PARAMETRIZING MAXIMAL ORDERS ALONG SUPERSINGULAR ℓ-ISOGENY PATHS

LAIA AMORÓS, JAMES CLEMENTS, AND CHLOE MARTINDALE

Abstract. Suppose you have a supersingular ℓ-isogeny graph with vertices given by j-invariants defined over $\mathbb{F}_{p^2}$, where $p = 4 \cdot f \cdot \ell^e - 1$ and $\ell \equiv 3 \pmod 4$. We give an explicit parametrization of the maximal orders in $B_{p,\infty}$ appearing as endomorphism rings of the elliptic curves in this graph that are $\leq e$ steps away from a root vertex with j-invariant 1728. This is the first explicit parametrization of this kind and we believe it will be an aid in better understanding the structure of supersingular ℓ-isogeny graphs that are widely used in cryptography. Our method makes use of the inherent directions in the supersingular isogeny graph induced via Bruhat-Tits trees, as studied in [1]. We also discuss how in future work other interesting use cases, such as $\ell = 2$, could benefit from the same methodology.

1. Introduction

For a large prime p and a small prime ℓ, the graphs of supersingular elliptic curves over $\mathbb{F}_{p^2}$ with vertices defined up to isomorphism and edges corresponding to ℓ-isogenies are optimal expander graphs, making them well suited for cryptography. The endomorphism ring of a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$ is a maximal order in the unique quaternion algebra $B_{p,\infty}$ ramified at p and ∞; via the Deuring correspondence [10] we see that the same graphs arise from ideals of norm ℓ between conjugacy classes of maximal orders in $B_{p,\infty}$. This correspondence lies at the heart of *isogeny-based cryptography*: The Endomorphism Ring problem, that is, computing the endomorphism ring of a given supersingular elliptic curve, is a hard problem on which the security of every major isogeny-based cryptographic scheme relies [27]. See for example SQISign [9], the only isogeny-based submission to the US National Institute for Standards in Technology (NIST) Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process [19], which relies very naturally on The Endomorphism Ring problem, or CSIDH [6], which was shown to be also solvable via the Endomorphism Ring Problem [26]. This relationship is fundamentally due to the fact that problems which are believed to be hard for elliptic curves, such as the Isogeny Path Problem, often translate into much easier problems for maximal orders, which can be solved with tools such as the 'KLPT algorithm' [17].

The more therefore that we know about the graph of maximal quaternion orders connected by ideals of norm ℓ, the more we learn about supersingular ℓ-isogeny graphs, both in terms of interrogating the robustness of the security of the aforementioned protocols and in terms of potential tricks to speed up implementations. For

Date: January 8, 2025.

Key words and phrases. public-key cryptography, elliptic curve, isogeny, endomorphism ring, quaternion.

this reason, in this work we consider the problem of giving an explicit parametrization of the maximal quaternion orders related to their position in this graph. Our main theorem, Theorem 3.1, gives an explicit parametrization for an interesting case in cryptography: $\ell \equiv 3 \pmod 4$, $p = 4 \cdot f \cdot \ell^e - 1 \equiv 3 \pmod 4$, and each maximal order parametrized in relation to its distance ($\leq e$) in the ℓ-ideal graph from $\mathcal{O}_{1728}$, the order isomorphic to the endomorphism ring of an elliptic curve with j-invariant 1728. Note that this does *not* parametrize every maximal order in the graph, only those close enough to the 'root' $\mathcal{O}_{1728}$, or in other words only those reachable by a short ℓ-isogeny walk such as those used in isogeny-based cryptography schemes.[1] In every major isogeny-based cryptographic primitive, the curve of j-invariant 1728 has a special role, which is the reason for this choice of root. The shapes of p and ℓ are primarily motivated by lending themselves to our methodology, although such p (with small f) are certainly also common among isogeny-based schemes as this lends itself to efficient elliptic curve arithmetic.[2] The choice of odd ℓ is less natural from a cryptographic perspective; although our methods should also work in the case of $\ell = 2$ (see Section 5.2) the formulae are more complex and quite different so we considered this to be out of scope.

To achieve our parametrization we use the theory of Bruhat-Tits trees and their links to isogeny graphs motivated by [1]. Ribet's correspondence [22], made explicit by Franc and Masdeu [13], allows us to see Bruhat-Tits trees, which are $(\ell + 1)$-regular infinite trees whose vertices are 2×2 matrices in $\mathrm{PGL}_2(\mathbb{Q}_\ell)$, as an infinite cover of the supersingular ℓ-isogeny graph. This covering gives a natural way of assigning directions to the edges in relation to the choices made at the root vertex: which elliptic curve E to map to the root (we choose $j(E) = 1728$) and a basis of $T_\ell(E)$. Our parametrization is in terms of these directions.

Additionally, by parametrizing the bases of maximal quaternion orders, we also parametrize their norm forms. This may present some interesting applications. Many efforts in the cryptanalysis of isogeny-based schemes have led to attempts at solving certain norm equations (for example [20, 21, 3]). A parametrization of all or most norm forms could for example give rise to new curves with easy-to-solve norm equations, or to ways of solving multiple norm equations in parallel. In particular, the solving of norm forms is of relevance to the version of the KLPT algorithm used in SQISign [9], which is used to find an (ideally short) ℓ-ideal path between two maximal orders $\mathcal{O}_1$, $\mathcal{O}_2$ in $B_{p,\infty}$. The algorithm currently used in SQISign finds an ℓ-ideal path, but it is far from optimally short. We leave for future work the question of whether or not our parametrization of all norm forms at a given distance can aid in finding an optimally short path for this subroutine; see Section 5.3 for discussion on this.

We structure this paper as follows. Section 2 provides preliminaries, defining how to translate level-increasing paths in Bruhat-Tits trees to paths of quaternion orders and supersingular elliptic curves. Section 3 gives the main theorem and its proof. Section 4 gives a simplification of the main theorem for a special subcase. Section 5 discusses some directions for future work.

---

[1] This is something of a shortfall, though: The maximal orders that are further than e steps in the ℓ-ideal graph from $\mathcal{O}_{1728}$ could be reached by a short walk in an ℓ'-graph, for example. We hope in future work to extend Theorem 3.1 to paths of arbitrary length.

[2] This makes it possible to choose $\mathbb{F}_p$- or $\mathbb{F}_{p^2}$-rational ℓ-torsion points to generate the kernel of the ℓ-isogenies.

We use SageMath [23] to provide correctness checks of some calculations for easy verification. When used, we state the file name, with files available online at: `https://github.com/quaternion-graph-parametrizations/proofs`.

Acknowledgements. We thank Annamaria Iezzi and Jana Sotáková for their contributions during the earlier stages of research, especially during a research visit funded by the Returning Carer's Scheme at the University of Bristol. Thank you also to Ross Bowden for useful discussions on the topic of Bruhat-Tits trees. This work was funded in part by the UK Engineering and Physical Sciences Research Council (EPSRC). James Clements is funded by EPSRC grant number EP/S022465/1.

2. Preliminaries

Our explicit parametrization relies on several non-canonical but well-motivated choices, although the methods in this paper could in principle be used (with non-trivial effort) to find a parametrization for other useful scenarios. These choices, following [1], come from exploiting the explicit connections between three categories (all relying on a large[3] prime p and a small[4] prime ℓ):

(1) Supersingular elliptic curves defined over a finite field $\mathbb{F}_{p^2}$, defined up to $\overline{\mathbb{F}}_p$-isomorphism, and ℓ-isogenies between these curves, defined up to post-composition with automorphisms; see Section 2.1.
(2) Maximal orders in the quaternion algebra $B_{p,\infty}$ ramified at p and infinity, defined up to conjugation, and the left-ideals of norm ℓ connecting them; see Section 2.2.
(3) The graph of the special fibre at ℓ of the Shimura curve $X(p\ell)$ of discriminant $p\ell$; if the reader is unfamiliar with this terminology it is not a problem as we give an explicit description of our case in Definition 2.12. Suffice it to say for now that the vertices are classes of explicit 2×2 ℓ-adic matrices, and the edges amount to simple matrix multiplication; see Section 2.3.

2.1. Supersingular isogeny graph.

Let ℓ and p be prime numbers with $\ell \neq p$.

Definition 2.1. *We define the* supersingular ℓ-isogeny graph $\mathcal{G}_{p,\ell}$ *to be the finite undirected graph that has as:*

- ***Vertices****: Each vertex represents a j-invariant of a supersingular elliptic curves defined over $\mathbb{F}_{p^2}$.*
- ***Edges****: Each edge $(j(E), j(E'))$ represents an ℓ-isogeny $E \to E'$ and its dual. Edges are identified up to post-composition with automorphisms.*

This graph is $(\ell+1)$-regular at every vertex except for vertices with automorphisms of degree ℓ and is connected. The properties of this graph have been extensively studied elsewhere in the literature, see for example [2].

2.2. Quaternion order graph.

The interested reader can find hundreds of pages of details on the joys of quaternions by reading [25]. Here we include only the facts that are strictly necessary to this paper. Let ℓ and p be prime numbers with $\ell \neq p$. We specifically work in the case $p \equiv 3 \mod 4$.

[3]Cryptographic size; typically at least 512 bits.
[4]Generally speaking of size at most polynomial in $\log(p)$.

Definition 2.2. *The* quaternion algebra $B_{p,\infty}$ *ramified at* $p \equiv 3 \mod 4$ *and* ∞ *is the 4-dimensional* $\mathbb{Q}$*-algebra*

$$B_{p,\infty} = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$$

such that $i^2 = -1$, $j^2 = -p$, *and* $ij = -ji = k$. *The* conjugate *of*

$$\alpha = a + bi + cj + dk \in B_{p,\infty},$$

where $a, b, c, d \in \mathbb{Q}$, *is defined to be*

$$\overline{\alpha} = a - bi - cj - dk.$$

The reduced norm *and* reduced trace *of* α *are defined to be*

$$\mathrm{nrd}(\alpha) = \alpha\overline{\alpha}$$

and

$$\mathrm{tr}(\alpha) = \alpha + \overline{\alpha}$$

respectively.

Definition 2.3. *An* ideal $I \subseteq B_{p,\infty}$ *is a* $\mathbb{Z}$*-lattice of rank 4. An* order $\mathcal{O}$ *of* $B_{p,\infty}$ *is an ideal that is also a subring of* $B_{p,\infty}$. *We say that* $\mathcal{O}$ *is* maximal *if it is not properly contained in any other order.*

We use the following form to express the bases of quaternion orders and ideals.

Definition 2.4. *Given a* $\mathbb{Z}$*-lattice* L *which is the span of* $b_1, ..., b_n \in B_{p,\infty}$ *we may describe* L *as a* $4 \times n$ *matrix where the* r*th column denotes a vector whose entries are* b_r*'s coefficients of* $1, i, j$ *and* k, *that is*

$$b_r = w + xi + yj + zk \mapsto \begin{pmatrix} w \\ x \\ y \\ z \end{pmatrix}.$$

For bases of orders and ideals these are 4×4 *matrices.*

Unlike number fields, quaternion algebras have infinitely many maximal orders, although in $B_{p,\infty}$ there are only finitely many up to isomorphism. An isomorphism in this context is a conjugation, i.e., the maximal orders $\mathcal{O}$ and $\mathcal{O}'$ are isomorphic if there exists $\alpha \in B_{p,\infty}$ such that $\alpha^{-1}\mathcal{O}\alpha = \mathcal{O}'$.

Definition 2.5. *A* left-ideal I *of a maximal order* $\mathcal{O}$ *in* $B_{p,\infty}$ *is an ideal* I *such that* $\mathcal{O}I \subseteq I$. *Two left-ideals* I *and* I' *are* equivalent *if there exists* $\alpha \in B_{p,\infty}^{\times}$ *such that* $I = I'\alpha$. *The* reduced norm $\mathrm{nrd}(I)$ *of* I *is*

$$\gcd\{\mathrm{nrd}(\alpha) : \alpha \in I\}.$$

Definition 2.6. *Let* I *be a left-ideal of a maximal order* $\mathcal{O}$ *in* $B_{p,\infty}$. *The* right-order *of* I *is*

$$\mathcal{O}_r(I) = \{x \in B_{p,\infty} : Ix \subseteq I\}.$$

We say that I connects $\mathcal{O}$ *to* $\mathcal{O}_r(I)$*; it is also referred to as a* connecting ideal.

Definition 2.7. *Let* ℓ, p, *and* $B_{p,\infty}$ *be as above. We define the* ℓ-ideal graph of $B_{p,\infty}$ *to be the finite undirected graph that has as:*

- ***Vertices****: Each vertex represents a maximal order of* $B_{p,\infty}$ *up to conjugation.*

- ***Edges**: Each edge $(\mathcal{O}, \mathcal{O}')$ represents a left-ideal I of $\mathcal{O}$ of reduced norm ℓ such that $\mathcal{O}' = \mathcal{O}_r(I)$ and its conjugate, a left-ideal I' of $\mathcal{O}'$ of reduced norm ℓ such that $\mathcal{O} = \mathcal{O}_r(I')$. Edges are identified up to equivalence.*

This graph is related to the supersingular isogeny graph of Section 2.1 via the *Deuring correspondence* [10]. Explicitly, the endomorphism ring of each supersingular elliptic curve defined over $\mathbb{F}_{p^2}$ is a maximal order in $B_{p,\infty}$, and furthermore for each maximal order $\mathcal{O}$, there exists either:

(a) a unique supersingular j-invariant defined over $\mathbb{F}_p$, or
(b) a unique p-Frobenius-conjugate pair of supersingular j-invariants defined over $\mathbb{F}_{p^2}$

whose endomorphism ring is isomorphic to $\mathcal{O}$.

2.3. **A special quotient of the Bruhat-Tits tree.** Let ℓ be a small odd[5] prime, and let p be a prime such that $\ell \mid (p+1)$.

Remark 2.8. *In isogeny-based cryptography, we are typically starting with supersingular elliptic curves E defined over $\mathbb{F}_p$, where p has been chosen so that $\#E(\mathbb{F}_p) = p+1$ is smooth (perhaps divisible by ℓ^n for n large, or by many small ℓ). This is to minimize the amount of computation performed in extension fields when computing isogenies.*

Definition 2.9. *The* Bruhat-Tits tree associated to $\mathrm{PGL}_2(\mathbb{Q}_\ell)$ *is an infinite tree which has as:*

- ***Vertices**: Each vertex is an element of $\mathrm{PGL}_2(\mathbb{Q}_\ell)/\mathrm{PGL}_2(\mathbb{Z}_\ell)$.*
- ***Edges**: There exists an edge $([M], [M'])$ when there exist representatives M and M' of the equivalence classes $[M]$ and $[M']$ respectively for which $\ell M \subsetneq M' \subsetneq M$.*

We say a walk in the infinite tree is *level-increasing* if each step descends the tree, getting further from the root.

By convention, this tree has $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ at the root. It is an $(\ell+1)$-regular tree which is an infinite cover of the supersingular isogeny graph of Section 2.1, as we will see explicitly below. Following [1][6], we label an edge $([M], [M'])$ by a matrix D such that $DM = M'$, and furthermore if the representatives of the classes $[M]$ and $[M']$ are chosen in the right way, then the choices for D at any given vertex are

$$D_i = \begin{pmatrix} 1 & 0 \\ i & \ell \end{pmatrix}, \text{ where } i = 0, \ldots, \ell-1, \text{ or } D_\infty = \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}.$$

This simple description of edges, and the resulting simple explicit description of edges as matrices, lends itself to aid in parametrizing the quaternion order graph and the supersingular isogeny graph. First we need to have an explicit description of how to take the quotient of this tree that gives the aforementioned 'graph of the special fibre at ℓ of the Shimura curve $X(p\ell)$ of discriminant $p\ell$'; for this we need to construct a matrix subgroup of $\mathrm{PGL}_2(\mathbb{Q}_\ell)/\mathrm{PGL}_2(\mathbb{Z}_\ell)$ which depends on $B_{p,\infty}$. The abstract correspondence was proven by Ribet [22], and Franc and Masdeu

[5] $\ell = 2$ presents some challenges in the explicit computation of these graphs, which we considered to be out-of-scope. See Section 5.2.

[6] We adopt a slightly different choice of notation than in [1] to avoid difficulties in the parametrizataion we derive.

gave the first computationally explicit methodology for this [13, 12]. We give here the explicit description for only our case of interest, which is a special case of the formulae of Franc and Masdeu; the explicit description depends on arbitrary choices made for the root of the tree, as well as some properties of p and ℓ.

If $p \equiv 3 \pmod 4$, then an elliptic curve $E_{1728}/\mathbb{F}_p$ of j-invariant 1728 is always supersingular [24]. We will choose this as the root of our Bruhat-Tits tree, as is also justified by its special role in isogeny-based cryptographic protocols such as SQISign [9], CSIDH [6], and M-SIDH [11]. The endomorphism ring of E_{1728} is given by $\mathcal{O}_{1728} \cong \mathrm{End}(E_{1728})$ where

$$\mathcal{O}_{1728} := \frac{1+k}{2}\mathbb{Z} + \frac{i+j}{2}\mathbb{Z} + j\mathbb{Z} + k\mathbb{Z} \subset B_{p,\infty}.$$

Lemma 2.10. *Let $\ell \neq 2$ be a prime dividing $p+1$. Then there is an embedding $\Phi_\ell : B_{p,\infty} \hookrightarrow M_2(\mathbb{Q}_\ell)$ defined by*

$$\begin{array}{rcc} B_{p,\infty} & \hookrightarrow & M_2(\mathbb{Q}_\ell) \\ 1 & \mapsto & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ i & \mapsto & \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \\ j & \mapsto & \begin{pmatrix} \sqrt{-p} & 0 \\ 0 & -\sqrt{-p} \end{pmatrix} \\ k & \mapsto & \begin{pmatrix} 0 & -\sqrt{-p} \\ -\sqrt{-p} & 0 \end{pmatrix}, \end{array}$$

and the image of $\mathcal{O}_{1728}$ under Φ_ℓ is $M_2(\mathbb{Z}_\ell)$.

Proof. This formula comes from applying the source code written by Franc and Masdeu [12] to our special case. However proving correctness for only this simple case is much more straightforward than the general case considered in their accompanying paper [13], so we re-prove it here.

First, note that as $\ell \mid (p+1)$, we have that $-p$ is a square mod ℓ, which implies by Hensel's lemma that $\sqrt{-p} \in \mathbb{Z}_\ell$, so Φ_ℓ is well-defined. Second, note that $\Phi_\ell(i)^2 = -I_2$, $\Phi_\ell(j)^2 = -pI_2$, and $\Phi_\ell(i)\Phi_\ell(j) = -\Phi_\ell(j)\Phi_\ell(i) = \Phi_\ell(k)$, so multiplication is preserved.

Now, as $\ell \neq 2$, the images of $(1+k)/2$, $(i+j)/2$, j, and k are all in $M_2(\mathbb{Z}_\ell)$. To see that these images generate a basis for the whole of $M_2(\mathbb{Z}_\ell)$, we map $M_2(\mathbb{Z}_\ell)$ to $(\mathbb{Z}_\ell)^4$ via the natural map

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix},$$

via which the basis matrix of the 4-dimensional $\mathbb{Z}_\ell^4$-algebra resulting from the images under Φ_ℓ of $(1+k)/2$, $(i+j)/2$, j, and k is

$$\begin{pmatrix} 1/2 & \sqrt{-p}/2 & \sqrt{-p} & 0 \\ -\sqrt{-p}/2 & -1/2 & 0 & -\sqrt{-p} \\ -\sqrt{-p}/2 & 1/2 & 0 & -\sqrt{-p} \\ 1/2 & -\sqrt{-p}/2 & -\sqrt{-p} & 0 \end{pmatrix},$$

the determinant of which is $-p \in (\mathbb{Z}_\ell)^\times$. □

Definition 2.11. *We can now define the matrix group by which we quotient the Bruhat-Tits tree. It is given by*

$$\Gamma_{\ell,+} := \Phi_\ell(\{\alpha \in \mathcal{O}_{1728}[1/\ell]^\times \,|\, \mathrm{nrd}(\alpha) = \ell^{2n}, \text{ for } n \in \mathbb{Z}\})/\mathbb{Z}[1/\ell]^\times.$$

Alternatively, this gives us an explicit description of the graph of the special fibre at ℓ of the Shimura curve $X(p\ell)$ of discriminant $p\ell$ as follows:

Definition 2.12. *Let $\ell \neq 2$ be a prime dividing $p+1$ and let Φ_ℓ be the map defined in Lemma 2.10. We define the* graph of the special fibre at ℓ of the Shimura curve $X(p\ell)$ of discriminant $p\ell$ *to be the finite graph which has as:*

- ***Vertices**: Each vertex is an element of*

$$\Phi_\ell(\{\alpha \in \mathcal{O}_{1728}[1/\ell]^\times \,|\, \mathrm{nrd}(\alpha) = \ell^{2n}, \text{ for } n \in \mathbb{Z}\})\backslash \mathrm{PGL}_2(\mathbb{Q}_\ell)/\mathrm{PGL}_2(\mathbb{Z}_\ell).$$

- ***Edges**: Each vertex $[M]$ has $\ell+1$ outgoing edges labelled by*

$$D_i = \begin{pmatrix} 1 & 0 \\ i & \ell \end{pmatrix}, \text{ where } i = 0, \ldots, \ell-1, \text{ or } D_\infty = \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}.$$

  The codomain vertex of D_i is $[D_i \cdot M]$. An edge labelled by a matrix D_i will be referred to as a step in direction i.

Via the map Φ_ℓ of Definition 2.10 we get a natural correspondence between the ℓ-ideal graph of $B_{p,\infty}$ of Section 2.2 and the graph of Definition 2.12. This therefore also maps via Deuring correspondence onto the supersingular isogeny graph $\mathcal{G}_{p,\ell}$ defined in Section 2.1.

In fact, the graph of the special fibre at ℓ of the Shimura curve $X(p\ell)$ of discriminant $p\ell$ is a double cover of $\mathcal{G}_{p,\ell}$, where the root $\left[\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right]$ maps to $j(E_{1728})$. This was shown by Ribet [22] and made explicit by Franc and Masdeu [13].

2.4. **Directing isogenies with Bruhat-Tits trees.** A detailed description of how to map the directions of Definition 2.12 onto the supersingular ℓ-isogeny graph is given in [1, Section 4.2]. We recall the main points here, restricted to our case study, for the benefit of the reader. While we impose restrictions on p and ℓ, we recall from Remark 2.8 that these are cryptographically relevant choices.

Proposition 2.13. *Let $2 \neq \ell$ be a small prime and let $p = 4 \cdot f \cdot \ell^e - 1$ be a prime, where f is an integer coprime to ℓ and e is any positive integer. Let $G(X(p\ell)_\ell)$ be the graph of the special fibre at ℓ of the Shimura curve $X(p\ell)$ of discriminant $p\ell$ of Definition 2.12. Let $E_{1728}/\mathbb{F}_p : y^2 = x^3 + x$ be an elliptic curve. For some $1 \leq n \leq e$, let $(x_P, y_P) = P \in E_{1728}(\mathbb{F}_p)$ be a generator of $\ker(-id + \pi_p) \cap E_{1728}[\ell^n]$ and let $Q = (-x_P, \sqrt{-1}y_P)$; then $\{P, Q\}$ is a basis of $E_{1728}[\ell^n]$. Let $\mathcal{G}_{p,\ell}$ be the supersingular ℓ-isogeny graph of Section 2.1. Then there exists a double covering map*

$$R : G(X(p\ell)_\ell) \to \mathcal{G}_{p,\ell}$$

that sends

$$\left[\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right] \mapsto 1728,$$

and sends the path $D_{d_0}, \ldots, D_{d_{n-1}}$ defined in Definition 2.12 to the isogeny with kernel generated by the entries of the following vector:

$$D_{d_{n-1}} \cdots D_{d_0} \begin{pmatrix} P \\ Q \end{pmatrix}.$$

Proof. See Ribet [22]; the explicit computational details are in [1, Section 4.2.3] and the accompanying code. □

3. A parametrization of orders

Here we state the main result of this paper, which in itself is a case study of the methods presented here for parametrization of orders in supersingular ℓ-isogeny graphs (see Section 2.1 for a definition). The parameters chosen for this case study are chosen to be cryptographically relevant as well as optimal for our methods.

Theorem 3.1. *Let $\ell \equiv 3 \pmod 4$ be prime. Let $p = 4 \cdot f \cdot \ell^e - 1$ be prime, with $f \in \mathbb{Z}_{>0}$ coprime to ℓ and $e \in \mathbb{Z}_{>0}$. Let G be the ℓ-ideal graph of $B_{p,\infty}$ defined in Section 2.2, with edges labelled by directions $\{0, \dots, \ell-1, \infty\}$ as defined in Definition 2.12 via the map Φ_ℓ of Lemma 2.10. Let V be the vertex reached via a level-increasing walk in directions $d_0, \dots, d_{n-1}$, where $n \leq e$, from the initial vertex $[\mathcal{O}_{1728}]$. Denote by $v_\ell(\cdot)$ the ℓ-adic valuation. Define:*

- *if $d_0 \neq \infty$, then $d = \sum_{i=0}^{n-1} d_i \ell^i$,*
- *if $d_0 = \infty$, for each i define[7] $d_i^\infty = \begin{cases} 0 & d_i = \infty \\ \infty & d_i = 0 \\ \ell - d_i & o.w. \end{cases}$ and $d = \sum_{i=0}^{n-1} d_i^\infty \ell^i$,*
- *a any integer lift of $(1+d^2)^{-1} \pmod{\ell^n}$,[8]*
- *$\alpha = \begin{cases} (1+\ell^n)/2 - a & d_0 \neq \infty \\ -(1+\ell^n)/2 + a & d_0 = \infty \end{cases}$ and $\beta = \ell^n/2 - ad$,*
- *$N = \frac{1}{4} + p(\alpha^2 + \beta^2) \in \ell^n\mathbb{Z}$,*
- *$g = \min\{n, v_\ell(N) - n\}$,*
- *$A, B \in \mathbb{Z}$ satisfying $Ap\ell^n + B\frac{N}{\ell^n} = \ell^g$,*
- *$h = \min\{g, v_\ell(1-2a)\}$, and*
- *$A', B' \in \mathbb{Z}$ satisfying $A'2\alpha p - B'\ell^g = \ell^h$.*

Then there is a representative $\mathcal{O}$ of V with basis given by

$$\begin{pmatrix} 1 & 0 & 0 & \frac{1}{2} \\ 0 & \ell^g - \frac{B}{2\ell^n}(4N-1) & \frac{p\beta}{\ell^h} & -\frac{p(2p\beta^2 A' + \alpha\ell^h)}{\ell^g} \\ 0 & -\frac{\beta B}{\ell^n} & \frac{1}{2\ell^h} & -\frac{p\beta A'}{\ell^g} \\ 0 & \frac{\alpha B}{\ell^n} & 0 & \frac{\ell^h}{2\ell^g} \end{pmatrix}.$$

Most of the rest of this paper is dedicated to the proof of this theorem via the following strategy:

(1) In Section 3.1, prove that the left-ideal I of $\mathcal{O}_{1728}$ such that $\mathcal{O} = \mathcal{O}_r(I)$ is

$$I = \begin{cases} \mathcal{O}_{1728}(-1 + j + (i+k)d) + \mathcal{O}_{1728}\ell^n & \text{if } d_0 \neq \infty \\ \mathcal{O}_{1728}(d(-1+j) + i + k) + \mathcal{O}_{1728}\ell^n & \text{if } d_0 = \infty. \end{cases}$$

(2) In Section 3.2 use Section 3.1 to get an explicit description of a $\mathbb{Z}$-basis for I.
(3) In Section 3.3, reconstruct the explicit basis of $\mathcal{O}$ from the $\mathbb{Z}$-basis for I.

[7] In the $d_0 = \infty$ subtree we need to relabel so that d is well-defined; with this swap we ensure for all i that $d_i^\infty \neq \infty$. This swap amounts to reordering the basis of $T_\ell(E_{1728})$.

[8] Note that this exists as $\ell \equiv 3 \pmod 4$.

3.1. **A description of the connecting ideal.** Lemma 3.2 constitutes the first step of the proof of Theorem 3.1: a simple form of the left-ideal I of $\mathcal{O}_{1728}$ such that $\mathcal{O} = \mathcal{O}_r(I)$.

Lemma 3.2. *Let all notation be as in Theorem 3.1. The left-ideal I of $\mathcal{O}_{1728}$ corresponding to the given walk with $\mathcal{O} = \mathcal{O}_r(I)$ is given by*

$$I = \begin{cases} \mathcal{O}_{1728}(-1 + j + (i+k)d) + \mathcal{O}_{1728}\ell^n & \text{if } d_0 \neq \infty \\ \mathcal{O}_{1728}(d(-1+j) + i + k) + \mathcal{O}_{1728}\ell^n & \text{if } d_0 = \infty. \end{cases}$$

Proof. We define the isomorphism between $\mathrm{End}(E_{1728})$ and $\mathcal{O}_{1728}$ as

$$\begin{array}{rccc} \varphi: & \mathrm{End}(E_{1728}) & \to & \mathcal{O}_{1728} \\ & \pi : (x,y) \mapsto (x^p, y^p) & \mapsto & j \\ & \iota : (x,y) \mapsto (-x, \sqrt{-1}y) & \mapsto & i. \end{array}$$

Recall from Proposition 2.13 that we have fixed a basis $\{P, Q\}$ of $E_{1728}[\ell^e]$ for which $\langle P \rangle = \ker(\varphi^{-1}(-1+j)) \cap E_{1728}[\ell^e]$ and $Q = \iota(P)$. From this we see $\pi(P) = P$, $\iota(P) = Q$, $\pi(Q) = \pi(\iota(P)) = -\iota(\pi(P)) = -\iota(P) = -Q$ and $\iota(Q) = \iota(\iota(P)) = -P$.

By [1, Section 4.2.3] for $d_0 \neq \infty$, the isogeny is determined by the subgroup $\langle R \rangle$ where $R = \ell^{e-n}(P + dQ)$. By the Deuring correspondence, the quaternion ideal corresponding to this isogeny is the ideal of all endomorphisms which have R contained in their kernel. We will show this is exactly the ideal given in the statement. As $n \leq e$ we have that R lies in the kernel of the scalar endomorphism $[\ell^n]$. Also R lies in the kernel of $\varphi^{-1}(-1 + j + (i+k)d)$ as $([-1] + \pi + [d] \circ \iota + [d] \circ \iota \circ \pi)(\ell^{e-n}P + d\ell^{e-n}Q) = \ell^{e-n}(-P - dQ + P - dQ + dQ - d^2P + dQ + d^2P) = 0$. Hence every endomorphism within the stated ideal has kernel containing R, so the ideal corresponding to our isogeny at least contains the stated ideal. To show they are equal one may then check the stated ideal has norm ℓ^n and so is the correct size.

For $d_0 = \infty$ the isogeny walk has kernel generated by $R = \ell^{e-n}(dP + Q)$. Again $\ell^{e-n}(dP+Q) \in \ker([\ell^n])$ and $\ell^{e-n}(dP+Q) \in \ker(\varphi^{-1}(d(-1+j)+i+k))$ because $([-d] + [d] \circ \pi + \iota + \iota \circ \pi)(d\ell^{e-n}P + \ell^{e-n}Q) = \ell^{e-n}(-d^2P - dQ + d^2P - dQ + dQ - P + dQ + P) = 0$. Then by the same reasoning as before, the ideal corresponding to the walk is exactly the ideal stated. □

3.2. **An explicit basis for the connecting ideal.** Lemma 3.2 gave us a formula for I, which leads to a way of parametrizing the bases of orders in the Bruhat-Tits tree by computing a $\mathbb{Z}$-basis of I and computing its right order. In this section we compute a $\mathbb{Z}$-basis of I.

Proposition 3.3. *Let all notation be as in Theorem 3.1. The left-ideal I of $\mathcal{O}_{1728}$ corresponding to the given walk with $\mathcal{O} = \mathcal{O}_r(I)$ is given by*

$$I = \left\langle \frac{1}{2} + \alpha j + \beta k, \frac{i}{2} - \beta j + \alpha k, \ell^n j, \ell^n k \right\rangle_{\mathbb{Z}}$$

where a is any integer lift of $(d^2+1)^{-1} \mod \ell^n$ and

$$\alpha = \frac{1+\ell^n}{2} - a, \text{ if } d_0 \neq \infty \quad \text{or} \quad \alpha = -\frac{1+\ell^n}{2} + a, \text{ if } d_0 = \infty$$

$$\text{and} \quad \beta = \frac{\ell^n}{2} - ad.$$

Remark 3.4. *Using Euler's theorem we could take for example $a = (d^2+1)^{\ell^n - \ell^{n-1} - 1}$.*

Before proving this proposition, we prove two technical lemmas to aid us in the linear algebra involved in the final step of the proof of Proposition 3.3 both for the case $d_0 \neq \infty$ (Lemma 3.5) and for the case $d_0 = \infty$ (Lemma 3.6).

Lemma 3.5. *Let $d_0 \neq \infty$ and let ℓ, p, n, and d be as in Theorem 3.1. Then the $\mathbb{Z}$-lattice spanned by*

$$\begin{pmatrix} \frac{-dp-1}{2} & \frac{-d-p}{2} & -p & -dp & \frac{\ell^n}{2} & 0 & 0 & 0 \\ \frac{d-p}{2} & \frac{pd-1}{2} & dp & -p & 0 & \frac{\ell^n}{2} & 0 & 0 \\ \frac{d+1}{2} & \frac{-d-1}{2} & -1 & d & 0 & \frac{\ell^n}{2} & \ell^n & 0 \\ \frac{d-1}{2} & \frac{1-d}{2} & -d & -1 & \frac{\ell^n}{2} & 0 & 0 & \ell^n \end{pmatrix}$$

can be rewritten as the $\mathbb{Z}$-span of

$$\begin{pmatrix} \frac{1}{2} & 0 & 0 & 0 \\ 0 & \frac{1}{2} & 0 & 0 \\ \frac{\ell^n+1}{2} - a & -\frac{\ell^n}{2} + ad & \ell^n & 0 \\ \frac{\ell^n}{2} - ad & \frac{\ell^n+1}{2} - a & 0 & \ell^n \end{pmatrix}.$$

Proof. We perform unimodular column operations to obtain 4 columns of zeroes. These are not quite the standard elementary column operations, as they are required to be integral and reversible. This means we column multiplication $c_i \mapsto kc_i$ is forbidden unless $k = \pm 1$, as scaling a vector results in a sublattice.

First for any $i \in \{0, 1, 2, 3\}$ we notice that using the last 4 rows we can always obtain a column of zeroes with ℓ^n in the ith entry in a reversible way. This means every entry in the first 4 columns can be reduced modulo ℓ^n. Since $p = 4 \cdot f \cdot \ell^e - 1$ we can replace p's with -1's resulting in matrix:

$$\begin{pmatrix} \frac{d-1}{2} & \frac{-d+1}{2} & 1 & d & \frac{\ell^n}{2} & 0 & 0 & 0 \\ \frac{d+1}{2} & \frac{-d-1}{2} & -d & 1 & 0 & \frac{\ell^n}{2} & 0 & 0 \\ \frac{d+1}{2} & \frac{-d-1}{2} & -1 & d & 0 & \frac{\ell^n}{2} & \ell^n & 0 \\ \frac{d-1}{2} & \frac{1-d}{2} & -d & -1 & \frac{\ell^n}{2} & 0 & 0 & \ell^n \end{pmatrix}.$$

We provide column operations for the remainder of the reduction below, where we note that $\gcd(d^2+1, \ell^n) = 1$ since assume for contradiction $\ell \mid d^2+1$ then $d^2 \equiv -1 \mod \ell$ but -1 is not a square modulo ℓ, since $\ell \equiv 3 \mod 4$. Define integers a, b as the solutions to $1 = a(d^2+1) + b\ell^n$ from the extended Euclidean algorithm.

1. $c_2 \mapsto c_2 + c_1$
2. $c_4 \mapsto c_4 - 2c_1 - c_3$
3. $c_5 \mapsto c_5 - \frac{\ell^n - 1}{2} c_3$
4. $c_3 \mapsto c_3 - 2c_5$
5. $c_1 \mapsto c_1 - (d-1)c_5 + (d+1)c_8$
6. $c_3 \mapsto c_3 + 2dc_6 + (1-d)c_7$
7. $c_1 \mapsto c_1 - (d-1)c_5 + \frac{d(d-1)}{2} c_8$
8. $c_1 \mapsto c_1 + d(d-1)c_6 - \frac{d(d-1)}{2} c_7$
9. $c_2 \mapsto c_2 + ac_1$
10. $c_2 \mapsto c_2 + bc_6$
11. $c_1 \mapsto c_1 - (d^2+1)c_2$
12. $c_1 \mapsto c_1 + \frac{b(d-1)(\ell^n - d - 1)}{2} c_8$
13. $c_1 \mapsto c_1 + \frac{b(-2d + d(\ell^n + d) - \ell^n + 1)}{2} c_7$
14. $c_6 \mapsto c_6 - \ell^n c_2 + \frac{a(2d - d(\ell^n + d) + \ell^n - 1)}{2} c_7$
15. $c_6 \mapsto c_6 - \frac{a(d-1)(\ell^n - d - 1)}{2} c_8$
16. $c_2 \mapsto c_2 + \frac{b(\ell^n + 1) + ad(d+1)}{2} c_8$
17. $c_2 \mapsto c_2 + \frac{ad(d+1) + b(\ell^n - 1)}{2} c_7$
18. $c_5 \mapsto c_5 - d(\ell^n - 1)c_2$
19. $c_5 \mapsto c_5 + \frac{d(\ell^n + 1 - 2a) - 2d}{2} c_8$

20. $c_5 \mapsto c_5 + \dfrac{2(1-a)+(d-2b)(\ell^n-1)}{2} c_7$
21. $c_1 \leftrightarrow c_5$
22. $c_3 \leftrightarrow c_7$
23. $c_4 \leftrightarrow c_8$
24. $c_2 \mapsto c_2 - c_3$

This results in the basis given in the statement. We provide symbolic verification of these column operations using Sagemath in file `ideal_basis.ipynb`. □

Lemma 3.6. *Let $d_0 = \infty$ and let ℓ, p, n, and d be as in Theorem 3.1. Then the $\mathbb{Z}$-lattice spanned by*

$$\begin{pmatrix} \frac{-d-p}{2} & \frac{-dp-1}{2} & -dp & -p & \frac{\ell^n}{2} & 0 & 0 & 0 \\ \frac{-dp+1}{2} & \frac{-d+1}{2} & p & -dp & 0 & \frac{\ell^n}{2} & 0 & 0 \\ \frac{d+1}{2} & \frac{-d-1}{2} & -d & 1 & 0 & \frac{\ell^n}{2} & \ell^n & 0 \\ \frac{-d+1}{2} & \frac{d-1}{2} & -1 & -d & \frac{\ell^n}{2} & 0 & 0 & \ell^n \end{pmatrix}$$

can be rewritten as the $\mathbb{Z}$-span of

$$\begin{pmatrix} \frac{1}{2} & 0 & 0 & 0 \\ 0 & \frac{1}{2} & 0 & 0 \\ -\frac{\ell^n+1}{2} + a & -\frac{\ell^n}{2} + ad & \ell^n & 0 \\ \frac{\ell^n}{2} - ad & -\frac{\ell^n+1}{2} + a & 0 & \ell^n \end{pmatrix}.$$

Proof. We start by applying column swap operations $c_1 \leftrightarrow c_2$ and $c_3 \leftrightarrow c_4$. Then we have almost the same matrix as in Lemma 3.5 so we can follow the proof, while noting some entries have different signs. By the same argument we replace occurances of p with -1. Then apply the same column operations, except changing the sign on operations labelled $6, 8, 9, 11, 13, 15, 16, 18, 20$, by which we mean operation $c_i \mapsto c_i + kc_j$ becomes $c_i \mapsto c_i - kc_j$. We provide symbolic verification in file `ideal_basis_inf.ipynb`. This completes the proof. □

Proof of Proposition 3.3. Recall that in Section 2.3 we fixed the $\mathbb{Z}$-basis of the order $\mathcal{O}_{1728}$ to be $\{\frac{1+k}{2}, \frac{i+j}{2}, j, k\}$, and by Lemma 3.2,

$$I = \begin{cases} \mathcal{O}_{1728}(-1+j+(i+k)d) + \mathcal{O}_{1728}\ell^n & \text{if } d_0 \neq \infty \\ \mathcal{O}_{1728}(d(-1+j)+i+k) + \mathcal{O}_{1728}\ell^n & \text{if } d_0 = \infty. \end{cases}$$

Hence we find a basis of I in three steps. Consider first the case $d_0 \neq \infty$:

(1) Scale the basis of $\mathcal{O}_{1728}$ to obtain a basis of lattice $\mathcal{O}_{1728}\ell^n$. This is trivial and gives

$$\mathcal{O}_{1728}\ell^n = \left\langle \frac{\ell^n}{2} + \frac{\ell^n}{2}k, \frac{\ell^n}{2}i + \frac{\ell^n}{2}j, \ell^n j, \ell^n k \right\rangle_{\mathbb{Z}}.$$

(2) Multiply basis elements of $\mathcal{O}_{1728}$ with $-1+j+(i+k)d$ to obtain a basis of lattice $\mathcal{O}_{1728}(-1+j+(i+k)d)$. The resulting basis elements are

(1) $-\left(\dfrac{pd+1}{2}\right) + \left(\dfrac{d-p}{2}\right)i + \left(\dfrac{d+1}{2}\right)j + \left(\dfrac{d-1}{2}\right)k,$
(2) $-\left(\dfrac{p+d}{2}\right) + \left(\dfrac{pd-1}{2}\right)i - \left(\dfrac{d+1}{2}\right)j + \left(\dfrac{1-d}{2}\right)k,$
(3) $-p + dpi - j - dk,$
(4) $-dp - pi + dj - k.$

(3) Compute a rank 4 basis of the sum of lattices $\mathcal{O}_{1728}(-1+j+(i+k)d)$ and $\mathcal{O}_{1728}\ell^n$.

This final step means reducing linear combinations of the 8 basis vectors above to linear combinations of 4 basis vectors. We write the 8 basis vectors in a 8×4 matrix in which each column represents a vector with entries given by the coefficients of $1, i, j$, and k respectively, and this results in the matrix of Lemma 3.5. For $d_0 \neq \infty$, the result now follows.

In the case $d_0 = \infty$ we take the same approach. The entries of the basis vectors have the same coefficients as those above, up to some differences in sign. They are given in matrix form in Lemma 3.6, where they are reduced. □

3.3. **Proof of Theorem 3.1.** Recall from the beginning of Section 3 our strategy to prove Theorem 3.1 was split into three parts:

(1) In Section 3.1, we proved that the left-ideal I of $\mathcal{O}_{1728}$ such that $\mathcal{O} = \mathcal{O}_r(I)$ is
$$I = \begin{cases} \mathcal{O}_{1728}(-1+j+(i+k)d) + \mathcal{O}_{1728}\ell^n & \text{if } d_0 \neq \infty \\ \mathcal{O}_{1728}(d(-1+j)+i+k) + \mathcal{O}_{1728}\ell^n & \text{if } d_0 = \infty. \end{cases}$$
(2) In Section 3.2 we used Section 3.1 to get an explicit description of a $\mathbb{Z}$-basis for I.
(3) Now, we reconstruct the explicit basis of $\mathcal{O}$ (the right-order of I) from the $\mathbb{Z}$-basis for I. For this, we follow the method implemented in SageMath for the function `.right_order()` [4]; it is more complicated in our situation due to the necessity to work symbolically, but the theory is the same. The reconstruction is split into three parts:
   (a) In Lemma 3.7, we use the $\mathbb{Z}$-basis of I from Proposition 3.3 to give $\mathbb{Z}$-bases of rank 4 $\mathbb{Z}$-modules J_1 and $J_2 \subseteq B_{p,\infty}$ such that $\mathcal{O} = J_1 \cap J_2$.
   (b) In Proposition 3.8, we give a $\mathbb{Z}$-basis of $J_1 + J_2$ defined as the span of the basis vectors of J_1 and J_2. This is aided by Lemma 3.9, which is a technical lemma on linear algebra.
   (c) Deduce a $\mathbb{Z}$-basis of $\mathcal{O} = J_1 \cap J_2$ from the derivation of the $\mathbb{Z}$-basis of $J_1 + J_2$.

Lemma 3.7. *Let all notation be as in Theorem 3.1. Then the order $\mathcal{O}$ is the intersection of the following rank 4 $\mathbb{Z}$-modules:*
$$J_1 = \left\langle 1, \frac{(1-2N)i - 2\beta j + 2\alpha k}{2N}, \frac{2p\alpha\ell^n + 2p\beta\ell^n i + \ell^n j}{2N}, \frac{2p\beta\ell^n - 2p\alpha\ell^n i + \ell^n k}{2N} \right\rangle_{\mathbb{Z}},$$
$$J_2 = \left\langle 1, -i, \frac{2p\alpha - 2p\beta i - j}{2\ell^n p}, \frac{2p\beta + 2p\alpha i - k}{2\ell^n p} \right\rangle_{\mathbb{Z}}.$$

Proof. Recall that Proposition 3.3 gave a $\mathbb{Z}$-basis of the left-ideal I of $\mathcal{O}_{1728}$ for which $\mathcal{O}$ is the right order. Denote by $\{b_1, b_2, \ell^n j, \ell^n k\}$ the $\mathbb{Z}$-basis of the ideal I from Proposition 3.3. Observe that $ib_1 = b_2$. For $r \in \{1,2,3,4\}$ define the left multiplication maps
$$\begin{array}{rccc} \varphi_r : & B_{p,\infty} & \to & B_{p,\infty} \\ & x & \mapsto & b_r x. \end{array}$$
Then the right order is given by
$$\mathcal{O} = \varphi_1^{-1}(I) \cap \varphi_2^{-1}(I) \cap \varphi_3^{-1}(I) \cap \varphi_4^{-1}(I).$$

We observe that only two of the four $\mathbb{Z}$-modules $\varphi_r^{-1}(I)$ are distinct:

$$J_1 := \varphi_1^{-1}(I) = \mathbb{Z} + b_1^{-1} i b_1 \mathbb{Z} + b_1^{-1} \ell^n j \mathbb{Z} + b_1^{-1} \ell^n k \mathbb{Z} = \varphi_2^{-1}(I),$$
$$J_2 := \varphi_3^{-1}(I) = \mathbb{Z} + i\mathbb{Z} + \frac{1}{\ell^n p} j b_1 \mathbb{Z} + \frac{1}{\ell^n p} k b_1 \mathbb{Z} = \varphi_4^{-1}(I),$$

hence $\mathcal{O} = J_1 \cap J_2$. To obtain the bases of J_1 and J_2 given in the lemma, we plug in $b_1 = \frac{1}{2} + \alpha j + \beta k$ and denote by $N = \mathrm{nrd}(b_1)$ its norm. Then the inverse is $b_1^{-1} = \frac{\overline{b_1}}{N} = \frac{\frac{1}{2} - \alpha j - \beta k}{N}$; the result follows by substitution. □

Lemma 3.7 above achieved part (3a) of our proof strategy; we now continue with part (3b), finding a $\mathbb{Z}$-basis of $J_1 + J_2$.

Proposition 3.8. *Let all notation be as in Theorem 3.1. Then indeed $N \in \ell^n\mathbb{Z}$ as stated, and A, B, A', $B' \in \mathbb{Z}$ can be defined by running the extended Euclidean algorithm for $\gcd(p\ell^n, N/\ell^n) = \ell^g$ and $\gcd(2\alpha p, \ell^g) = \ell^h$. Furthermore, let J_1 and J_2 be as in Lemma 3.7 and let $\gamma, \delta \in \mathbb{Z}$ be such that $\gamma\ell^h - \delta 2\beta p = 1$. Then $J_1 + J_2 \subseteq B_{p,\infty}$ is a rank 4 $\mathbb{Z}$-module given by the following basis matrix:*

$$\begin{pmatrix} \frac{1}{\ell^g} & 0 & \frac{\alpha\ell^{g-h}(2Ap\ell^{n-g}-1)}{N} & \frac{-B'\ell^g\beta(2Ap\ell^{n-g}-1)}{N} \\ 0 & 1 & \frac{\ell^{g-h}(\beta+2N\delta)}{N} & \frac{2B'\ell^g\alpha+A'}{2N} \\ 0 & 0 & \frac{\ell^{g-h}}{2Np} & -\frac{\beta A'}{N} \\ 0 & 0 & 0 & \frac{\ell^h}{2Np} \end{pmatrix}.$$

In order to shorten the length of the symbolic matrix reductions involved in the proof of this proposition, we first prove a technical linear algebra result.

Lemma 3.9. *Let c_1 and c_2 be columns of the basis matrix of a lattice. Denote by $(c_1)_i, (c_2)_i$ their entries on row i,*[9] *and use the extended Euclidean algorithm to define values w, u, v with $u(c_1)_i + v(c_2)_i = w = \gcd((c_1)_i, (c_2)_i)$. Then the columns can be replaced by the following columns, with the resulting matrix defining the same lattice.*

$$c_1' = uc_1 + vc_2$$
$$c_2' = -\frac{(c_2)_i}{w} c_1 + \frac{(c_1)_i}{w} c_2$$

Proof. The operation is invertible as we can derive c_1 and c_2 from integral linear combinations of c_2' and c_1':

$$\begin{aligned} u \cdot c_2' + \frac{(c_2)_i}{w} \cdot c_1' &= u\left(-\frac{(c_2)_i}{w} c_1 + \frac{(c_1)_i}{w} c_2\right) + \frac{(c_2)_i}{w}(uc_1 + vc_2) \\ &= \frac{1}{w}\left(u(c_1)_i + v(c_2)_i\right) c_2 = c_2, \end{aligned}$$

$$\begin{aligned} -v \cdot c_2' + \frac{(c_1)_i}{w} \cdot c_1' &= -v\left(-\frac{(c_2)_i}{w} c_1 + \frac{(c_1)_i}{w} c_2\right) + \frac{(c_1)_i}{w}(uc_1 + vc_2) \\ &= \frac{1}{w}\left(v(c_2)_i + u(c_1)_i\right) c_1 = c_1. \end{aligned}$$

Hence if L is the lattice generated by c_1, c_2 and L' by c_1', c_2' then by definition $L' \subseteq L$ and by the above $L \subseteq L'$ so $L = L'$. □

[9]Note that in the 'usual' notation for matrix entries, if this matrix were A, then this would give $A_{ij} = (c_j)_i$.

Proof of Proposition 3.8. Recall N, g, A, B, h, A', B' from the statement of Theorem 3.1. First of all, to see that $N \in \ell^n\mathbb{Z}$, recall from the proof of Lemma 3.7 that $N = \mathrm{nrd}(b_1)$ is the reduced norm of the first basis entry of a $\mathbb{Z}$-basis for I, the connecting ideal between $\mathcal{O}_{1728}$ and $\mathcal{O}$. Then, note that

$$\ell^g = \ell^{\min\{n, v_\ell(N)-n\}} = \gcd(p\ell^n, N/\ell^n)$$

and

$$\ell^h = \ell^{\min\{g, v_\ell(1-2a)\}} = \gcd(2\alpha p, \ell^g),$$

where $v_\ell(\cdot)$ is the ℓ-adic valuation, so A, B, A', and $B' \in \mathbb{Z}$ are well-defined and can be computed efficiently via the extended Euclidean algorithm.

All elements of $J_1 + J_2$ are the sum of an element in J_1 and an element in J_2, and are hence a linear combination of the 4 basis vectors for J_1 and the 4 basis vectors for J_2 given in Lemma 3.7. The rank of the ideal is 4 so we can reduce these 8 vectors to 4 vectors. We do this in a similar way to the proof of Proposition 3.3 by writing the 8 basis vectors in a 4×8 matrix

$$\begin{pmatrix} 1 & 0 & \frac{p\alpha\ell^n}{N} & \frac{p\beta\ell^n}{N} & 1 & 0 & \frac{\alpha}{\ell^n} & \frac{\beta}{\ell^n} \\ 0 & \frac{1}{2N} - 1 & \frac{p\beta\ell^n}{N} & -\frac{p\alpha\ell^n}{N} & 0 & -1 & -\frac{\beta}{\ell^n} & \frac{\alpha}{\ell^n} \\ 0 & -\frac{\beta}{N} & \frac{\ell^n}{2N} & 0 & 0 & 0 & -\frac{1}{2\ell^n p} & 0 \\ 0 & \frac{\alpha}{N} & 0 & \frac{\ell^n}{2N} & 0 & 0 & 0 & -\frac{1}{2\ell^n p} \end{pmatrix}$$

and using unimodular column operations to obtain 4 columns of zeroes. The process of reducing the matrix involves computing gcds in each row, for which we introduced in the statement the new variables γ and δ. To see that γ and δ are well-defined, we first show that $\gcd(2\alpha, 2\beta, \ell^g) = 1$. Let K be such that $a(d^2+1) = 1 + K\ell^n$. Then

$$-1 \cdot 2\alpha - d \cdot 2\beta + \ell^{n-g}(-2K + 1 + d) \cdot \ell^g = 1,$$

which combined with $\gcd(p, \ell^g) = 1$ gives $\gcd(2\alpha p, 2\beta p, \ell^g) = 1$. Then, by definition of h this means $\gcd(2\beta p, \ell^h) = 1$, hence we can define γ, δ such that $\gamma\ell^h - \delta 2\beta p = 1$.

With these definitions, the unimodular column operations to reduce the above 4×8 matrix to the matrix in the proposition statement are given below. We provide symbolic verification of these column operations in Sagemath file `sum.ipynb`. We denote by $c_s, c_t \mapsto uc_s + vc_t, -\frac{(c_t)_i}{w}c_s + \frac{(c_s)_i}{w}c_t$ the use of Lemma 3.9 on columns c_s and c_t.

1. $c_2 \mapsto c_2 - c_6$
2. $c_6 \mapsto -c_6$
3. $c_5 \mapsto c_5 - c_1$
4. $c_3, c_7 \mapsto Ac_3 - Bc_7, N/\ell^{n+g}c_3 + p\ell^{n-g}c_7$
5. $c_4, c_8 \mapsto Ac_4 - Bc_8, N/\ell^{n+g}c_4 + p\ell^{n-g}c_8$
6. $c_1, c_7 \mapsto -B'c_1 + A'c_7, -\frac{2\alpha p}{\ell^h}c_1 + \ell^{g-h}c_7$
7. $c_1, c_8 \mapsto \gamma c_1 - \delta c_8, -2\beta p c_1 + \ell^h c_8$
8. $c_4 \mapsto -c_4$
9. $c_2, c_4 \mapsto A'c_2 + B'c_4, \ell^{g-h}c_2 + \frac{2\alpha p}{\ell^h}c_4$
10. $c_3, c_4 \mapsto \gamma c_3 + \delta c_4, 2\beta p c_3 + \ell^h c_4$
11. $c_4 \mapsto c_4 - 2\ell^g c_6$
12. $c_7 \mapsto c_7 - \frac{2\alpha p}{\ell^h}c_5$
13. $c_8 \mapsto c_8 + 2p\beta B'c_5$
14. $c_5 \mapsto -c_5$
15. $c_2 \leftrightarrow c_4$
16. $c_2 \leftrightarrow c_6$

□

We now have all the necessary tools to prove our main theorem.

Proof of Theorem 3.1. First note that the notation N, g, A, B, h, A', B' is well-defined and A, B, A', B' can be derived directly using the extended Euclidean algorithm by Proposition 3.8.

We have that $\mathcal{O}$ is the intersection of rank 4 $\mathbb{Z}$-modules J_1 and J_2 with $\mathbb{Z}$-bases $\{u_1, u_2, u_3, u_4\}$ and $\{v_1, v_2, v_3, v_4\}$ respectively fixed to be the bases described in Lemma 3.7. Our strategy is now as follows:

(i) First, we argue that $J_1 \cap J_2$ is in bijection with the kernel of the matrix
$$M = \begin{pmatrix} 1 & 0 & \frac{p\alpha\ell^n}{N} & \frac{p\beta\ell^n}{N} & 1 & 0 & \frac{\alpha}{\ell^n} & \frac{\beta}{\ell^n} \\ 0 & \frac{1}{2N} - 1 & \frac{p\beta\ell^n}{N} & -\frac{p\alpha\ell^n}{N} & 0 & -1 & -\frac{\beta}{\ell^n} & \frac{\alpha}{\ell^n} \\ 0 & -\frac{\beta}{N} & \frac{\ell^n}{2N} & 0 & 0 & 0 & -\frac{1}{2\ell^n p} & 0 \\ 0 & \frac{\alpha}{N} & 0 & \frac{\ell^n}{2N} & 0 & 0 & 0 & -\frac{1}{2\ell^n p} \end{pmatrix}.$$
This is the concatenation of the basis matrix of J_1 with the basis matrix of J_2 discussed already in the proof of Proposition 3.8.

(ii) Second, we compute (the relevant part of) a basis of the kernel of M using standard linear algebra techniques.

(iii) Finally, we map this basis via the aforementioned bijection to a basis of
$$J_1 \cap J_2 = \mathcal{O}.$$

For (i), to show that $J_1 \cap J_2$ is in bijection with the kernel of M, we define a map
$$\begin{array}{rccc} \psi: & J_1 \cap J_2 & \to & \mathbb{Z}^8 \\ & x = x_1u_1 + \cdots + x_4u_4 & \mapsto & (x_i)_{i=1,\ldots,8}. \\ & \quad = -x_5v_1 - \cdots - x_8v_4 & & \end{array}$$
Then, for any $x \in J_1 \cap J_2$ we can represent the fact that 'x written in terms of the J_1-basis' $-$ 'x written in terms of the J_2-basis' $= 0$ via the linear system:
$$M \cdot \begin{pmatrix} x_1 \\ x_2 \\ \ldots \\ x_8 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$
Therefore, any vector in the image of ψ lies in the kernel of M. To see that the map ψ defines a *bijection* from $J_1 \cap J_2$ to the kernel of M, we need now only observe that the inverse map is given by
$$\psi^{-1} : (x_i)_{i=1,\ldots,8} \mapsto x_1u_1 + \cdots + x_4u_4.$$
This completes part (i).

For part (ii), we recall that a basis of the kernel of M is given by the columns of a *kernel matrix* of M, which is defined to be a 8×4 integral matrix X of linearly independent columns for which $MX = 0_{4\times 4}$. We recall further that X can be computed by applying unimodular column operations to the augmented matrix $\begin{pmatrix} M \\ \hline I_8 \end{pmatrix}$ until the final four columns of the upper matrix are all zeroes; then X is given by the lower right-hand 8×4 submatrix of the resulting augmented matrix. Now observe that M is exactly the matrix that we, in the proof of Proposition 3.8, reduced to a 4×4 matrix via unimodular column operations, so all that remains is to apply those column operations to I_8 in order to obtain X. In fact, as our goal is only to compute a basis of $J_1 \cap J_2$ via ψ^{-1}, and ψ^{-1} requires only the top 4 rows of a vector in the kernel of M, we only need to compute the top 4 rows of X, which

we call K. We compute K symbolically in Sagemath file `order_basis.ipynb`, obtaining:

$$K = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \ell^g & 0 & 0 \\ 0 & 2Ap\beta & \frac{N}{\ell^{n+h}} & -\frac{2pN\beta A'}{\ell^{n+g}} \\ 0 & -2Ap\alpha & 0 & N\ell^{h-n-g} \end{pmatrix}.$$

This completes part (ii).

For part (iii), it remains to apply ψ^{-1} to K, which is given by the multiplication:

$$\begin{pmatrix} 1 & 0 & \frac{p\alpha\ell^n}{N} & \frac{p\beta\ell^n}{N} \\ 0 & \frac{1}{2N} - 1 & \frac{p\beta\ell^n}{N} & -\frac{p\alpha\ell^n}{N} \\ 0 & -\frac{\beta}{N} & \frac{\ell^n}{2N} & 0 \\ 0 & \frac{\alpha}{N} & 0 & \frac{\ell^n}{2N} \end{pmatrix} \cdot K$$

$$= \begin{pmatrix} 1 & 0 & \frac{p\alpha}{\ell^h} & \frac{p\beta(-2p\alpha A' + \ell^h)}{\ell^g} \\ 0 & 2Ap\ell^n - \ell^g - \frac{Ap\ell^n - \ell^g}{2N} & \frac{p\beta}{\ell^h} & -\frac{p(2p\beta^2 A' + \alpha\ell^h)}{\ell^g} \\ 0 & \frac{\beta(Ap\ell^n - \ell^g)}{N} & \frac{1}{2\ell^h} & -\frac{p\beta A'}{\ell^g} \\ 0 & -\frac{\alpha(Ap\ell^n - \ell^g)}{N} & 0 & \frac{\ell^h}{2\ell^g} \end{pmatrix}.$$

This completes part (iii).

To get the matrix in the theorem statement, we simplify the top row with 2 more unimodular column operations $c_3 \mapsto c_3 - \frac{p\alpha}{\ell^h} c_1$ and $c_4 \mapsto c_4 + (adpB' - \frac{\ell^n pB' - 1}{2})c_1$. For the second of these, note the operation is integral since B' is odd due to the relation $A'2\alpha p - B'\ell^g = \ell^h$. In the second column we also use relation $Ap\ell^n + B\frac{N}{\ell^n} = \ell^g$ for simplification. □

4. Direction 0 Parametrization

In Theorem 3.1, some variables arise as coefficients from the extended Euclidean algorithm. This may pose a challenge to certain applications, for instance when trying to put an arbitrary basis of a maximal order into this form, some thought would be needed to identify the values these variables could take (if even possible). In this section we discuss applying Theorem 3.1 to a simple subgraph in which there exists a parametrization without coefficients from the extended Euclidean algorithm: Here we consider the basis of an order $n \leq e/2 = v_\ell(p+1)/2$ steps from the root order $\mathcal{O}_{1728}$ in direction 0, and also consider the parametrized norm forms (c.f. also [1, Example 5.4]). There may be more such subgraphs; for example our choice of directions forces this subgraph to contain only j-invariants defined over $\mathbb{F}_p$ which may impact the simplicity of the parametrization. If so, one interesting direction for further research could be to simplify the parametrization for only $\mathbb{F}_p$-curves.

Proposition 4.1. *Let all notation be as in Theorem 3.1, but fix*[10] $d = 0$ *and restrict to* $n \leq e/2$. *Then*

$$\mathcal{O} = \left\langle \frac{1+k}{2}, \frac{i + \ell^n j + (\ell^{2n} - 1)k}{2\ell^n}, j, \ell^n k \right\rangle_{\mathbb{Z}}.$$

[10]Equivalently, let $[\mathcal{O}]$ be the vertex n steps away from $[\mathcal{O}_{1728}]$ where each step is in direction 0.

Proof. We start by computing the necessary variables to use Theorem 3.1. From $a(d^2+1) \equiv 1 \mod \ell^n$ we can take $a = 1$. Then by definition we have $\alpha = \frac{\ell^n - 1}{2}$ and $\beta = \frac{\ell^n}{2}$ and

$$N = \frac{1}{4} + p(\alpha^2 + \beta^2) = \frac{p+1}{4} + \frac{\ell^n(\ell-1)}{2}.$$

Then as $v_\ell(p+1) = n$ we get that $v_\ell(N) = n$ and hence $g = 0$. Then as $0 \leq h \leq g$, we get also that $h = 0$ and we can take $A' = 0, B' = -1$. For A and B we can choose $A = \frac{p+1}{2\ell^{2n}} - 2(\ell^n - 1) + p - \frac{p+1}{\ell^n}$ and $B = -2p + 4\ell^n$ and we use the restriction $n \leq \frac{e}{2}$ ensure that $A, B \in \mathbb{Z}$.

We substitute these values into the basis matrix for $\mathcal{O}$ given by Theorem 3.1

$$\begin{pmatrix} 1 & 0 & 0 & \frac{1}{2} \\ 0 & \frac{p^2}{\ell^n} + p(\ell^n - 1)(2p - 4\ell^n) - 2p + 1 & \frac{p\ell^n}{2} & -\frac{p(\ell^n-1)}{2} \\ 0 & p - 2\ell^n & \frac{1}{2} & 0 \\ 0 & -p + \frac{p}{\ell^n} + 2\ell^n - 2 & 0 & \frac{1}{2} \end{pmatrix}.$$

This can be simplified to

$$\begin{pmatrix} \frac{1}{2} & 0 & 0 & 0 \\ 0 & \frac{1}{2\cdot\ell^n} & 0 & 0 \\ 0 & \frac{1}{2} & 1 & 0 \\ \frac{\ell^n}{2} & \frac{\ell^{2n}-1}{2\cdot\ell^n} & 0 & \ell^n \end{pmatrix}$$

by applying the following column operations, which are verified in file `direction_0.ipynb`:

1. $c_1 \mapsto c_1 - 2c_4$
2. $c_1 \leftrightarrow c_4$
3. $c_2 \mapsto c_2 - (2p - 4\ell^n)c_4$
4. $c_4 \mapsto c_4 - 2c_3$
5. $c_4 \mapsto -c_4$
6. $c_2 \mapsto c_2 + 2c_4$
7. $c_3 \mapsto c_3 - \frac{\ell^n + 1}{2}c_4$
8. $c_3 \mapsto -c_3$
9. $c_4 \mapsto c_4 - 2c_3$
10. $c_2 \mapsto c_2 - 2\frac{p+1}{\ell^n}c_3$
11. $c_3 \mapsto c_3 + \frac{\ell^n - 1}{2}c_2$
12. $c_2 \mapsto c_2 + 2c_3$
13. $c_3 \mapsto c_3 - \frac{p+1}{2\ell^{2n}}c_2$
14. $c_2 \mapsto c_2 - 2c_3$
15. $c_3 \mapsto c_3 + (1 - \ell^n)c_4$
16. $c_2 \mapsto c_2 - 2c_4$
17. $c_3 \mapsto c_3 - \frac{\ell^n - 1}{2}c_2$
18. $c_2 \mapsto c_2 + 2c_3$
19. $c_2 \mapsto c_2 + (3 + 2p)c_4$
20. $c_3 \mapsto c_3 + pc_4$
21. $c_3 \mapsto c_3 + \frac{\ell^n + 1}{2}c_2$
22. $c_2 \mapsto c_2 - 2c_3$
23. $c_2 \mapsto c_2 + (2p - 1)c_4$
24. $c_2 \mapsto -c_2$
25. $c_2 \leftrightarrow c_3$
26. $c_4 \mapsto c_4 + (\ell^n - 1)c_3$
27. $c_4 \mapsto -c_4$
28. $c_2 \mapsto c_2 + (p + \frac{p+1}{\ell^n})c_4$
29. $c_2 \mapsto c_2 + (1 + p\ell^n - \frac{p+1}{\ell^n} - \frac{\ell^n - 1}{2})c_3$
30. $c_1 \mapsto c_1 + \ell^n p(\ell^n - 1)c_2$
31. $c_1 \mapsto c_1 - \ell^n p\frac{\ell^n - 1}{2}c_3$
32. $c_1 \mapsto c_1 + (-\ell^n p\frac{\ell^n - 1}{2} + \frac{(\ell^n - 1)(p+1)}{2\ell^n})c_4$

This gives the simplified basis matrix in the proposition statement. □

Notice the basis parametrization in direction 0 always contains the element j; this is because we chose the basis of $E_{1728}[\ell^e]$ exactly so that direction 0 is always an $\mathbb{F}_p$ direction (up to e steps from the root).

Now we use this example to revisit our earlier motivation of discovering properties of norm forms. The following lemma gives us one approach to getting uniquely represented integers:

Lemma 4.2. *For each $0 \leq n \leq \frac{e}{2}$ denote by $\mathcal{O}_n$ the order n steps in direction 0 from root order $\mathcal{O}_{1728}$. The parametrized norm form is*

$$\frac{x_0^2}{4} + \frac{x_1^2}{4\ell^{2n}} + p\left(\frac{x_1}{2} + x_2\right)^2 + p\left(\frac{x_0\ell^n}{2} + \frac{x_1(\ell^{2n}-1)}{2\ell^n} + \ell^n x_3\right)^2$$

which for all $0 < m \leq \frac{e}{2}$ has the property that $\mathcal{O}_n$ contains a trace zero element with norm

$$\frac{p+1}{4\ell^{2m}} + \frac{p(\ell^{2m}-1)}{4}$$

if and only if $n = m$.

Proof. From Proposition 4.1 an arbitrary element of $x \in \mathcal{O}_n$ can be written as:

$$x = \frac{x_0}{2} + \left(\frac{x_1}{2\ell^n}\right) i + \left(\frac{x_1}{2} + x_2\right) j + \left(\frac{x_0\ell^n}{2} + \frac{x_1(\ell^{2n}-1)}{2\ell^n} + \ell^n x_3\right) k.$$

Taking the norm results in the norm form given above. Since x_0 is the only variable that contributes to the trace, for trace zero elements we set $x_0 = 0$. We rewrite the parametrized norm form as:

$$n((x_i), n) = \frac{(p+1)x_1^2}{4\ell^{2n}} + \frac{p(\ell^{2n}-1)x_1^2}{4} + p\ell^{2n}(x_3^2 + x_1x_3) + p\left(x_2^2 + x_1x_2 - x_1x_3\right).$$

Setting $x_1 = 1$ and $x_2 = x_3 = 0$ we see that $\mathcal{O}_m$ represents $\frac{p+1}{4\ell^{2m}} + \frac{p(\ell^{2m}-1)}{4}$. It remains to show $\mathcal{O}_n$ for $n \neq m$ does not represent this value. Suppose for contradiction such an n does exist then there exists x_i such that modulo p:

$$n((x_i), n) \equiv \frac{(p+1)x_1^2}{4\ell^{2n}} \equiv \frac{p+1}{4\ell^{2m}} \mod p,$$

which implies $x_1 = \ell^{n-m}$ and $n \geq m > 0$. Then evaluating the coefficients of p we must have

$$\frac{(\ell^{2m}-1)}{4} = \frac{(\ell^{2n}-1)\ell^{2n-2m}}{4} + \ell^{2n}(x_3^2 + \ell^{n-m}x_3) + \left(x_2^2 + \ell^{n-m}x_2 - \ell^{n-m}x_3\right).$$

Multiplying through by 4 and working modulo ℓ leaves $-1 \equiv 4x_2^2 \mod \ell$ which has no integral solution since -1 is not a square modulo ℓ for $\ell \equiv 3 \mod 4$. □

5. Future work

In this final section, we discuss three of the most cryptographically relevant natural directions for future work, and some challenges around them:

(1) Extending Theorem 3.1 to cover the whole quaternion order graph, rather than only the maximal orders $\leq e$ steps from the root $\mathcal{O}_{1728}$.
(2) Extending Theorem 3.1 to apply to $\ell = 2$.
(3) Using (a version of) Theorem 3.1 to improve the KLPT subroutine in SQISign [9].

5.1. **Parametrizing the full ℓ-ideal graph.** An ℓ-isogeny graph has a diameter of roughly $\log(p)$ [2], hence for $p = 4 \cdot f \cdot \ell^e - 1$, if f is very small then Theorem 3.1 covers a large proportion of the graph. One example with $f = 1$ is as follows. But for larger f, e.g. $f \sim \sqrt{p}$ as for SIDH primes [16], the coverage is very small.

Example 5.1. *For $p = 4 \cdot 3^7 - 1 = 8747$ and $\ell = 3$ there are 730 conjugacy classes of maximal orders in $B_{p,\infty}$. Theorem 3.1 parametrizes those within a degree 3^7 walk of E_{1728}, which experimentally we see is 691 maximal orders. Therefore it covers 94.7% of the maximal order graph.*

If using our parametrization for constructive purposes, then p and ℓ could be chosen to maximise coverage, but even then as we see in the example above, not every vertex will be covered.

The challenge in extending Theorem 3.1 to paths of length $> e$ (that is $n > e$) is that there is no longer a nice canonical choice for the basis $\{P, Q\}$ of $E_0[\ell^n]$. Our choice of basis, motivated by similar choices made for efficiency reasons in implementations of SIKE [14], is a large part of the reason that the formulae remain simple enough to spot patterns and simplify the algebra. However, perhaps the algebraic manipulations in this paper and the accompanying code provide enough insight to extend the ideas to other choices of basis, in particular of $E_0[\ell^n]$ with $n > e$, with some more work. For example, it could be possible to 'reset' the root of the Bruhat-Tits tree at step e to the vertex reached and define a new nice basis at that point.

5.2. **The case of even ℓ.** From a cryptographic perspective, a version of Theorem 3.1 with $\ell = 2$ is just as interesting, if not more interesting, than the stated case of all primes $\ell \equiv 3 \pmod 4$. Isogenies of degree 2 are especially efficient to compute [8], and as a result cryptographic primitives often favour choices of prime for which $p + 1$ is highly divisible by 2, see for example [5, 14, 7]. The main obstacle in extending Theorem 3.1 to $\ell = 2$ is a practical one: We rely on Franc and Masdeu [13] for our explicit computations mapping $B_{p,\infty}$ onto the vertices of the Bruhat-Tits tree. The map Φ_ℓ they choose only maps the basis of $\mathcal{O}_{1728}$ to $M_2(\mathbb{Z}_\ell)$ if $2 \in (\mathbb{Z}_\ell)^\times$. Franc and Masdeu have extended their work to the case $\ell = 2$, but their code for this case is only implemented in Magma (referenced in [12]) and is not open source. This is therefore probably not difficult to overcome, but the formulae will be quite different and hence the amount of work for the $\ell = 2$ case is probably as much as the work we did for this paper again.

5.3. **Towards improving KLPT.** One idea that we are working towards with the methods put forward in this paper is the following: Suppose that we have overcome the issues described in Sections 5.1 and 5.2. Suppose also that we can do the same for any chosen root $\mathcal{O}$. We then have a parametrization of all the bases of the maximal orders in $B_{p,\infty}$, and hence also the norm forms, relative to their position in the 2-ideal graph with $\mathcal{O}$ at the root. Can we use the additional structure given by the parametrized norm form to improve the KLPT subroutine, or even replace it entirely? For instance, considering the space of directions $\mathcal{D}_n = \{(d_1, ..., d_n)\}$, perhaps we could find large batches of paths $S_1, S_2, ... \subseteq \mathcal{D}_n$ where for each S_i the corresponding norm forms have a certain property, such as representing certain integers. Checking these properties for the KLPT input ideal may allow us to rule out batches S_i until we are left with a small number of possible directions

$\mathcal{D}_n \setminus (S_{i_1} \cup S_{i_2} \cup ...)$. Then we could efficiently check which of the remaining paths give ideals equivalent to the input ideal. This would guarantee finding a degree ℓ^n path from $\mathcal{O}$ if one exists.

We should also think about potential cryptanalytic implications of solving the remaining issues above: Suppose (again) that you can cover the entire graph of maximal orders with parametrisations, and to each order you assign a uniquely represented integer in a similar way to Lemma 4.2. Then given a curve, finding its endomorphism ring amounts to determining whether or not endomorphisms with degrees equal to those particular integers exist.

References

[1] Laia Amorós, Annamaria Iezzi, Kristin Lauter, Chloe Martindale, and Jana Sotáková. "Explicit Connections Between Supersingular Isogeny Graphs and Bruhat–Tits Trees". In: *Women in Numbers Europe III: Research Directions in Number Theory*. Springer, 2021, pp. 39–73. DOI: 10.1007/978-3-030-77700-5_2.

[2] Sarah Arpin, Catalina Camacho-Navarro, Kristin Lauter, Joelle Lim, Kristina Nelson, Travis Scholl, and Jana Sotáková. "Adventures in Supersingularland". In: *Experimental Mathematics* 32.2 (2023), pp. 241–268. DOI: 10.1080/10586458.2021.1926009.

[3] Sarah Arpin, James Clements, Pierrick Dartois, Jonathan Komada Eriksen, Péter Kutas, and Benjamin Wesolowski. "Finding orientations of supersingular elliptic curves and quaternion orders". In: *Designs, Codes and Cryptography* (2024). DOI: 10.1007/s10623-024-01435-5.

[4] Jon Bobber, William Stein, Julian Rueth, Peter Bruin, and David Kohel. *SageMath Documentation on Quaternion Algebras*. Last accessed: 15th January 2024. URL: https://doc.sagemath.org/html/en/reference/quat_algebras/sage/algebras/quatalg/quaternion_algebra.html#.

[5] Wouter Castryck and Thomas Decru. "CSIDH on the Surface". In: *Post-Quantum Cryptography. PQCrypto 2020*. Vol. 12100. Lecture Notes in Comp. Sci. Springer, 2020, pp. 111–129. DOI: 10.1007/978-3-030-44223-1_7.

[6] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. "CSIDH: An Efficient Post-Quantum Commutative Group Action". In: *ASIACRYPT (3)*. Vol. 11274. Lecture Notes in Computer Science. Springer, 2018, pp. 395–427. DOI: 10.1007/978-3-030-03332-3_15.

[7] Denis X. Charles, Eyal Z. Goren, and Kristin E. Lauter. "Cryptographic hash functions from expander graphs". In: *J. Cryptology* 22.1 (2009), pp. 93–113. ISSN: 0933-2790. DOI: 10.1007/s00145-007-9002-x.

[8] Craig Costello. "Computing supersingular isogenies on Kummer surfaces". In: *Advances in cryptology—ASIACRYPT 2018. Part III*. Vol. 11274. Lecture Notes in Comput. Sci. Springer, 2018, pp. 428–456. DOI: 10.1007/978-3-030-03332-3_16.

[9] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. "SQISign: Compact Post-quantum Signatures from Quaternions and Isogenies". In: *Advances in Cryptology – ASIACRYPT 2020*. Springer, 2020, pp. 64–93. DOI: 10.1007/978-3-030-64837-4_3.

[10] Max Deuring. "Die Typen der Multiplikatorenringe elliptischer Funktionenkörper." In: *Abh. Math. Sem. Hansischen Univ.* 14 (1941), pp. 197–272.

[11] Tako Boris Fouotsa, Tomoki Moriya, and Christophe Petit. "M-SIDH and MD-SIDH: Countering SIDH Attacks by Masking Information". In: *Advances in Cryptology – EUROCRYPT 2023*. Springer, 2023, pp. 282–309.

[12] Cameron Franc and Marc Masdeu. *BTQuotient package*. `https://github.com/mmasdeu/btquotients`. Last accessed: 17/01/2024.

[13] Cameron Franc and Marc Masdeu. "Computing fundamental domains for the Bruhat-Tits tree for $\mathrm{GL}_2(\mathbb{Q}_p)$, p-adic automorphic forms, and the canonical embedding of Shimura curves". In: *LMS Journal of Computation and Mathematics* 17.01 (2014), pp. 1–23. DOI: 10.1112/S1461157013000235.

[14] David Jao, Reza Azarderakhsh, Matthew Campagna, Craig Costello, Luca De Feo, Basil Hess, Aaron Hutchinson, Amir Jalali, Koray Karabina, Brian Koziel, Brian LaMacchia, Patrick Longa, Michael Naehrig, Geovandro Pereira, Joost Renes, Vladimir Soukharev, and David Urbanik. "Supersingular Isogeny Key Encapsulation". In: *Updated version of [15] for round 4 of [18]* (2020).

[15] David Jao, Reza Azarderakhsh, Matthew Campagna, Craig Costello, Luca De Feo, Basil Hess, Amir Jalali, Brian Koziel, Brian LaMacchia, Patrick Longa, Michael Naehrig, Joost Renes, Vladimir Soukharev, and David Urbanik. "Supersingular Isogeny Key Encapsulation". In: *Submission to [18]* (2017). `https://sike.org`.

[16] David Jao and Luca De Feo. "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies". In: *PQCrypto*. Vol. 7071. Lecture Notes in Computer Science. Springer, 2011, pp. 19–34. DOI: 10.1007/978-3-642-25405-5_2.

[17] David Kohel, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol. "On the quaternion ℓ-isogeny path problem". In: *LMS J. Comput. Math.* 17.suppl. A (2014), pp. 418–432. DOI: 10.1112/S1461157014000151.

[18] National Institute of Standards and Technology. *Post-Quantum Cryptography Standardization*. `https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization`. Dec. 2016.

[19] National Institute of Standards and Technology. *Post-Quantum Cryptography: Digital Signature Schemes*. `https://csrc.nist.gov/projects/pqc-dig-sig/standardization/call-for-proposals`. June 2023.

[20] Christophe Petit. "Faster Algorithms for Isogeny Problems Using Torsion Point Images". In: *ASIACRYPT (2)*. Vol. 10625. Lecture Notes in Computer Science. Springer, 2017, pp. 330–353. DOI: 10.1007/978-3-319-70697-9_12.

[21] Victoria de Quehen, Péter Kutas, Chris Leonardi, Chloe Martindale, Lorenz Panny, Christophe Petit, and Katherine E. Stange. "Improved Torsion-Point Attacks on SIDH Variants". In: *Advances in Cryptology – CRYPTO 2021*. Springer, 2021, pp. 432–470. DOI: 10.1007/978-3-030-84252-9_15.

[22] Kenneth A. Ribet. "On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms". In: *Invent. Math.* 100 (1990), pp. 431–476.

[23] Sage Developers. *SageMath, the Sage Mathematics Software System (Version 10.1)*. `https://www.sagemath.org`. 2024.

[24] Joseph H Silverman. *The arithmetic of elliptic curves*. Vol. 106. Graduate Texts in Mathematics. Springer, 2009. DOI: 10.1007/978-0-387-09494-6.

[25] John Voight. *Quaternion Algebras*. Vol. 288. Graduate Texts in Mathematics. Springer, 2021. DOI: 10.1007/978-3-030-56694-4.

[26] Benjamin Wesolowski. "Orientations and the supersingular endomorphism ring problem". In: *Advances in Cryptology – Eurocrypt 2022*. 2022, pp. 345–371. DOI: 10.1007/978-3-031-07082-2_13.

[27] Benjamin Wesolowski. "The supersingular isogeny path and endomorphism ring problems are equivalent". In: *Foundations of Computer Science – FOCS 2021*. 2021. DOI: 10.1109/FOCS52979.2021.00109.

Finnish Meteorological Institute
Email address: laia.amoros@fmi.fi

University of Bristol
Email address: james.clements@bristol.ac.uk

University of Bristol
Email address: chloe.martindale@bristol.ac.uk