^{\psi_1} & \downarrow{\scriptstyle \tau} & \nearrow_{\psi_2} & \\ & & E' & & \end{array}$$

Then,

$$\phi_2\phi_1 = \psi_2\tau\widehat{\tau}\widehat{\psi_1} = \psi_2\widehat{\psi_1}[\#G]$$

does not have cyclic kernel.

Now assume that $\ker(\phi_2\phi_1)$ is not cyclic. Let $S \in E_2(\overline{\mathbb{F}_q})$ such that $\ker\phi_2 = \langle S\rangle$, the cyclic group generated by S, and let $Q \in E_1(\overline{\mathbb{F}_q})$ such that $\phi_1(Q) = S$. Also let $P \in E_1(\overline{\mathbb{F}_q})$ such that $\langle P\rangle = \ker\phi_1$.

First, we claim that $\ker(\phi_2\phi_1) = \langle P\rangle + \langle Q\rangle$. Let $P' \in \ker(\phi_2\phi_1)$. Then, $\phi_1(P') = [a]S$ for some a. Therefore, $P' - [a]Q \in \ker\phi_1$. Thus,

$$P' = (P' - [a]Q) + [a]Q \in \ker\phi_1 + \langle Q\rangle = \langle P\rangle + \langle Q\rangle,$$

i.e. $\ker(\phi_2\phi_1) \subseteq \langle P\rangle + \langle Q\rangle$. Since $\phi_1(\langle P\rangle + \langle Q\rangle) \subseteq \ker\phi_2$, we also have that $\ker(\phi_2\phi_1) \supseteq \langle P\rangle + \langle Q\rangle$. Thus, $\ker(\phi_2\phi_1) = \langle P\rangle + \langle Q\rangle$.

Since we assume that $\ker(\phi_2\phi_1)$ is not cyclic, $\langle P\rangle + \langle Q\rangle$ contains $E_1[d]$ for some $d > 1$. Note that d and $\deg\phi_1$ are not coprime, since otherwise $\phi_1(E_1[d]) = E_2[d]$ and thus $E_2[d] \subseteq \ker\phi_2$, contradicting the assumption that $\ker\phi_2$ is cyclic. Let $g = \gcd(d, \deg\phi_1)$. Then, $E_1[g] \subseteq E_1[d]$ and $E_1[g] \subseteq E_1[\deg\phi_1]$. Now we have that $\phi_1(E_1[g]) \subseteq \ker\phi_2$ and also $\phi_1(E_1[g]) \subseteq \ker\widehat{\phi_1} = \phi_1(E_1[\deg\phi_1])$, therefore $\phi_1(E_1[g]) \subseteq \ker\widehat{\phi_1} \cap \ker\phi_2$. Since ϕ_1 is cyclic and $g > 1$, $\phi_1(E_1[g]) \neq 0$, so $\ker\widehat{\phi_1} \cap \ker\phi_2 \neq 0$. □

Lemma 3.11. *Let E_1 be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$ and let $\alpha = \pi\widehat{\phi^{(p)}}\psi\phi$ be an inseparable reflection of degree $d_1^2 dp$. Then the kernel of α is cyclic.*

Proof. It suffices to show that $\widehat{\phi^{(p)}}\psi\phi \colon E_1 \to E_1^{(p)}$ has cyclic kernel. Assume that $\ker(\widehat{\phi^{(p)}}\psi\phi)$ is not cyclic. Let E_2 be the codomain of ϕ. We show that there is an isogeny $\tau \colon E_2 \to E_3$ such that $\ker\tau \subseteq \ker\widehat{\phi}$ and E_3 has a (d, ϵ)-structure. By Lemma 3.10, we have that $G = \ker\widehat{\phi} \cap \ker\widehat{\phi^{(p)}}\psi \neq 0$. Note that G is defined over $\mathbb{F}_{p^2}$, since it is contained in $\ker\widehat{\phi}$ which is defined over $\mathbb{F}_{p^2}$. Let $\tau \colon E_2 \to E_3$ be an isogeny defined over $\mathbb{F}_{p^2}$ with kernel G.

$$\begin{array}{ccccc} E_1 & \xrightarrow{\phi} & E_2 & \xrightarrow{\tau} & E_3 \\ {\scriptstyle \pi}\downarrow & & \downarrow{\scriptstyle \psi} & & \\ E_1^{(p)} & \xrightarrow{\phi^{(p)}} & E_2^{(p)} & & \end{array}$$

We show that E_3 has an (d,ϵ)-structure. By [CS21, Lemma 1], it suffices to show that $\mathrm{End}(E_3)$ contains a quadratic order isomorphic to $\mathbb{Z}[\sqrt{-dp}]$.

First, we claim that $\pi\psi(G) = G$. Since $G \subseteq \ker(\widehat{\phi^{(p)}}\psi)$, we have that

$$\psi(G) \subseteq \ker \widehat{\phi^{(p)}} = \pi(\ker \widehat{\phi}).$$

Since $\gcd(d_1, d) = 1$, we see that ψ induces an isomorphism $E_2[d_1] \to E_2^{(p)}[d_1]$. Thus, since $G \subset E_2[d_1]$, we have $\#\psi(G) = \#G$. Moreover, $\ker \widehat{\phi}$ is cyclic, so $\pi(\ker \widehat{\phi})$ is also cyclic. Therefore, $\psi(G)$ is the unique subgroup of $\pi(\ker \widehat{\phi})$ of order $\#G$. Since the unique subgroup of $\ker \widehat{\phi}$ of order $\#G$ is also G, we have

$$\psi(G) = \pi(G).$$

From this we conclude that

$$\pi\psi(G) = \pi(\pi(G)) = G,$$

where the last equality holds since τ is defined over $\mathbb{F}_{p^2}$. Therefore the proof of the claim is complete.

Now consider the endomorphism

$$\rho = \tau\pi\psi\widehat{\tau} \in \mathrm{End}(E_3).$$

We claim that $\rho(E_3[\deg\tau]) = 0$. Indeed,

$$\rho(E_3[\deg\tau]) = \tau\pi\psi\widehat{\tau}(E_3[\deg\tau]) = \tau\pi\psi(\ker\tau) = \tau\pi\psi(G) = \tau(G) = 0.$$

Thus, $\mu = \frac{1}{\deg\tau}\rho$ is an endomorphism of E_3. Observe that

$$\mu^2 = \frac{1}{(\deg\tau)^2}\tau\pi\psi\widehat{\tau}\tau\pi\psi\widehat{\tau} = \frac{1}{\deg\tau}\tau\pi\psi\pi\psi\widehat{\tau} = \frac{-dp}{\deg\tau}\tau\widehat{\tau} = -dp,$$

so $\mathbb{Z}[\mu] \simeq \mathbb{Z}[\sqrt{-dp}]$. As mentioned above, by Lemma 1 of [CS21], it follows that E_3 has a (d,ϵ)-structure (indeed, $\mu = \pi\psi'$ for an isogeny $\psi' \colon E_3 \to E_3^{(p)}$, and (E_3, ψ') is the desired (d,ϵ)-structure).

□

We now use Lemma 3.9, Lemma 3.10, and Lemma 3.11 to prove that we can choose two inseparable endormophisms that do not commute.

Theorem 3.12. *Let E be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$, and let $\alpha_1 = \pi\widehat{\phi_1^{(p)}}\psi_1\phi_1$ and $\alpha_2 = \pi\widehat{\phi_2^{(p)}}\psi_2\phi_2$ be inseparable reflections of degree d_1^2dp and d_2^2dp. If $\ker\phi_1 \neq \ker\phi_2$, then α_1 and α_2 do not commute.*

Proof. Assume that α_1 and α_2 commute. Then, $\mathbb{Q}(\alpha_1) = \mathbb{Q}(\alpha_2)$, so there exist integers k, m, n such that $[k]\alpha_1 = [m] + [n]\alpha_2$. By Lemma 3.9, we have $\mathrm{Trd}(\alpha_1) = \mathrm{Trd}(\alpha_2) = 0$, so $m = 0$ and $[k]\alpha_1 = [n]\alpha_2$. We claim that $k|n$. Write $n = kq + r$ with $0 \leq r < k$. Note that since $[n](\alpha_2(E[k])) = 0$, we also have $[r](\alpha_2(E[k])) = 0$. This implies $\alpha_2\left(E\left[\frac{k}{\gcd(k,r)}\right]\right) = 0$. The kernel of α_2 is cyclic by Lemma 3.11, so we must have that $k/\gcd(k,r) = 1$ and hence $\gcd(k,r) = k$ implying $r = 0$. Thus $k|n$. Therefore $\alpha_1 = [n/k]\alpha_2$. Now, since α_1 has cyclic kernel by Lemma 3.11, we conclude $n/k = \pm 1$. Thus, $\alpha_1 = \pm\alpha_2$ and so, $\ker\alpha_1 = \ker\alpha_2$ and $\deg\phi_1 = \deg\phi_2$. Therefore, using the property that $\ker\alpha_i$ is cyclic for $i = 1, 2$, we obtain $\ker\phi_1 = \ker\phi_2$. □

4 Bass suborders of $\mathrm{End}(E)$

In this section we show how to construct Bass suborders of $\mathrm{End}(E)$ using inseparable reflections.

Proposition 4.1. *Let E be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$, and let d_1, d_2, d be three pairwise coprime integers, with d square-free. For $i = 1, 2$, let $\alpha_i = \pi\widehat{\phi_i^{(p)}}\psi_i\phi_i \in \mathrm{End}(E)$ be inseparable reflections of degree d_i^2dp.*

(i) The endomorphisms $1, \alpha_1, \alpha_2, \alpha_1\alpha_2$ generate an order

$$\Lambda_{\alpha_1\alpha_2} := \mathbb{Z} + \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \mathbb{Z}\alpha_1\alpha_2 \subseteq \mathrm{End}(E).$$

(ii) The endomorphism $\alpha_1\alpha_2$ factors through the multiplication-by-p map, so

$$\rho := \frac{-\alpha_1\alpha_2}{p}$$

is an endomorphism of E. The discriminant of $\Lambda_{\alpha_1\alpha_2}$ is

$$\mathrm{disc}(\Lambda_{\alpha_1\alpha_2}) = p^4 \cdot (\mathrm{Tr}(\rho)^2 - 4\deg(\rho))^2 = p^4 \cdot \mathrm{disc}(\rho)^2.$$

(iii) The order $\Lambda_{\alpha_1\alpha_2}$ is Gorenstein.

Proof. Lemma 3.9 implies α_1 and α_2 are non-scalar endomorphisms. Since $d_1 \neq d_2$, we have that $\ker\phi_1 \neq \ker\phi_2$ so $\alpha_1\alpha_2 \neq \alpha_2\alpha_1$ by Theorem 3.12. The endomorphisms α_1 and α_2 are noncommuting, nonscalar elements of $\mathrm{End}^0(E)$, so $\Lambda_{\alpha_1\alpha_2}$ is a lattice in $\mathrm{End}^0(E)$. Since $\alpha_1, \alpha_2, \alpha_1\alpha_2$ are integral, the lattice $\Lambda_{\alpha_1\alpha_2}$ is a ring containing 1, so it is an order, completing the proof of part (i).

To prove part (ii) we compute discrd($\Lambda_{\alpha_1\alpha_2}$). Since $\mathrm{Trd}\,\alpha_i = 0$, we have $\widehat{\alpha_i} = -\alpha_i$, so

$$\rho = \frac{-1}{p}\alpha_1\alpha_2 = \frac{1}{p}\widehat{\phi_1}\widehat{\psi_1}\widehat{\pi}\pi\phi_1^{(p)}\widehat{\phi_2^{(p)}}\psi_2\phi_2 = \widehat{\phi_1}\widehat{\psi_1}\phi_1^{(p)}\widehat{\phi_2^{(p)}}\psi_2\phi_2.$$

The Gram matrix of the basis $1, \alpha_1, \alpha_2, \alpha_1\alpha_2$ is

$$G := \begin{pmatrix} 2 & 0 & 0 & -p\,\mathrm{Trd}(\rho) \\ 0 & 2pdd_1^2 & p\,\mathrm{Trd}(\rho) & 0 \\ 0 & p\,\mathrm{Trd}(\rho) & 2pdd_2^2 & 0 \\ -p\,\mathrm{Trd}(\rho) & 0 & 0 & 2(pd_1d_2d)^2 \end{pmatrix}.$$

A calculation shows its determinant, and therefore the discriminant of $\Lambda\alpha_1\alpha_2$, is

$$\det(G) = p^4 \cdot (\mathrm{Tr}(\rho)^2 - 4\deg(\rho))^2 = p^4 \cdot \mathrm{disc}(\rho)^2.$$

Finally we prove part (iii). We claim that the ternary quadratic form attached to $\Lambda_{\alpha_1\alpha_2}$ is

$$Q(x, y, z) = pdd_2^2x^2 + pdd_1^2y^2 + z^2 - tpxy,$$

where $t = \mathrm{Trd}\,\rho$. A calculation shows the basis $1, i = \alpha_1, j = \alpha_2, k = \alpha_2\alpha_1$ of $\Lambda_{\alpha_1\alpha_2}$ is a *good basis* in the sense of [Voi21, 22.4.7], i.e., there exist integers a, b, c, u, v, w satisfying $i^2 = ui - bc$, $j^2 = vj - ac$, $k^2 = wk - ab$ and $jk = a\widehat{i}$, $ki = b\widehat{j}$, and $ij = c\widehat{k}$. Given a good basis, the corresponding ternary quadratic form is $ax^2+by^2+cz^2+uyz+vxz+wxy$ (see the proof of [Voi21, Proposition 22.4.12]). Since d_1, d_2, d, and p are pairwise coprime, we see that Q is primitive and thus, Λ is Gorenstein by [Voi21, Theorem 24.2.10]. □

Remark 4.2. The lattice $\Lambda_\rho := \mathbb{Z} + \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \mathbb{Z}\rho$ in $\mathrm{End}(E)$ is also a suborder of $\mathrm{End}(E)$ and clearly $\Lambda_{\alpha_1\alpha_2} \subsetneq \Lambda_\rho$. The order $\Lambda_{\alpha_1\alpha_2}$ is non-maximal precisely at p and the primes dividing the discriminant of ρ. Assuming that $p \nmid \mathrm{disc}(\rho)$, the order Λ_ρ is the unique p-maximal order containing $\Lambda_{\alpha_1\alpha_2}$ whose localizations at all $\ell \neq p$ agree with those of $\Lambda_{\alpha_1\alpha_2}$.

Theorem 4.3. *Let E be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$, and let d_1, d_2, d be three pairwise coprime integers, with d square-free. For $i = 1, 2$, let $\alpha_i = \pi_p\widehat{\phi_i^{(p)}}\psi_i\phi_i \in \mathrm{End}(E)$ be inseparable reflections of degree d_i^2dp. Finally, assume that $-dp \not\equiv 1 \pmod 4$. Then the order $\Lambda_{\alpha_1\alpha_2}$ is Bass.*

Proof. Proposition 4.1 implies that $\Lambda_{\alpha_1\alpha_2}$ is an order. We show that $\Lambda_{\alpha_1\alpha_2}$ is locally basic, and hence locally Bass by [Brz90, Proposition 1.11] at every prime ℓ. This suffices, since being Bass is a local property [Voi21, Proposition 24.5.10].

Consider the quadratic order $R_i = \mathbb{Z}[\alpha_i] \simeq \mathbb{Z}[d_i\sqrt{-dp}]$ in $\Lambda_{\alpha_1\alpha_2} \subseteq \mathrm{End}(E)$. Since $-dp$ is square-free and not congruent to 1 modulo 4, the maximal order in the fraction field of R_i is isomorphic to $\mathbb{Z}[\sqrt{-dp}]$, so the conductor of R_i is d_i. Then, for any prime ℓ, at least one of R_1 or R_2 is maximal at ℓ since R_1 is maximal at every prime ℓ which does not divide d_1, and R_2 is maximal at every prime ℓ which does not divide d_2. This shows $\Lambda_{\alpha_1\alpha_2}$ is locally basic at each prime ℓ. □

5 Computing $\mathrm{End}(E)$ with inseparable endomorphisms and enumeration

We consider the following computational problem:

Problem 1. *Given a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$, compute the endormorphism ring $\mathrm{End}(E)$ of E, that is, compute a basis of the maximal order $\mathcal{O}$ in the quaternion algebra $B_{p,\infty}$ such that $\mathrm{End}(E) \cong \mathcal{O}$.*

In the previous section we saw that inseparable reflections of E can be used to build a Bass suborder Λ of $\mathrm{End}(E)$. Next, we enumerate the maximal orders of $B_{p,\infty}$ containing Λ and return the one which is isomorphic to $\mathrm{End}(E)$. Therefore, our algorithm to compute the endomorphism ring of a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$ involves three algorithms:

- **Algorithm** 1: Given a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$ and two coprime integers ℓ and d, with d square-free, the algorithm returns an inseparable reflection $\alpha = \pi\widehat{\phi^{(p)}}\psi\phi$ of degree $\ell^{2n}dp$, for some integer n.
- **Algorithm** 2: Given a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$ and three pairwise coprime integers ℓ_1, ℓ_2, and d, with d square-free, the algorithm runs Algorithm 1 twice to get two inseparable reflections $\alpha_1 = \pi\widehat{\phi_1^{(p)}}\psi_1\phi_1$ and $\alpha_2 = \pi\widehat{\phi_2^{(p)}}\psi_2\phi_2$ of degree respectively $\ell_1^{2n_1}dp$ and $\ell_2^{2n_2}dp$. Then, it returns the Bass order
$$\Lambda_{\alpha_1\alpha_2} := \mathbb{Z} + \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \mathbb{Z}\alpha_1\alpha_2.$$
- **Algorithm** 3: Given a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$ and three pairwise coprime integers ℓ_1, ℓ_2, and d, with d square-free, the algorithm runs Algorithm 2 to get a Bass order Λ contained in $\mathrm{End}(E)$. Then, the algorithm enumerates the maximal orders $\mathcal{O}$ of $B_{p,\infty}$ containing Λ, until $\mathcal{O} \cong \mathrm{End}(E)$.

5.1 Computing inseparable reflections

We compute an inseparable reflection of degree $\ell^{2t}dp$ by taking random non-backtracking walks beginning at E of length t, which correspond to cyclic ℓ^t isogenies $\phi\colon E \to E'$, until finding a (d,ϵ)-structure (E',ψ). The resulting inseparable reflection of E is $\pi\widehat{\phi^{(p)}}\psi\phi$. In order to bound the expected runtime of this approach, we must consider the probability that a random non-backtracking walk of length t terminates at a supersingular curve E' with a (d,ϵ)-structure.

Let $p > 3$ be a prime. Let $V = V(p) = \{E_i\}_{1\le i\le n}$ denote a complete set of representatives of isomorphism classes of supersingular elliptic curves over $\mathbb{F}_{p^2}$. For a prime $\ell \neq p$, let a_{ij} denote the number of cyclic subgroups C of $E_i[\ell]$ such that $E_i/C \simeq E_j$. Consider the $\mathbb{C}$-vector space H with basis V. Define an inner product on H by $\langle E_i, E_j\rangle = w_i\delta_{ij}$ and extended via linearity, where δ_{ij} is the Kronecker delta function and $w_i := \#\operatorname{Aut}(E_i)/2$. Define the operator A on H by $AE_i = \sum_j a_{ij}E_j$. Then, A is self-adjoint as an operator on H with respect to $\langle,\rangle$. A walk on the graph $G(p,\ell)$ is defined to be a sequence of edges $\phi_1,\phi_2,\ldots,\phi_k$ such that the codomain of ϕ_i is isomorphic to the domain of ϕ_{i+1}. A walk has no backtracking, or is non-backtracking, if $\phi_{i+1} \neq u\widehat{\phi_i}$ for any automorphism u. Thus, non-backtracking walks in $G(p,\ell)$ beginning at E_i are in bijection with cyclic subgroups of $E_i[\ell^\infty]$. Holding ℓ constant, the following proposition states that a walk of length $O(\log p)$ will land in a set $X \subseteq V$ with probability proportional to $\#X/\#V$.

Proposition 5.1. *Let $J \subseteq \{1,2,\ldots,n\}$ and $X = \{E_j\}_{j\in J} \subseteq V$. If*
$$t/2 - \log_\ell\left(t + \frac{\ell-1}{\ell+1}\right) \ge \log_\ell\left(\frac{(p-1)^{3/2}}{24\sum_{j\in J} w_j^{-1}}\right),$$
then a non-backtracking random walk of length t beginning at E_i lands in X with probability at least
$$\frac{6}{p-1}\sum_{j\in J} w_j^{-1}.$$

Proof. Let $P^{(t)}$ be the transition matrix for the non-backtracking random walk on $G(p,\ell)$ of length t. Let $\pi^{(t)} = P^{(t)}E_i$ be the probability distribution on V resulting from a random non-backtracking walk of length t beginning at E_i. Also, let $\mathcal{E} = \sum w_j^{-1}E_j$, so $s = \frac{1}{\langle \mathcal{E},\mathcal{E}\rangle}$ is the stationary distribution for the random walk on $G(p,\ell)$. Then, by Theorem 11 of [BCC+23],

$$|\pi^{(t)}(X) - s(X)| \le d_{TV}(\pi^{(t)}, s) \le \frac{(p-1)^{1/2}}{4} \cdot \left(t + \frac{\ell-1}{\ell+1}\right) \cdot \ell^{-t/2}.$$

We have

$$s(X) = \frac{12}{p-1} \sum_{j\in J} w_j^{-1}.$$

We see that if

$$t/2 - \log_\ell \left(t + \frac{\ell-1}{\ell+1}\right) \ge \log_\ell \left(\frac{(p-1)^{3/2}}{24\sum_{j\in J} w_j^{-1}}\right),$$

then

$$\frac{(p-1)^{1/2}}{4} \cdot \left(t + \frac{\ell-1}{\ell+1}\right) \cdot \ell^{-t/2} \le \frac{6}{p-1} \sum_{j\in J} w_j^{-1},$$

so

$$\pi^{(t)}(X) \ge \frac{6}{p-1} \sum_{j\in J} w_j^{-1},$$

as desired. □

First, we show that if $d < p/4$, a curve E has a (d,ϵ)-structure if and only if E is d-isogenous to $E^{(p)}$. This holds if and only if $\Phi_d(j(E), j(E)^p) = 0$, giving us an efficient method for testing whether E has a (d,ϵ)-structure. The following lemma is an adaptation of [CGL09, Lemma 6], and we include a proof for convenience.

Lemma 5.2. *Let E be a supersingular elliptic curve over $\mathbb{F}_{p^2}$, and let $1 < d < p/4$ be square-free and coprime to p. Then E has a (d,ϵ)-structure (E,ψ) if and only if E is d-isogenous to $E^{(p)}$.*

Proof. If (E,ψ) is a (d,ϵ)-structure, then $\psi\colon E \to E^{(p)}$ is a d-isogeny. Assume now that E is d-isogenous to $E^{(p)}$, and let $\psi\colon E \to E^{(p)}$ be a d-isogeny. We show that the characteristic polynomial of $\mu = \pi\psi$ is $x^2 + dp$: if this holds, then we have an embedding $\mathbb{Z}[\sqrt{-dp}] \hookrightarrow \mathrm{End}(E)$ defined by sending $\sqrt{-dp}$ to $\mu = \pi\psi$, and [CS21, Lemma 1] then implies that (E,ψ) is a (d,ϵ)-structure. Since the degree of μ is $(\deg\pi)(\deg\psi) = pd$, we only need to show that $t \coloneqq \operatorname{Trd}\mu$ is zero. The ring $\mathbb{Z}[\mu]$ must be an imaginary quadratic order since $\deg\mu$ is not a square and p cannot split in this order. Thus, $x^2 - tx + pd \equiv x^2 - tx \pmod p$ cannot have distinct roots modulo p, so we must have $t \equiv 0 \pmod p$. Since the discriminant of μ is negative, by our assumption that $d < p/4$, we have

$$|t| < 2\sqrt{pd} < p.$$

Thus, $t = 0$. □

We now bound the expected number of random walks beginning at E which we take before finding a (d,ϵ)-structure. Let $\operatorname{llog} x$ denote $\log\log x$.

Proposition 5.3 (GRH)**.** *Assume GRH. Let $p > 12$ be a prime, and let E be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$ such that $\#E(\mathbb{F}_{p^2}) = (p+\epsilon)^2$ for $\epsilon = \pm 1$. Let $\ell \ne p$ be a prime, and let $d = 1$ or 2. Let X be the collection of isomorphism classes of supersingular elliptic curves with a (d,ϵ)-structure. If*

$$t/2 - \log_\ell \left(t + \frac{\ell-1}{\ell+1}\right) \ge \log_\ell \left(\frac{(p-1)^{3/2}}{8}\right),$$

then a non-backtracking walk in $G(p,\ell)$ beginning at E of length t lands in X with probability at least $\Omega\left(\frac{1}{\sqrt{p}\operatorname{llog} p}\right)$.

Proof. The set X is nonempty because [CS21, Corollary 1] implies that the number of isomorphism classes of (d,ϵ)-structures is at least the class number of $\mathbb{Z}[\sqrt{-dp}]$. Since X is nonempty, we have

$$\sum_{E\in X}\frac{2}{\#\operatorname{Aut}(E)}\geq 1/3,$$

so for t satisfying the hypothesis in the proposition, we have

$$\begin{aligned} t/2-\log_\ell\left(t+\frac{\ell-1}{\ell+1}\right) &\geq \log_\ell\left(\frac{(p-1)^{3/2}}{8}\right)\\ &\geq \log_\ell\left(\frac{(p-1)^{3/2}}{24\sum_{E\in X}\frac{2}{\#\operatorname{Aut}(E)}}\right). \end{aligned}$$

By Proposition 5.1, a non-backtracking walk beginning at E lands in X with probability at least

$$\frac{6}{p-1}\cdot\sum_{E\in X}\frac{2}{\#\operatorname{Aut}(E)}\geq\frac{6}{p-1}(\#X-7/6).$$

Let $K=\mathbb{Q}(\sqrt{-pd})$. By [CS21, Corollary 1], there are at least h_K many (d,ϵ)-structures, up to $\mathbb{F}_{p^2}$-isomorphism. Since any given E has at most $d+1$ d-isogenies, and since the number of distinct $\mathbb{F}_{p^2}$-isomorphism classes of curves with the same j-invariant is at most 6, we have that

$$\#X\geq\frac{1}{6(d+1)}h_K.$$

Assuming the Generalized Riemann Hypothesis,

$$h_K=\Omega(\sqrt{pd}/\operatorname{llog}(pd))=\Omega(\sqrt{p}/\operatorname{llog}(p))$$

by [Lit28, Theorem 1]. We conclude that a non-backtracking walk of length t lands in X with probability $\Omega\left((\sqrt{p}\operatorname{llog}(p))^{-1}\right)$.

□

Algorithm 1: Compute an inseparable reflection

Input: A supersingular elliptic curve $E/\mathbb{F}_{p^2}$ and two coprime integers ℓ and d, with d square-free and $d<p/4$.

Output: An inseparable reflection $\alpha=\pi_p\widehat{\phi^{(p)}}\psi\phi\in\operatorname{End}(E)$ where $\phi\colon E\to E'$ is an ℓ^n-isogeny (represented by a sequence of ℓ-isogenies) and $\psi\colon E'\to E'^{(p)}$ a d-isogeny such that (E',ψ) is a (d,ϵ)-structure.

Compute the least integer t such that $t/2-\log_\ell\left(t+\frac{\ell-1}{\ell+1}\right)\geq\log_\ell\left(\frac{(p-1)^{3/2}}{8}\right)$;

repeat

  Compute a random, non-backtracking walk $W=\{\phi_1\colon E\to E_1,\dots,\phi_t\colon E_{t-1}\to E_t\}$ in $G(p,\ell)$ of length t;

until E_t *is* d*-isogenous to* $E_t^{(p)}$;

Let $k=\min_{1\leq i\leq t}\{i : E_i \text{ is } d\text{-isogenous to } E_i^{(p)}\}$;

Compute a (d,ϵ)-structure (E_k,ψ);

return $\{\phi_1,\dots,\phi_k,\psi,\widehat{\phi_k}^{(p)},\dots,\widehat{\phi_1}^{(p)},\pi_p\}$

While we allow ℓ and d to vary to give the algorithm some flexibility, we only need to run Algorithm 1 on inputs of the form $(E,\ell,2)$ (to compute Bass orders) and inputs $(E,\ell,1)$ (for our heuristic algorithm described in Section 6), where ℓ is a fixed small prime, such as $2,3$, or 5. Thus in our complexity analysis below, we are treating ℓ and d as constants. Similar results hold for square-free $d=O(\log p)$ and prime $\ell=O(\log p)$. Let $\mathsf{M}(n)$ denote the cost of multiplying two n-bit integers (we may take $\mathsf{M}(n)=O(n\log n)$ by [HvdH21]). Below, we analyze the complexity of Algorithm 1.

Proposition 5.4 (GRH)**.** *Assume GRH. Let $p > 3$ be a prime, and let E be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$. Let $\ell \in \{2, 3, 5\}$ and $d \in \{1, 2\}$. On input (E, ℓ, d), Algorithm 1 is correct and terminates in expected $O(\sqrt{p}(\log p)^2(\operatorname{llog} p)^3)$ time.*

Proof. First, we argue that Algorithm 1 is correct. Let $\alpha = \pi\widehat{\phi^{(p)}}\psi\phi$ with $\deg\phi = \ell^k$ be the output of Algorithm 1 on input (E, ℓ, d). We claim that α satisfies the hypotheses of Theorem 3.12. Because Algorithm 1 uses non-backtracking walks, the ℓ^k-isogeny ϕ is cyclic. Because the walk is truncated so that the final vertex is the first curve in the walk with a (d, ϵ)-structure, ϕ does not factor nontrivially through an isogeny to another curve with a (d, ϵ) structure. We conclude that α is an inseparable reflection.

We now bound the expected number of bit operations performed by the algorithm. We can do Step 1 with Newton's method, for example, and the resulting t will be in $O(\log p)$. We compute Φ_ℓ and Φ_2, if $d = 2$, and store these polynomials. Since we treat ℓ and d as constants, we ignore these costs, and in any case this computation can be done in $O(\ell^3 \log^3 \ell \operatorname{llog} \ell)$ expected time assuming GRH [BLS12, Theorem 1]. We can take one step in $G(p, \ell)$ using the modular polynomial Φ_ℓ. Let $E_0 = E$ and $j_0 = j(E_0)$. Suppose we are at vertex j_i. The neighbors of j_i are the roots of $\Phi_\ell(j_i, Y)$. We can evaluate $\Phi_\ell(X, Y)$ at (j_i, Y) in $O(\ell^2)$ many multiplications and additions in $\mathbb{F}_{p^2}$, the cost of which is dominated by the $O(\mathsf{M}(\ell \log p)(\operatorname{llog} p))$ bit operations needed to compute a random root of $\Phi_\ell(j_i, Y)$ using the randomized algorithm of [Rab80]. To take a non-backtracking step, we compute a random root of $\Phi_\ell(j_i, Y)/(Y - j_{i-1})$ where j_{i-1} is the previous vertex of the walk. Let X denote the set of supersingular j-invariants in $\mathbb{F}_{p^2}$ which are d-isogenous to their Galois conjugate. By Lemma 5.2, we can test if j_t is in S by testing whether $\Phi_d(j_t, j_t^p) = 0$ when $d > 1$ and simply whether $j_t^p = j_t$ when $d = 1$, both of which we can do with $O(\log p)$ multiplications in $\mathbb{F}_{p^2}$. Since the length of the walk is $O(\log p)$, and since we treat ℓ as a constant, Step 3 takes $O(\mathsf{M}(\log p)(\log p)(\operatorname{llog} p))$ time.

We now calculate the expected number of iterations of Step 3. Assuming GRH, by Proposition 5.3 a non-backtracking walk beginning at E lands in X with probability $\Omega\left(\frac{1}{\sqrt{p}\operatorname{llog} p}\right)$. Thus the expected number of non-backtracking walks we must take is $O(\sqrt{p}\operatorname{llog} p)$. Multiplying the expected number of walks by the expected number of bit operations per walk and using $\mathsf{M}(n) = O(n \log n)$ yields the cost

$$O(\mathsf{M}(\log p)(\log p)(\operatorname{llog} p) \cdot \sqrt{p}(\operatorname{llog} p)) = O(\sqrt{p}(\log p)^2(\operatorname{llog} p)^3).$$

Let $j_0 = j(E), j_1, \ldots, j_t$ be a sequence of adjacent j-invariants in $G(p, \ell)$ with $j_t \in X$. We next obtain the sequence of isogenies $\phi_i \colon E_i \to E_{i+1}$ for $i = 0, \ldots, t-1$ and the (d, ϵ)-structure (E_t, ψ) with $O((\log p)^{O(1)})$ bit operations: for example, if p is sufficiently large and if j_{i+1} is a simple root of $\Phi_\ell(j_i, Y)$ and given an equation for E_i with j-invariant j_i, we can compute a short Weierstrass equation for an elliptic curve E_{i+1} and a normalized ℓ-isogeny $\phi_i \colon E_i \to E_{i+1}$ with $O(\ell^2)$ operations in $\mathbb{F}_{p^2}$ using Elkies algorithm [Elk98] (see [Gal12, Algorithm 28] for an explicit description of the algorithm). The time to compute the sequence of isogenies associated to the path $j_0, \ldots, j_t$ is therefore dominated by the time required to complete the while-loop, since ℓ is a constant. Similarly, the time required to truncate the path and to compute the (d, ϵ)-structure is also dominated by the time required to complete the while-loop.

□

Remark 5.5. There are some natural optimizations which we do not explore here, such as testing more vertices along the path for the presence of (d, ϵ)-structures, or, more generally, testing whether a given curve E_k along the path is ℓ'-isogenous to a curve defined over $\mathbb{F}_p$ with the algorithm of [SCS22].

5.2 Computing a Bass suborder of $\mathrm{End}(E)$

Theorems 3.12 and 4.3 suggest the following approach to compute a Bass suborder of $\mathrm{End}(E)$: run Algorithm 1 twice, first on the input $(E, 3, 2)$ and then on the input $(E, 5, 2)$, to produce two inseparable reflections $\alpha_i = \pi\widehat{\phi_i^{(p)}}\psi_i\phi_i$ of E and the Bass order $\Lambda_{\alpha_1\alpha_2}$ generated by α_1 and α_2.

Theorem 5.6 (GRH)**.** *Assume GRH. On input a supersingular elliptic curve $E/\mathbb{F}_{p^2}$ and the primes $\ell_1 = 3$, $\ell_2 = 5$, and $d = 2$, Algorithm 2 is correct and terminates in expected $O(\sqrt{p}(\log p)^2(\operatorname{llog} p)^3)$ time.*

Algorithm 2: Compute a Bass order contained in $\mathrm{End}(E)$

Input: A supersingular elliptic curve $E/\mathbb{F}_{p^2}$ and three pairwise coprime integers ℓ_1, ℓ_2 and d, with d square-free and $-dp \not\equiv 1 \pmod 4$.

Output: A compact representation of a Bass order contained in $\mathrm{End}(E)$.

1 Use Algorithm 1 twice, on input respectively (E, ℓ_1, d) and (E, ℓ_2, d), to compute two inseparable reflections α_1, α_2 of E;

2 **return** $\Lambda = \langle 1, \alpha_1, \alpha_2, \alpha_1\alpha_2 \rangle$

Proof. By Proposition 5.4, the two endomorphisms constructed in Step 1 are inseparable reflections. Write $\alpha_i = \pi\widehat{\phi_i^{(p)}}\psi_i\phi_i$ where $\phi_i \colon E \to E_i$ is an isogeny of degree $\ell_i^{t_i}$. Since $\ell_1 \neq \ell_2$, the kernels of ϕ_1 and ϕ_2 are distinct. Therefore Theorem 3.12 implies Λ is an order in $\mathrm{End}(E)$, and Theorem 4.3 implies Λ is Bass. Thus, Algorithm 2 is correct. By Proposition 5.4, Step 1 terminates in expected $O(\sqrt{p}(\log p)^2(\operatorname{llog} p)^3)$ time. □

5.3 Computing $\mathrm{End}(E)$ from a Bass suborder

With an algorithm for computing a Bass order Λ in $\mathrm{End}(E)$, we obtain an algorithm for computing the endomorphism ring of E using the algorithms of [EHL+]. In Algorithm 3 below, we enumerate the maximal orders $\mathcal{O}' \supset \Lambda$ until finding an order isomorphic to $\mathrm{End}(E)$. We can efficiently check whether a given maximal order $\mathcal{O}'$ is isomorphic to $\mathrm{End}(E)$ using the algorithms and reductions in [EHL+18, Wes22]. Our main observation is that Algorithm 2, whose runtime is conditional only on GRH, can be used as a subroutine in an algorithm for computing $\mathrm{End}(E)$ with the same expected runtime. Thus, we remove all the heuristics needed for the correctness and the expected runtime of the algorithms of [EHL+], except for GRH. We sketch the algorithm here below and in its proof of correctness.

Algorithm 3: Compute End(E)

Input: A supersingular elliptic curve $E/\mathbb{F}_{p^2}$.

Output: A maximal order $\mathcal{O} \subseteq B_{p,\infty}$ isomorphic to $\mathrm{End}(E)$.

1 Run Algorithm 2 on input $(E, 3, 5, 2)$ to compute a Bass order Λ contained in $\mathrm{End}(E)$;

2 Compute an isomorphism $f \colon \Lambda \otimes \mathbb{Q} \to B_{p,\infty}$;

3 Enumerate the maximal orders $\mathcal{O}'$ such that $f(\Lambda) \subseteq \mathcal{O}' \subseteq B_{p,\infty}$, until $\mathcal{O}' \simeq \mathrm{End}(E)$;

4 **return** $\mathcal{O}'$

Theorem 5.7 (GRH)**.** *Assume GRH. Algorithm 3 is correct and terminates in expected* $O(\sqrt{p}(\log p)^2(\operatorname{llog} p)^3)$ *time.*

Proof. By Theorem 5.6, Step 1 runs in expected time $O(\sqrt{p}(\log p)^2(\operatorname{llog} p)^3)$. Moreover, Λ is Bass. We now discuss Step 2. First, compute the Gram matrix G under the trace pairing of the basis $1, \alpha_1, \alpha_2, \alpha_1\alpha_2$ for Λ: by the discussion in Section 4, we need to compute a single trace, namely $\mathrm{tr}(-\alpha_1\alpha_2/p)$. This trace can be computed in time polynomial in $\log p$ with a generalization of Schoof's algorithm [Koh96, BCNE+19], since $\alpha_1\alpha_2/p$ is a cyclic isogeny of degree $2^2 3^{2t_3} 5^{2t_5}$ and $t_3, t_5 = O(\log p)$. With G, compute $a, b \in \mathbb{Q}^\times$ such that $\Lambda \otimes \mathbb{Q}$ is isomorphic to $H(a, b)$ with the Gram-Schmidt process. We now identify Λ with its image in $H(a, b)$.

We factor $\mathrm{disc}(\alpha_1\alpha_2)$ to obtain a factorization of $\mathrm{discrd}(\Lambda) = p^2 |\mathrm{disc}(\alpha_1\alpha_2)|$. Since $\alpha_1\alpha_2$ is the product of $2 + 2t_3 + 2t_5 = O(\log p)$ isogenies of degree at most 5, the degree of $\alpha_1\alpha_2$ is $O(p^C)$ for some C. This implies $-\mathrm{disc}(\alpha_1\alpha_2) = O(p^C)$ as well, since $-\mathrm{disc}(\alpha_1\alpha_2) \leq 4 \deg \alpha_1\alpha_2$. Therefore we can factor $\mathrm{disc}(\alpha_1\alpha_2)$ in time subexponential in $\log p$ [LP92, Theorem 1]. Having factored $\mathrm{discrd}(\Lambda)$, we can compute a maximal order $\mathcal{O}$ in $H(a, b)$ in polynomial time [Voi13, Algorithms 7.9, 7.10; Theorem 7.14]. Next, we compute a supersingular elliptic curve E_0 and an order $\mathcal{O}_0 \subseteq B_{p,\infty}$ isomorphic to $\mathrm{End}(E_0)$, which can be done efficiently, assuming GRH [EHL+18, Proposition 3]. Finally, with $\mathcal{O} \subseteq H(a, b)$ and $\mathcal{O}_0 \subseteq B_{p,\infty}$, we can compute an isomorphism $H(a, b) \to B_{p,\infty}$ of quaternion algebras in time polynomial in $\log p$ [CKMZ22, Proposition 4.1].

We let $f\colon \Lambda \otimes \mathbb{Q} \to B_{p,\infty}$ be the composition

$$\Lambda \otimes \mathbb{Q} \to H(a,b) \to B_{p,\infty}.$$

We now outline how to do Step 3. For each $q \mid \operatorname{discrd}(\Lambda)$ such that $q \neq p$, we can enumerate maximal $\mathbb{Z}_q$-orders containing $f(\Lambda) \otimes \mathbb{Z}_q$ efficiently using Algorithm 4.3 of [EHL$^+$] and then enumerate the $\mathbb{Z}$-orders containing $f(\Lambda)$; see Steps 1(a) and 3(a) in Algorithm 5.4 of [EHL$^+$]. For each maximal order $\mathcal{O}'$ containing $f(\Lambda)$, compute an elliptic curve E' with $\operatorname{End}(E') \simeq \mathcal{O}'$. This can be done in polynomial time in $\log p$: first, compute a connecting ideal J between $\mathcal{O}_0$ and $\mathcal{O}'$. By Theorem 6.4 of [Wes22], assuming GRH, we can, in expected polynomial time, compute an equivalent ideal I to J such that the norm of I is B-powersmooth for some $B = O((\log p)^c)$ for some constant c. Since the norm of I is B-powersmooth, we can efficiently compute the corresponding isogeny $\phi_I\colon E_0 \to E'$. The codomain E' of ϕ_I is a curve whose endomorphism ring is isomorphic to $\mathcal{O}'$, since $\operatorname{End}(E') \simeq \mathcal{O}_R(I) \simeq \mathcal{O}_R(J) = \mathcal{O}'$. If $j(E') \in \{j(E), j(E)^p\}$, we return $\mathcal{O}'$. Thus the algorithm is correct.

By Proposition 4.2 of [EHL$^+$], the number of maximal overorders of $f(\Lambda)$ is bounded by

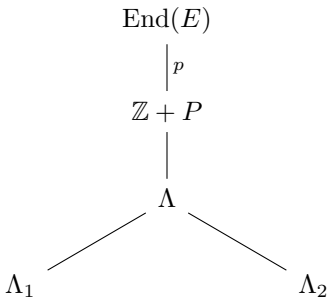
$$\prod_{\substack{q \mid \operatorname{disc}(\rho) \\ q \neq p}} v_q(\operatorname{disc}(\rho)) + 1,$$

the number of divisors of $\operatorname{disc}(\rho)/p^{v_p(\operatorname{disc}(\rho))}$. The number of divisors of an integer n is $O(n^\epsilon)$ for every $\epsilon > 0$ [HW08, Theorem 315]. We conclude that Step 3 takes $O(p^\epsilon)$ time for any $\epsilon > 0$. In particular, the expected time required to complete Step 3 is dominated by the expected time required to complete Step 1. □

6 The expected number of inseparable reflections in a generating set for $\mathbb{Z} + P$

Let E be a supersingular elliptic curve E over $\mathbb{F}_{p^2}$. Let $P \coloneqq \pi \operatorname{Hom}(E, E^{(p)}) \subseteq \operatorname{End}(E)$ be the ideal of inseparable endomorphisms of E. By Theorem 4.3, with two calls to Algorithm 1 we compute a generating set for a Bass order Λ contained in $\mathbb{Z} + P$. One could proceed to compute $\operatorname{End}(E)$ by enumerating maximal orders of Λ, as in Algorithm 3. A simpler strategy is to compute additional inseparable reflections with Algorithm 1 until finding a generating set for $\mathbb{Z} + P$ and then compute a basis for a maximal order containing $\mathbb{Z} + P$ using the algorithms of [Voi13]. The maximal order containing $\mathbb{Z} + P$ is $\operatorname{End}(E)$, by Proposition 3.1. A natural question is whether we can bound the number of calls to Algorithm 1 before producing enough endomorphisms to generate $\mathbb{Z} + P$. We do not prove a bound here, leaving this to future work. Instead, we introduce a heuristic which implies that the expected number of calls is bounded by a constant independent of p and of E.

Suppose we run Algorithm 2 twice on input a supersingular elliptic curve E over $\mathbb{F}_{p^2}$, producing two (not necessarily Bass) orders Λ_1, Λ_2 in $\operatorname{End}(E)$ generated respectively by $1, \alpha_1, \alpha_2, \alpha_1\alpha_2$ and $1, \alpha_3, \alpha_4, \alpha_3\alpha_4$, where α_i is an inseparable reflection for every $i = 1, \ldots, 4$. Let Λ be the order in $\operatorname{End}(E)$ generated by the bases of Λ_1 and Λ_2,



then $\mathrm{discrd}(\Lambda) = \mathrm{discrd}(\mathbb{Z}+P)\cdot[\mathbb{Z}+P:\Lambda] = p^2\cdot[\mathbb{Z}+P:\Lambda]$, and $\mathrm{discrd}(\Lambda)$ divides both $\mathrm{discrd}(\Lambda_1) = p^2|\operatorname{disc}(\rho_1)|$ and $\mathrm{discrd}(\Lambda_2) = p^2|\operatorname{disc}(\rho_2)|$, where $\rho_1 = \frac{\alpha_1\alpha_2}{p}$ and $\rho_2 = \frac{\alpha_3\alpha_4}{p}$. In particular, $[\mathbb{Z}+P:\Lambda] = \frac{\mathrm{discrd}(\Lambda)}{p^2}$ divides $\gcd(\operatorname{disc}(\rho_1),\operatorname{disc}(\rho_2))$. If the distributions of the integers $\operatorname{disc}(\rho_1)$ and $\operatorname{disc}(\rho_2)$ follow the same distribution as two random integers, then $\operatorname{disc}(\rho_1)$ and $\operatorname{disc}(\rho_2)$ are coprime with probability $6/\pi^2$. Assuming this, four calls to Algorithm 1 produce a generating set for $\mathbb{Z}+P$ with *at least* $6/\pi^2 \approx 0.6$ probability.

Unfortunately, the integers $D_i = \operatorname{disc}(\rho_i)$ are not distributed like random integers. First of all, the integer D_i is a discriminant, which imposes congruency conditions on D_i. Second, the prime p is not split in $\mathbb{Z}[\rho_i]$, imposing another congruence condition. Finally, because ρ_i is an endomorphism of smooth degree, this enforces relations in the ideal class group of $\mathbb{Z}[\rho_i]$. In any case, the following heuristic suffices:

Heuristic 6.1. The discriminants of the outputs of Algorithm 1 on input $(E/\mathbb{F}_{p^2}, \ell, 1)$ are coprime with probability which is bounded from below by a constant, independent of p.

The following theorem follows from the above discussion:

Theorem 6.2. *Assume Heuristic 6.1. Let $p \neq \ell$ be primes, and let E be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$. Then the expected number of calls to Algorithm 1 on input $(E, \ell, 1)$ in order to produce a generating set for $\mathbb{Z}+P$ is bounded from above by a constant, independent of p.*

Heuristic 6.1 is [EHL$^+$, Heuristic 5.2] which is assumed in [EHL$^+$18, Theorem 5.3] to prove that [EHL$^+$, Algorithm 5.1] produces a Bass order in $\mathrm{End}(E)$ and terminates in expected $O(p^{1/2+\epsilon})$ time. We use the heuristic in a new way. In forthcoming work, we will discuss experimental evidence for this heuristic along with details of an implementation of an algorithm for computing $\mathrm{End}(E)$. We first compute a few inseparable reflections with Algorithm 1 until obtaining a generating set for $\mathbb{Z}+P$. Then, we can recover $\mathrm{End}(E)$ from $\mathbb{Z}+P$ as $\mathrm{End}(E)$ is the *radical idealizer* of $\mathbb{Z}+P$, i.e. the order $\mathcal{O}_L(\mathrm{rad}(\mathbb{Z}+P))$ where $\mathrm{rad}(\mathcal{O})$ is the Jacobson radical of an order $\mathcal{O}$. More simply, we can apply [Voi13, Algorithms 7.9, 7.10; Theorem 7.14] to recover a basis for $\mathrm{End}(E)$ from a basis for $\mathbb{Z}+P$.

References

[ACNL$^+$23] Sarah Arpin, Catalina Camacho-Navarro, Kristin Lauter, Joelle Lim, Kristina Nelson, Travis Scholl, and Jana Sotáková. Adventures in supersingularland. *Experimental Mathematics*, 32(2):241–268, 2023.

[BCC$^+$23] Andrea Basso, Giulio Codogni, Deirdre Connolly, Luca De Feo, Tako Boris Fouotsa, Guido Maria Lido, Travis Morrison, Lorenz Panny, Sikhar Patranabis, and Benjamin Wesolowski. Supersingular curves you can trust. In *Advances in Cryptology – EUROCRYPT 2023: 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23–27, 2023, Proceedings, Part II*, page 405–437, Berlin, Heidelberg, 2023. Springer-Verlag.

[BCNE$^+$19] Efrat Bank, Catalina Camacho-Navarro, Kirsten Eisenträger, Travis Morrison, and Jennifer Park. Cycles in the supersingular ℓ-isogeny graph and corresponding endomorphisms. In Jennifer S. Balakrishnan, Amanda Folsom, Matilde Lalín, and Michelle Manes, editors, *Research Directions in Number Theory*, pages 41–66, Cham, 2019. Springer International Publishing.

[BLS12] Reinier Bröker, Kristin Lauter, and Andrew V. Sutherland. Modular polynomials via isogeny volcanoes. *Math. Comp.*, 81(278):1201–1231, 2012.

[Brz90] J. Brzezinski. On automorphisms of quaternion orders. *J. Reine Angew. Math.*, 403:166–186, 1990.

[BS11] Gaetan Bisson and Andrew V. Sutherland. Computing the endomorphism ring of an ordinary elliptic curve over a finite field. *J. Number Theory*, 131(5):815–831, 2011.

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

[CKMZ22] Tímea Csahók, Péter Kutas, Mickaël Montessinos, and Gergely Zábrádi. Explicit isomorphisms of quaternion algebras over quadratic global fields. *Res. Number Theory*, 8(4):Paper No. 77, 24, 2022.

[CS21] Mathilde Chenu and Benjamin Smith. Higher-degree supersingular group actions. *Mathematical Cryptology*, 2021.

[CSV21] Sara Chari, Daniel Smertnig, and John Voight. On basic and Bass quaternion orders. *Proc. Amer. Math. Soc. Ser. B*, 8:11–26, 2021.

[EHL$^+$] Kirsten Eisenträger, Sean Hallgren, Chris Leonardi, Travis Morrison, and Jennifer Park. Computing endomorphism rings of supersingular elliptic curves and connections to path-finding in isogeny graphs. *Proceedings of the Fourteenth Algorithmic Number Theory Symposium*, pages 215–232.

[EHL$^+$18] Kirsten Eisenträger, Sean Hallgren, Kristin Lauter, Travis Morrison, and Christophe Petit. Supersingular isogeny graphs and endomorphism rings: Reductions and solutions. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2018*, pages 329–368, Cham, 2018. Springer International Publishing.

[Eic36] Martin Eichler. Untersuchungen in der Zahlentheorie der rationalen Quaternionenalgebren. *J. Reine Angew. Math.*, 174:129–159, 1936.

[Elk98] Noam D. Elkies. Elliptic and modular curves over finite fields and related computational issues. In *Computational perspectives on number theory (Chicago, IL, 1995)*, volume 7 of *AMS/IP Stud. Adv. Math.*, pages 21–76. Amer. Math. Soc., Providence, RI, 1998.

[Gal12] Steven D. Galbraith. *Mathematics of public key cryptography.* Cambridge University Press, Cambridge, 2012.

[GPS17] Steven D. Galbraith, Christophe Petit, and Javier Silva. Identification protocols and signature schemes based on supersingular isogeny problems. In *Advances in cryptology—ASIACRYPT 2017. Part I*, volume 10624 of *Lecture Notes in Comput. Sci.*, pages 3–33. Springer, 2017.

[HvdH21] David Harvey and Joris van der Hoeven. Integer multiplication in time $O(n \log n)$. *Ann. of Math. (2)*, 193(2):563–617, 2021.

[HW08] Godfrey H. Hardy and Edward M. Wright. *An introduction to the theory of numbers.* Oxford University Press, Oxford, sixth edition, 2008.

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

[Lit28] John E. Littlewood. On the class-number of the corpus $P(\sqrt{-k})$. *Proc. London Math. Soc. (2)*, 27(5):358–372, 1928.

[LP92] H. W. Lenstra, Jr. and Carl Pomerance. A rigorous time bound for factoring integers. *J. Amer. Math. Soc.*, 5(3):483–516, 1992.

[Piz80] Arnold Pizer. Theta series and modular forms of level p^2M. *Compositio Math.*, 40(2):177–241, 1980.

[Rab80] Michael O. Rabin. Probabilistic algorithms in finite fields. *SIAM J. Comput.*, 9(2):273–280, 1980.

[SCS22] Maria Corte-Real Santos, Craig Costello, and Jia Shi. Accelerating the delfs-galbraith algorithm with fast subfield root detection. In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part III*, volume 13509 of *Lecture Notes in Computer Science*, pages 285–314. Springer, 2022.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*. Springer, New York, 2009.

[Voi13] John Voight. Identifying the matrix ring: algorithms for quaternion algebras and quadratic forms. *Developments in Mathematics*, 31:255–298, 2013.

[Voi21] John Voight. *Quaternion algebras*, volume 288 of *Graduate Texts in Mathematics*. Springer, Cham, 2021.

[Wes22] Benjamin Wesolowski. The supersingular isogeny path and endomorphism ring problems are equivalent. In *FOCS 2021 - 62nd Annual IEEE Symposium on Foundations of Computer Science*, Denver, Colorado, United States, February 2022.