NTNU | Norwegian University of Science and Technology

THE QUATERNION EMBEDDING PROBLEM

Applications and Algorithms

Jonathan Komada Eriksen and Antonin Leroux

January 22, 2024

Contents

- Previous KULB seminars: Deuring correspondence.
  - Passing between ideals and isogenies second nature now...?
- In this talk, we add *orientations* into the picture.
  - CSIDH, SCALLOP, ...
- Extra data of an *imaginary quadratic* order inside of a quaternion order.

- We will look at orientations, purely on the quaternion side.
  - Optimal embeddings, and quadratic/quaternion ideals.
- "In the quaternion world, everything is easy".
  - The central theme of today: The quaternion embedding problem

Problem

Given an order $\mathcal{O} \subset B_{p,\infty}$, and an imaginary quadratic order $\mathfrak{O}$, compute an optimal embedding $\iota : \mathfrak{O} \hookrightarrow \mathcal{O}$, or decide none exists.

- We'll finish / summarize with an "isogeny magic trick".

Imaginary Quadratic Fields

- $K := \mathbb{Q}(\sqrt{-d})$ for some $d \in \mathbb{Z}$.
  - 2-dimensional $\mathbb{Q}$-algebra $\mathbb{Q} + \sqrt{-d}\mathbb{Q}$.
- An element $\alpha = x + \sqrt{-d}y$ has a conjugate $\bar{\alpha} = x - \sqrt{-d}y$.
- Can define the trace

$$\mathrm{tr}(\alpha) = \alpha + \bar{\alpha} = 2x$$

  and norm

$$\mathrm{n}(\alpha) = \alpha\bar{\alpha} = x^2 + dy^2$$

- Every $\alpha \in K$ satisfies $\alpha^2 - \mathrm{tr}(\alpha)\alpha + n(\alpha) = 0$.

Imaginary Quadratic Fields

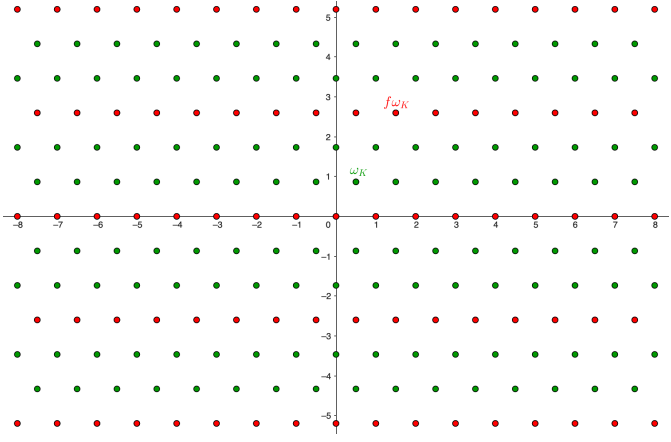
- A *lattice* L in K is something of the form

$$L = \beta_1\mathbb{Z} + \beta_2\mathbb{Z}$$

  where β_1, β_2 is a $\mathbb{Q}$-basis of K.
- An *order* $\mathfrak{O}$ is a lattice that is also a subring of K.
  - $1 \in \mathfrak{O}$ and $\mathfrak{O}$ is closed under multiplication.
- There is a *maximal* order $\mathfrak{O}_K \subset K$, containing all other orders in K.
- The *conductor* of $\mathfrak{O}$ is $f := [\mathfrak{O}_K : \mathfrak{O}]$. In this case, $\mathfrak{O} = \mathbb{Z} + f\mathfrak{O}_K$.

Example

The Eisenstein integers and a suborder in $\mathbb{Q}(\sqrt{-3})$.



Background

- A quaternion algebra B over $\mathbb{Q}$ is a 4-dimensional $\mathbb{Q}$-algebra.$\mathbb{Q} + \mathbf{i}\mathbb{Q} + \mathbf{j}\mathbb{Q} + \mathbf{k}\mathbb{Q}$.
  - Multiplication defined by $\mathbf{i}^2 = -q, \mathbf{j}^2 = -p, \mathbf{ij} = -\mathbf{ji} = \mathbf{k}$.
- Define the conjugate of $\alpha = t + \mathbf{i}x + \mathbf{j}y + \mathbf{k}z$ to be $\bar{\alpha} = t - \mathbf{i}x - \mathbf{j}y - \mathbf{k}z$.
- The *reduced trace* of $\alpha \in B_{p,\infty}$ is

$$\mathrm{trd}(\alpha) := \alpha + \bar{\alpha} = 2t$$

- The *reduced norm* of $\alpha \in B_{p,\infty}$ is

$$\mathrm{nrd}(\alpha) := \alpha\bar{\alpha} = t^2 + qx^2 + py^2 + pqz^2$$

- Every $\alpha \in B_{p,\infty}$ satisfies $\alpha^2 - \mathrm{trd}(\alpha)\alpha + \mathrm{nrd}(\alpha) = 0$.

Lattices

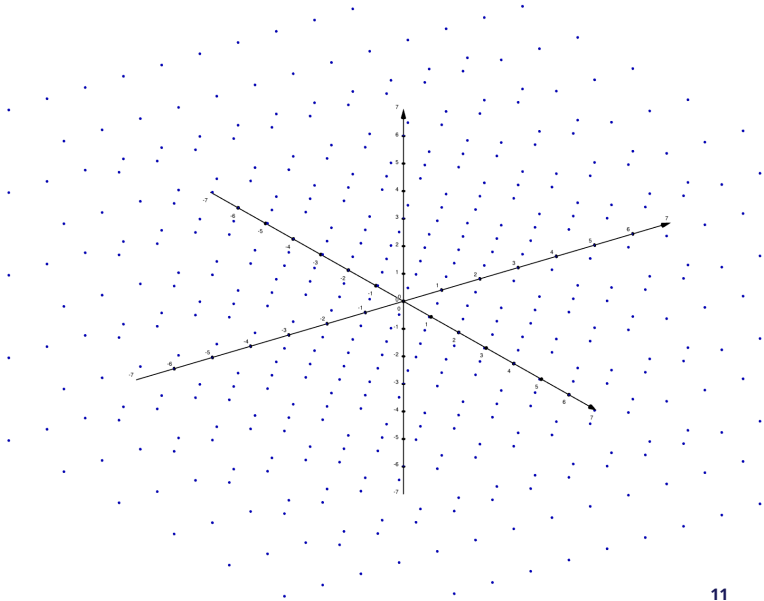
- A *lattice* L in $B_{p,\infty}$ is something of the form

$$L = \beta_1\mathbb{Z} + \beta_2\mathbb{Z} + \beta_3\mathbb{Z} + \beta_4\mathbb{Z}$$

  where $\beta_1, \beta_2, \beta_3, \beta_4$ is a $\mathbb{Q}$-basis of $B_{p,\infty}$.
- An *order* $\mathcal{O}$ is a lattice that is also a subring of $B_{p,\infty}$.
- ~~There is a maximal order containing all other orders~~ There are many maximal orders in $B_{p,\infty}$.
- NB! Sometimes in this talk, we might refer to things as “lattices”, even if they don’t have full rank.

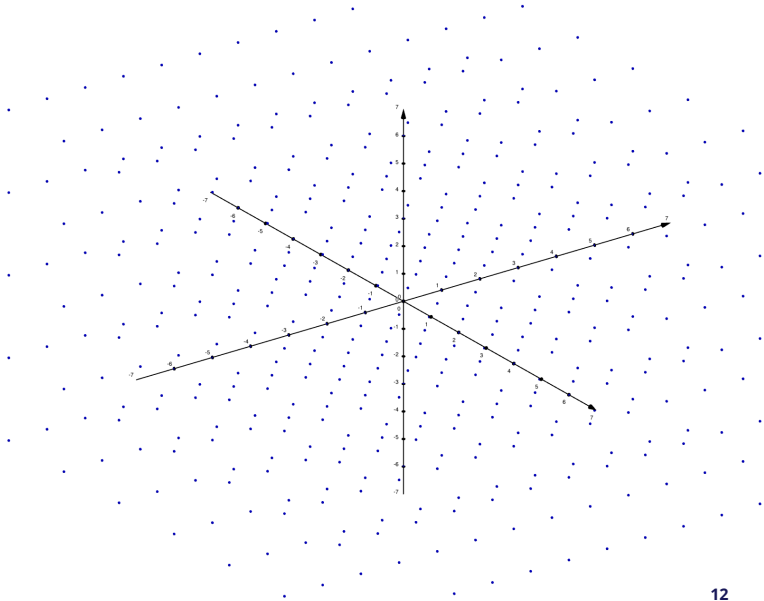
Quaternion Orders

A “quaternion order”



Quaternion Orders

A “quaternion order”
(caveat: $3 = 4$)

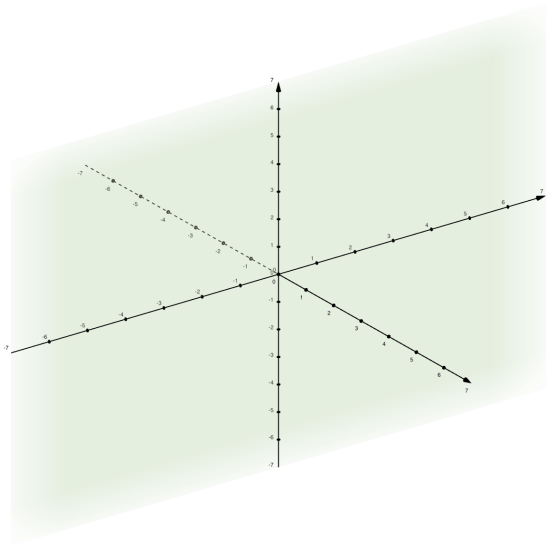


Embeddings

- The central theme of this talk is embeddings $\iota : K \hookrightarrow B_{p,\infty}$.
- Of course, $\iota(1_K) = 1_{B_{p,\infty}}$
- Let $K := \mathbb{Q}(\omega)$. What should $\iota(\omega)$ be?
  - Recall $\omega^2 - \mathrm{tr}(\omega)\omega + \mathrm{n}(\omega) = 0$.
  - Enough to find $\alpha \in B_{p,\infty}$ with $\mathrm{trd}(\alpha) = \mathrm{tr}(\omega), \mathrm{nrd}(\alpha) = \mathrm{n}(\omega)$.
  - ι is uniquely defined by $\iota(\omega)$.

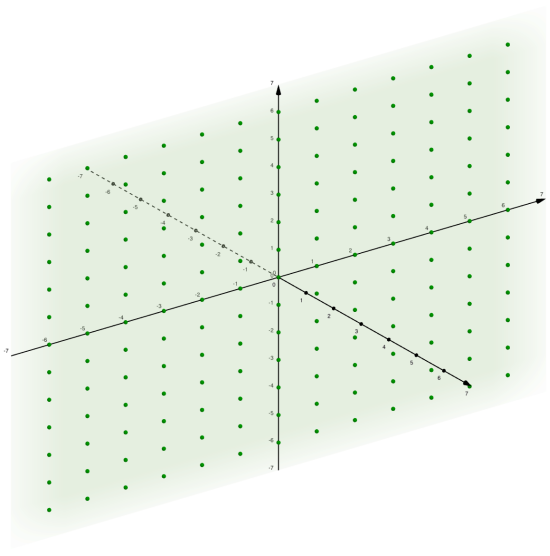
Embedding

$\iota : \mathbb{Q}(\sqrt{-1}) \hookrightarrow B$ defined by $\iota(\sqrt{-1}) = i$.



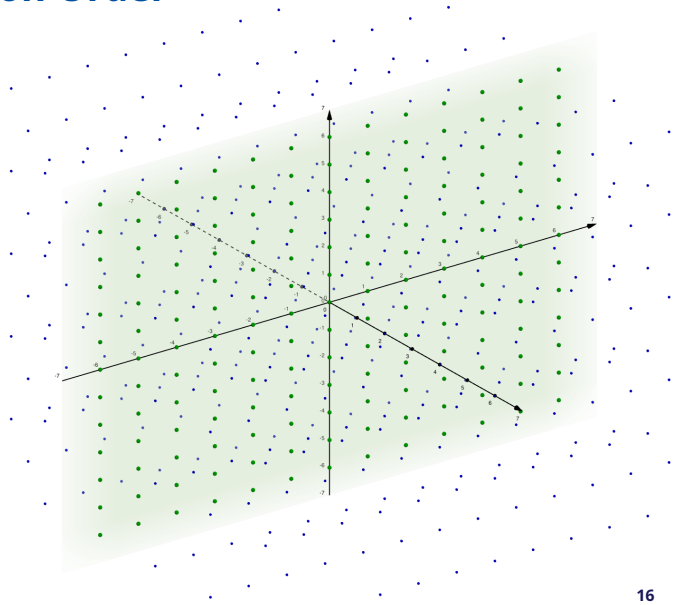
Embedding

Adding $\iota(\mathfrak{O}_K)$,
$\mathfrak{O}_K = \mathbb{Z}[\sqrt{-1}]$.



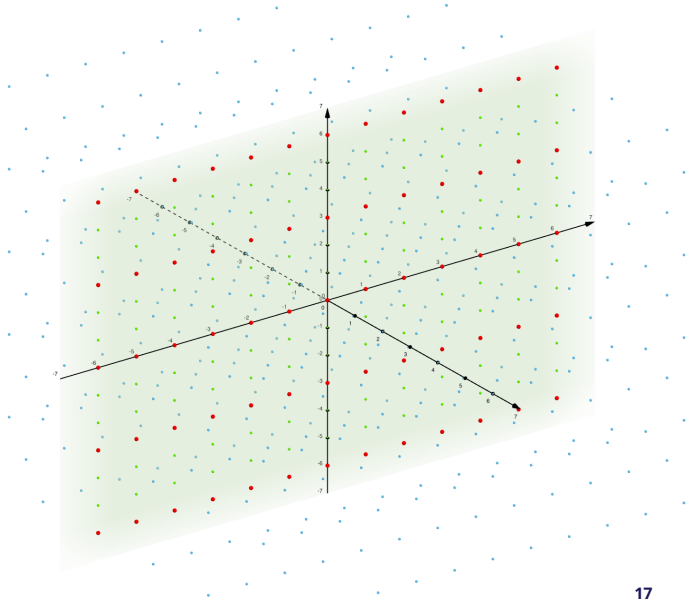
Adding back the quaternion Order

We add back the quaternion order $\mathcal{O}$, and can ask, what is $\iota(K) \cap \mathcal{O}$?



An optimal embedding

$$\iota(K) \cap \mathcal{O} = \iota(\mathbb{Z} + 3\mathfrak{O}_K).$$



Primitively Oriented Orders

- We say that $\iota : \mathfrak{O} \hookrightarrow \mathcal{O}$ is an *optimal embedding* whenever

$$\iota(K) \cap \mathcal{O} = \mathfrak{O}$$

- Given an embedding $\iota : K \hookrightarrow B_{p,\infty}$, we call the pair $(\mathcal{O}, \iota)$ a primitively $\mathfrak{O}$-oriented order $\mathcal{O}$, if $\iota(K) \cap \mathcal{O} = \iota(\mathfrak{O})$.

Correspondence of ideals

Let $(\mathcal{O}, \iota)$ be a primitively $\mathfrak{O}$-oriented order.

- Given an $\mathfrak{O}$-ideal $\mathfrak{l}$, we can look at the corresponding left $\mathcal{O}$-ideal $\mathcal{O}\langle\iota(\mathfrak{l})\rangle$.
- Correspondingly, given a left $\mathcal{O}$-ideal I, we get a $\iota(\mathfrak{O})$-ideal $I \cap \iota(K)$.

How are these operations related?

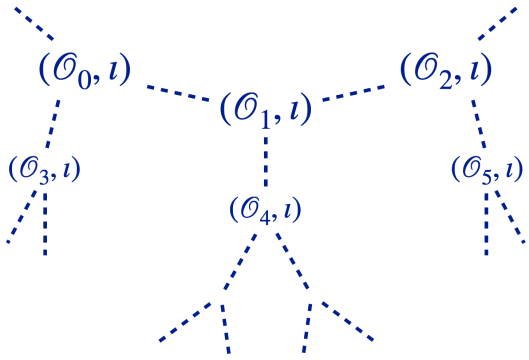
Proposition

- *Given an invertible $\mathfrak{O}$-ideal $\mathfrak{l}$, we have that $\mathcal{O}\langle\iota(\mathfrak{l})\rangle \cap \iota(\mathfrak{O}) = \iota(\mathfrak{l})$.*
- *Given a left $\mathcal{O}$-ideal I, we have that $I \supseteq \mathcal{O}\langle I \cap \iota(K)\rangle \supseteq \mathcal{O}\langle \mathrm{n}(I)\rangle$.*

Horizontal and vertical ideals

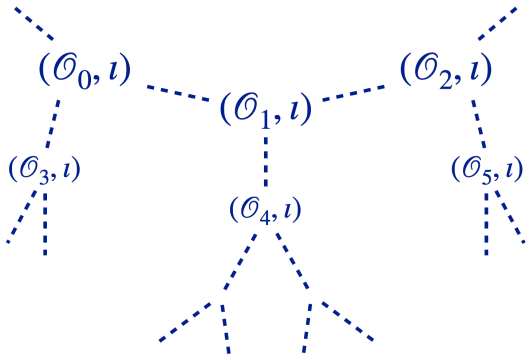
Assume $n(I)$ is prime. Three cases:

- $\mathcal{O}\langle I \cap \iota(K)\rangle = \mathcal{O}\langle n(I)\rangle$



Horizontal and vertical ideals

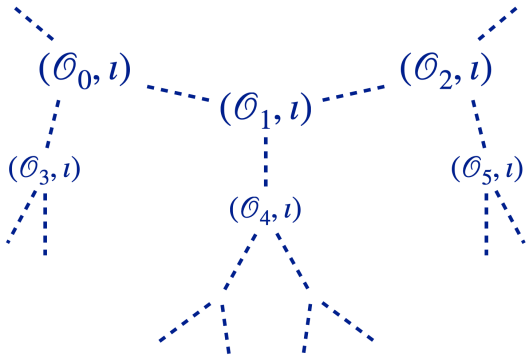
Assume $n(I)$ is prime. Three cases:



Horizontal and vertical ideals

Assume $n(I)$ is prime. Three cases:

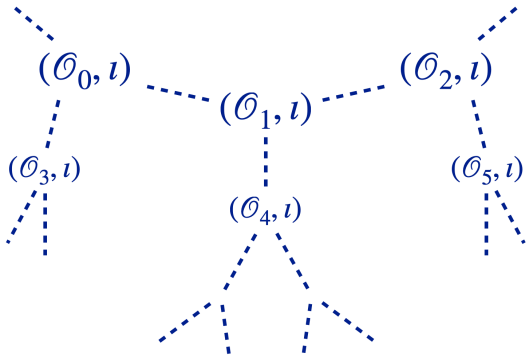
- $\mathcal{O}\langle I \cap \iota(K)\rangle = \mathcal{O}\langle n(I)\rangle$
  - I is a descending ideal



Horizontal and vertical ideals

Assume $n(I)$ is prime. Three cases:

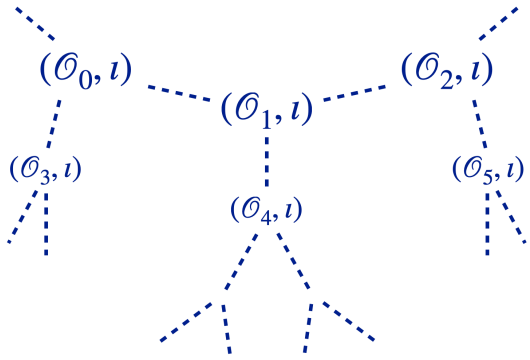
- $\mathcal{O}\langle I \cap \iota(K)\rangle = \mathcal{O}\langle n(I)\rangle$
  - I is a descending ideal
- $\mathcal{O}\langle I \cap \iota(K)\rangle = I$



Horizontal and vertical ideals

Assume $n(I)$ is prime. Three cases:

- $\mathcal{O}\langle I \cap \iota(K)\rangle = \mathcal{O}\langle n(I)\rangle$
  - I is a descending ideal
- $\mathcal{O}\langle I \cap \iota(K)\rangle = I$
  - I is a *horizontal* ideal if $n(I) \nmid f$, the conductor.
  - I is an *ascending* ideal if $n(I) \mid f$, the conductor.



What is missing?

Given two primitively $\mathfrak{O}$-oriented maximal orders, find an $\mathfrak{O}$-ideal connecting them.

- Vectorization reduces to endomorphism ring computation.
- From [CVP20][1], this was first shown for $\mathfrak{O} = \mathbb{Z}[\sqrt{-p}]$, i.e. the CSIDH case.
- Later generalised to *almost* arbitrary orders in [Wes22][2].
  - Exponential in the number of distinct prime factors of the discriminant.
- However, we can *almost* get it "for free".

[1] Rational isogenies from irrational endomorphisms
[1] Orientations and the supersingular endomorphism ring problem

A new reduction

The new reduction follows from the following simple proposition:

Proposition

Let $(\mathcal{O}_1, \iota), (\mathcal{O}_2, \iota)$ be two primitively $\mathfrak{O}$-oriented orders. Then their connecting ideal I is horizontal.

So, given $(\mathcal{O}_1, \iota_1), (\mathcal{O}_2, \iota_2)$, we need only fix the orientations.

- Find an element $\beta \in B_{p,\infty}$ such that $(\beta\mathcal{O}_2\beta^{-1}, \iota_1)$ is primitively $\mathfrak{O}$-oriented.
  - Solve $\beta\iota_2(\omega) - \iota_1(\omega)\beta = 0$.
- Compute the connecting ideal $I := \mathcal{O}_1\mathcal{O}_2N$
- Find the solution as $\iota_1(\mathfrak{l}) = I \cap \iota_1(K)$.

Computing equivalent ideals of a given norm

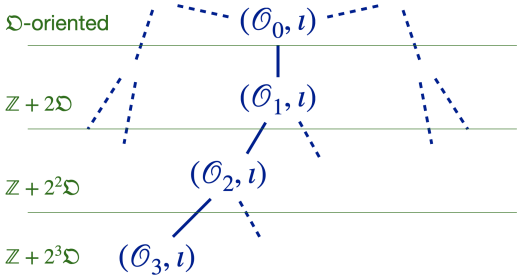
Computing isogenies of fixed degree d: Compute the endomorphism rings + look for ideals equivalent to the connecting ideal of norm d.

- Let I be the connecting ideal.
- $d < p^{1/2}$: Compute reduced basis of I.
- $d > p^{15/4}$: KLPT.
- For d in between here, the problem seems hard [BKM23][3].
- Connected to the quaternion embedding problem.

[3] Improved algorithms for finding fixed-degree isogenies between supersingular elliptic curves

Computing equivalent ideals of a given norm

- We are trying to find an ideal equivalent to $\mathcal{O}_0\mathcal{O}$ of norm d.
- $\mathcal{O}$ is primitively oriented by $\mathfrak{O}$, an ideal I of norm d induces a (not necessarily primitive) $\mathbb{Z} + d\mathfrak{O}$-orientation on $\mathcal{O}_R(I)$



Computing equivalent ideals of a given norm

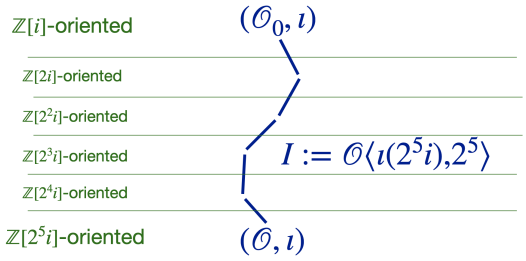
$\mathbb{Z}[i]$-oriented $(\mathcal{O}_0, \iota)$

- Important special case: $\mathcal{O}_0$ oriented by $\mathbb{Z}[i]$.
- Computed a primitive $\mathbb{Z}[2^5]$-orientation on $\mathcal{O}$.

$\mathbb{Z}[2^5 i]$-oriented $(\mathcal{O}, \iota)$

Computing equivalent ideals of a given norm

- Important special case: $\mathcal{O}_0$ oriented by $\mathbb{Z}[i]$.
- Computed a primitive $\mathbb{Z}[2^5]$-orientation on $\mathcal{O}$.
- The ascending ideal is easily computed.



Computing equivalent ideals of a given norm

- Later: can compute embeddings of $\mathfrak{O}$ into generic orders in $B_{p,\infty}$, whenever $\mathrm{disc}(\mathfrak{O}) < p^{4/3}$.
- Corollary: We can compute ideals of norm $d < p^{2/3}$ between $\mathcal{O}_0$ and $\mathcal{O}$ if they exist (with $\mathcal{O}_0$ special).
  - In general: computing these ideals of norm d reduces to computing optimal embeddings of $\mathbb{Z}[di]$.
- For generic $\mathcal{O}_0$, the reduction only works up to $d < p^{2/3}$, and requires computing optimal embeddings up to $\mathrm{disc}(\mathfrak{O}) < p^2$.

Relation to ternary quadratic forms

In general the quaternion embedding problem seems hard.

- Wlog. we can assume that $\mathrm{tr}(\alpha) = 0$, so $\alpha \in (\mathcal{O})^0$.
- Voigt, Chp 22: There is a discriminant-preserving bijection

$$\left\{ \begin{array}{l} \text{Quaternion orders} \\ \text{up to isomorphism} \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} \text{Ternary quadratic forms} \\ \text{up to similarity} \end{array} \right\}$$

  that can be given by sending $\mathcal{O}$ to the norm form of $(\mathcal{O})^0$.
  - i.e. if $\beta_1, \beta_2, \beta_3$ is a basis of $(\mathcal{O})^0$, the associated ternary quadratic form is $Q(x, y, z) := \mathrm{nrd}(x\beta_1 + y\beta_2 + z\beta_3)$.
- Our case: The quaternion embedding problem $\Leftrightarrow$ representing an integer by a positive definite ternary quadratic forms of discriminant p.

A very easy special case algorithm

From this point forward, we will think of the embedding problem as given an order $\mathcal{O} \subset B_{p,\infty}$ and an integer n, find $\alpha \in \mathcal{O}$ with $\mathrm{trd}(\alpha) = 0$ and $\mathrm{nrd}(\alpha) = n$.
Special case: Let $\mathbf{i}^2 = -1, \mathbf{j}^2 = -p$, and $\mathcal{O} = \mathbb{Z} + \mathbf{i}\mathbb{Z} + \mathbf{j}\mathbb{Z} + \mathbf{k}\mathbb{Z}$.

- The associated norm form is $Q(x, y, z) = x^2 + py^2 + pz^2$
- Solve it modulo p to find x_0, with $x_0^2 \equiv n \pmod{p}$.
- Find y, z satisfying $y^2 + z^2 = (n - (x_0 + kp)^2)/p$ for increasing k with Cornacchia.
- Then $\alpha = \mathbf{i}(x_0 + kp) + \mathbf{j}y + \mathbf{k}z$ is a solution.

B-b-b-bonus application!

Finding a curve oriented by a given order $\mathfrak{O}$:

- When $\mathfrak{O} = \mathbb{Z} + f\mathbb{Z}[i]$, this is solved by SetUpCurve in SCALLOP.
  - Computes a random decending f-isogeny from $j(E_0) = 1728$, by computing an endomorphism of degree fN with N smooth.
- For general $\mathfrak{O}$, another existing algorithm is to first solve it on the quaternion side, then standard KLPT + translate ideal
  - This used to be in Séta's key generation, took 10 hours.
- New algorithm: "as efficient as the first, but as general as the second":
  - Compute an embedding of $\mathbb{Z} + g\mathfrak{O}$ in $\mathcal{O} = \mathbb{Z} + \mathbf{i}\mathbb{Z} + \mathbf{j}\mathbb{Z} + \mathbf{k}\mathbb{Z}$, until this defines a optimal embedding of $\mathbb{Z} + g\mathfrak{O}$ into $\mathrm{End}(E_0)$.
  - Compute the ascending isogeny of degree g using the embedding.

The generic case

Given a "random" quaternion order $\mathcal{O}$, compute an element $\alpha \in \mathcal{O}(0)$ with $\mathrm{nrd}(\alpha) = n$.

- First result [Wes22]: Computing a reduced basis of $\mathcal{O}$ reveals α if $n < p^{1/2}$.
  - (Really works up to $n < p^{2/3}$).
- Again [BKM23]: Techniques applied to the order embedding problem works conjecturally up to $n < p^{4/5}$.
- This summer [ACD23][4]: Generic algorithm which works up to $n < p$ in all cases.
- New: Improving previous algorithm up to $n < p^{4/3}$, another (for arbitrary orders, not just maximal!) with the same bound, and special case improvements assuming factorisation.

[4] Finding orientations of supersingular elliptic curves and quaternion orders

A first algorithm - HNF basis

Given a quaternion order $\mathcal{O}$, compute an element $\alpha \in \mathcal{O}^{(}0)$ with $\mathrm{nrd}(\alpha) = n$.

- This algorithm works with the order in HNF form

$$\begin{aligned}\mathcal{O} = \langle e_{00} + e_{01}\mathbf{i} + e_{02}\mathbf{j} + e_{03}\mathbf{k},\\ e_{11}\mathbf{i} + e_{12}\mathbf{j} + e_{13}\mathbf{k},\\ e_{22}\mathbf{j} + e_{23}\mathbf{k},\\ e_{33}\mathbf{k}\rangle_{\mathbb{Z}}\end{aligned}$$

- Solving for trace and mod p, we get $\alpha_0 = t\beta_1 + x_0\beta_2$
- For increasing k, solve for y, z, such that $\alpha_1 = kp\beta_2 + y\beta_3 + z\beta_4$ gives the solution $\alpha_0 + \alpha_1$

Improving the HNF basis algorithm

- Notice that when α_0 is set, we are looking for k, y, z defining

$$\alpha_1 = k \cdot p\beta_2 + y \cdot \beta_3 + z \cdot \beta_4$$

- This defines a new lattice Λ in $B_{p,\infty}$.
  - In fact, this lattice Λ is exactly the trace-free part of the unique two-sided $\mathcal{O}$-ideal of norm p.
- Whenever $n < p^{4/3}$, we have that α_1 is the CVP solution to α_0 in Λ.

A new algorithm using a reduced basis

For any solution α, and any $\beta \in \mathcal{O} \setminus \mathbb{Z}[\alpha]$, the trace pairing $\mathrm{trd}(\alpha\beta)$ can be revealed mod $\Delta = \mathrm{discrd}(\mathcal{O})$ (and upper bounded).

- Found by computing the discriminant of $\mathbb{Z}\langle\alpha, \beta\rangle \subseteq \mathcal{O}$.
- Let $1, \beta_1, \beta_2, \beta_3$ be a reduced basis of $\mathcal{O}$. If $\mathrm{nrd}(\beta_i)n < \Delta^2$, the value $\mathrm{trd}(\alpha\beta)$ is known exactly, and one finds α by soling the linear system.
  - Again, for maximal orders, this "usually" happens for $n < p^{4/3}$.
- Exploit the fact that this works for any order, not just maximal!

Similarity with CVP improvement?

- Compute any solution α_0 with

$$\mathrm{trd}(\alpha_0\beta_i) = \mathrm{trd}(\alpha\beta_i) \pmod{p}$$

- Again: Look for an $\alpha_1 := \alpha - \alpha_0$ in the unique two-sided ideal of norm p.
- Hence, given any (not necessarily reduced) basis, we can again recover the same complexity by doing a CVP search for the last step.

Pathological cases

- All these except HNF-algorithm, relies on the reduced basis being somewhat uniform
  - $1, \beta_1, \beta_2, \beta_3$, with $\mathrm{nrd}(\beta_i) \approx p^{2/3}$
- Previous two: Runtime dominated by $\max\{\mathrm{nrd}(\beta_i)\}$
- However, with factorization, we get a runtime dominated by $\min\{\mathrm{nrd}(\beta_i)\}$
- Again, reduces to solving a principal quadratic form.
  - Unlike the HNF-basis method, there's seemingly no way to re-randomize this.

A magic trick

- Just like a magic trick, this is as cool as it is useless!
- Let $p \equiv 11 \pmod{12}$. We compute the shortest path between $j(E_1) = 0$ and $j(E_2) = 1728$ in the 2-isogeny graph.

A magic trick

- Let $p = 2^{55} \cdot 3 - 1 \equiv 11 \pmod{12}$. We work in the quaternion algebra

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

  where $\mathbf{i}^2 = -1$ and $\mathbf{j}^2 = -p$.
- The standard order $\mathcal{O} \cong \mathrm{End}(E_2)$ is

$$\mathbb{Z} + \mathbf{i}\,\mathbb{Z} + \frac{\mathbf{i}+\mathbf{j}}{2}\,\mathbb{Z} + \frac{1+\mathbf{k}}{2}\,\mathbb{Z}$$

- We want the smallest k such that $\mathbb{Z}[2^k\omega]$ embeds into $\mathcal{O}$, for $\omega = \frac{1+\sqrt{-3}}{2}$.

A magic trick

- For $k = 54$, we find the embedding

$$\iota(2^{54}\omega) = 9007199254740992 + \frac{19924704230006999}{2}i - \frac{23041705}{2}\mathbf{j} - 34653096\mathbf{k},$$

- Translating the ideal $I := \mathcal{O}\langle \iota(2^{54}\omega), 2^{54} \rangle$ to an isogeny from

$$E_2 : y^2 = x^3 + x$$

reveals that the point $K \in E_2$ with

$$x(K) = 86739268981076750i + 69276702275648044, \quad i^2 = -1$$

generates a 2^{54}-isogeny$\varphi : E_2 \to E_1$ with $j(E_1) = 0$.

Thank you for your attention