NTNU | Nor
Scie

THE QUATERNION
PROBLE

Applications and A

Jonathan Komada Eriksen an

January 22, 20

Contents

Previous KULB seminars: Deuring corres

Passing between ideals and isogenies s

In this talk, we add *orientations* into the p

CSIDH, SCALLOP, …

Extra data of an *imaginary quadratic* orde

We will look at orientations, purely on th

Optimal embeddings, and quadratic/qu

"In the quaternion world, everything is ea

The central theme of today: The quatern

Problem

Given an order $\mathcal{O} \subset B_{p\,\infty}$ and an imaginary qu
optimal embedding $\iota : \quad \hookrightarrow \mathcal{O}$ or decide none

We'll finish / summarize with an "isogeny

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 $\quad = x + \sqrt{\ d}y$ has a conjuga

Can define the trace

$$\mathrm{tr}(\ \ ) = \quad + \ ^{-}$$

and norm

$$\mathrm{n}(\ \ ) = \quad ^{-} = x$$

Every $\quad \in K$ satisfies $\quad ^{2} \quad \mathrm{tr}(\ \ ) \quad + n(\ \ ) =$

Imaginary Quadratic Fields

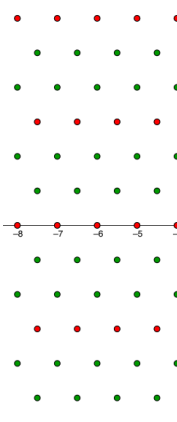
A *lattice* L in K is something of the form

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

where β_1, β_2 is a $\mathbb{Q}$-basis of K.
An *order* is a lattice that is also a subri
$1 \in$ and is closed under multiplicati
There is a *maximal* order $_K \subset K$, conta
The *conductor* of is $f := [\ _K : \ ]$. In th

Example

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



Background

A quaternion algebra B over $\mathbb{Q}$ is a 4-dim
$\mathbb{Q}$-algebra.$\mathbb{Q} + \ \mathbb{Q} + \mathbf{j}\mathbb{Q} + \mathbf{k}\mathbb{Q}$.

Multiplication defined by $^2 = \ q, \mathbf{j}^2 =$

Define the conjugate of $= t + \ x + \mathbf{j}y +$

The *reduced trace* of $\in B_{p\,\infty}$ is

$$\mathrm{trd}(\ ) := \ +$$

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

$$\mathrm{nrd}(\ ) := \ ^- = t^2 + q$$

Every $\in B_{p\,\infty}$ satisfies $^2 \ \mathrm{trd}(\ ) \ + \mathrm{n}$

Lattices

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

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

where $\beta_1, \beta_2, \beta_3, \beta_4$ is a $\mathbb{Q}$-basis of $B_{p\,\infty}$.

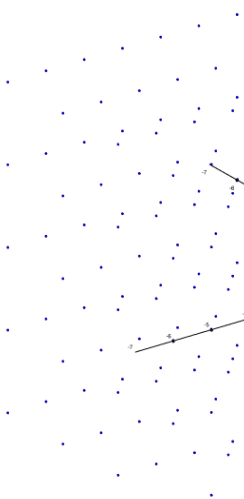
An *order* $\mathcal{O}$ is a lattice that is also a subri

~~There is a maximal order containing all o~~
maximal orders in $B_{p\,\infty}$.

NB Sometimes in this talk, we might refe
they don't have full rank.

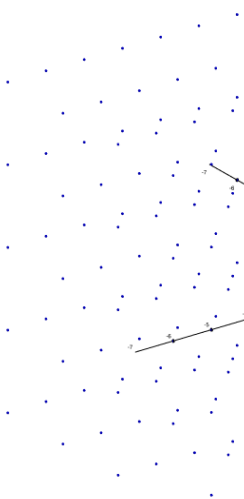
Quaternion Orders

A “quaternion order”



Quaternion Orders

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



Embeddings

The central theme of this talk is embedd

Of course, $\iota(1_K) = 1_{B_p}$

Let $K := \mathbb{Q}(\omega)$. What should $\iota(\omega)$ be?

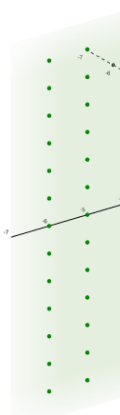
- Recall $\omega^2 \quad \mathrm{tr}(\omega)\omega + \mathrm{n}(\omega) = 0$.
- Enough to find $\quad \in B_p \quad$ with $\mathrm{trd}(\ \ ) = \mathrm{t}$
- ι is uniquely defined by $\iota(\omega)$.

Embedding

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

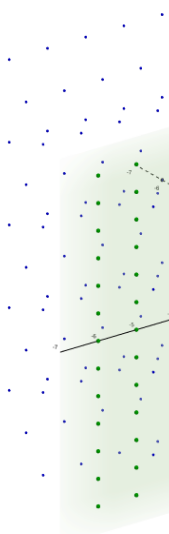
Embedding

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



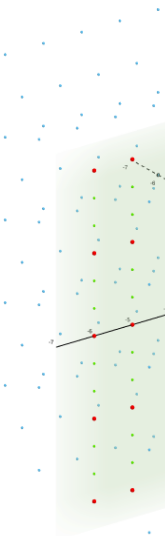
Adding back the quaternion Order

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



An optimal embedding

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



Primitively Oriented Orders

We say that $\iota :$ $\hookrightarrow \mathcal{O}$ is an *optimal embe*

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

Given an embedding $\iota : K \hookrightarrow B_{p\,\infty}$, we ca
-oriented order $\mathcal{O}$, if $\iota(K) \cap \mathcal{O} = \iota(\quad)$.

Correspondence of ideals

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

Given an -ideal $\mathfrak{l}$, we can look at the co

Correspondingly, given a left $\mathcal{O}$-ideal I, w

How are these operations related?

Proposition

Given an invertible -ideal $\mathfrak{l}$ we have that

Given a left $\mathcal{O}$-ideal I we have that $I \supseteq \mathcal{O}\langle$

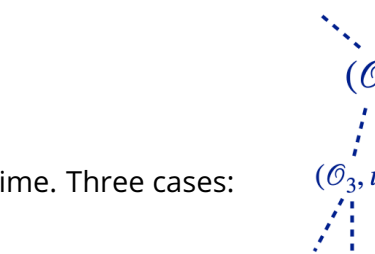
Horizontal and vertical ideals

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:

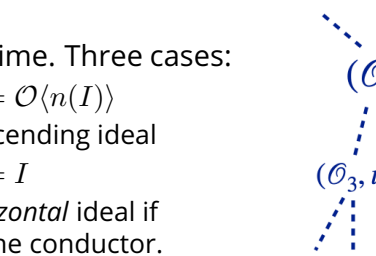
$\mathcal{O}\langle I \cap \iota(K)\rangle = \mathcal{O}\langle n(I)\rangle$

I is a descending ideal

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

I is a *horizontal* ideal if $n(I) \quad f$, the conductor.

I is an *ascending* ideal if $n(I) \mid f$, the conductor.



What is missing?

Given two primitively -oriented maximal or
them.

Vectorization reduces to endomorphism

From [CVP20][1], this was first shown for

Later generalised to *almost* arbitrary ord

Exponential in the number of distinct pr

However, we can *almost* get it “for free”.

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

A new reduction

The new reduction follows from the following

Proposition

Let $(\mathcal{O}_1, \iota), (\mathcal{O}_2, \iota)$ *be two primitively -oriented* I *is horizontal.*

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

Find an element $\beta \in B_{p,\infty}$ such that $(\beta\mathcal{O}_2$

Solve $\beta\iota_2(\omega) \quad \iota_1(\omega)\beta = 0$.

Compute the connecting ideal $I := \mathcal{O}_1\mathcal{O}_2$

Find the solution as $\iota_1(\mathfrak{l}) = I \cap \iota_1(K)$.

Computing equivalent ideals of a g

Computing isogenies of fixed degree d: Comp
look for ideals equivalent to the connecting i

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 seen

Connected to the quaternion embedding

[3] Improved algorithms for finding fixed-degree isoge
curves

Computing equivalent ideals of a g

We are trying to find an ideal equivalent to $\mathcal{O}_0\mathcal{O}$ of norm d.

$\mathcal{O}$ is primitively oriented by , an ideal I of norm d induces a (not necessarily primitive) $\mathbb{Z}+d$ -orientation on $\mathcal{O}_R(I)$

Computing equivalent ideals of a g

$\mathbb{Z}[i]$-or

Important special case: $\mathcal{O}_0$ oriented by $\mathbb{Z}[i]$.

Computed a primitive $\mathbb{Z}[2^5]$-orientation on $\mathcal{O}$.

$\mathbb{Z}[2^5 i]$-

Computing equivalent ideals of a g

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.

$\mathbb{Z}[i]$-o

$\mathbb{Z}[2i]$-o

$\mathbb{Z}[2^2i]$-

$\mathbb{Z}[2^3i]$-

$\mathbb{Z}[2^4i]$-

$\mathbb{Z}[2^5i]$-

Computing equivalent ideals of a g

Later: can compute embeddings of int
whenever $\mathrm{disc}(\quad) < p^{4/3}$.

Corollary: We can compute ideals of nor
they exist (with $\mathcal{O}_0$ special).

In general: computing these ideals of n
embeddings of $\mathbb{Z}[di]$.

For generic $\mathcal{O}_0$, the reduction only works
computing optimal embeddings up to di

Relation to ternary quadratic form

In general the quaternion embedding proble

Wlog. we can assume that $\mathrm{tr}(\ \ ) = 0$, so

Voigt, Chp 22: There is a discriminant-pre

$$\left.\begin{array}{l}\text{Quaternion orders}\\ \text{up to isomorphism}\end{array}\right\} \Leftrightarrow \quad \begin{array}{l}\text{Te}\\ \text{up}\end{array}$$

that can be given by sending $\mathcal{O}$ to the no

i.e. if $\beta_1, \beta_2, \beta_3$ is a basis of $(\mathcal{O})$, the asso
$Q(x, y, z) := \mathrm{nrd}(x\beta_1 + y\beta_2 + z\beta_3)$.

Our case: The quaternion embedding pr
by a positive definite ternary quadratic fo

A very easy special case algorithm

From this point forward, we will think of the e
order $\mathcal{O} \subset B_{p\,\infty}$ and an integer n, find $\in \mathcal{O}$ v
Special case: Let $^2 = \quad 1, \mathbf{j}^2 = \quad p$, and $\mathcal{O} = \mathbb{Z}$

The associated norm form is $Q(x, y, z) =$

Solve it modulo p to find x_0, with $x_0^2 \equiv n$

Find y, z satisfying $y^2 + z^2 = (n \quad (x_0 + kp$
Cornacchia.

Then $= (x_0 + kp) + \mathbf{j}y + \mathbf{k}z$ is a solution

B-b-b-bonus application

Finding a curve oriented by a given order :

When $= \mathbb{Z} + f\mathbb{Z}[i]$, this is solved by Set

Computes a random decending f-isoge
an endomorphism of degree fN with N

For general , another existing algorithm
quaternion side, then standard KLPT + tr

This used to be in Séta's key generation

New algorithm: "as efficient as the first, b

Compute an embedding of $\mathbb{Z} + g$ in $\mathcal{O}$
a optimal embedding of $\mathbb{Z} + g$ into End
Compute the ascending isogeny of degr

The generic case

Given a "random" quaternion order $\mathcal{O}$, compu
$\mathrm{nrd}(\ \ ) = n$.

First result [Wes22]: Computing a reduce
(Really works up to $n < p^{2/3}$).

Again [BKM23]: Techniques applied to th
works conjecturally up to $n < p^{4/5}$.

This summer [ACD23][4]: Generic algorith
cases.

New: Improving previous algorithm up t
orders, not just maximal) with the same
improvements assuming factorisation.

[4] Finding orientations of supersingular elliptic curves

A first algorithm - HNF basis

Given a quaternion order $\mathcal{O}$, compute an ele

This algorithm works with the order in H

$$\mathcal{O} = \langle e_{00} + e_{01} \quad + e$$
$$e_{11} \quad + e$$
$$e$$

Solving for trace and mod p, we get $\quad_0 =$

For increasing k, solve for y, z, such that

solution $\quad_0 + \quad_1$

Improving the HNF basis algorithm

Notice that when $_0$ is set, we are lookin

$$_1 = k \cdot p\beta_2 + y \cdot$$

This defines a new lattice Λ in $B_{p\,\infty}$.

In fact, this lattice Λ is exactly the trace-
$\mathcal{O}$-ideal of norm p.

Whenever $n < p^{4/3}$, we have that $_1$ is th

A new algorithm using a reduced b

For any solution , and any $\beta \in \mathcal{O} \setminus \mathbb{Z}[\ ]$, the t
revealed mod $= \mathrm{discrd}(\mathcal{O})$ (and upper boun

Found by computing the discriminant of

Let $1, \beta_1, \beta_2, \beta_3$ be a reduced basis of $\mathcal{O}$. It
is known exactly, and one finds by soli

Again, for maximal orders, this "usually"

Exploit the fact that this works for any or

Similarity with CVP improvement?

Compute any solution $_0$ with

$$\mathrm{trd}(\ _0\beta_i) = \mathrm{trd}(\ \beta$$

Again: Look for an $_1 :=$ $_0$ in the un

Hence, given any (not necessarily reduce
same complexity by doing a CVP search f

Pathological cases

All these except HNF-algorithm, relies on
somewhat uniform

$1, \beta_1, \beta_2, \beta_3$, with $\mathrm{nrd}(\beta_i) \approx p^{2/3}$

Previous two: Runtime dominated by ma

However, with factorization, we get a run

Again, reduces to solving a principal qua

Unlike the HNF-basis method, there's se
this.

A magic trick

Just like a magic trick, this is as cool as it

Let $p \equiv 11 \pmod{12}$. We compute the sh
and $j(E_2) = 1728$ in the 2-isogeny graph.

A magic trick

Let $p = 2^{55} \cdot 3 \quad 1 \equiv 11 \pmod{12}$. We wor

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

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

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

We want the smallest k such that $\mathbb{Z}[2^k\omega]$

A magic trick

For $k = 54$, we find the embedding

$$\iota(2^{54}\omega) = 9007199254740992 + \frac{19924704230}{2}$$

Translating the ideal $I := \mathcal{O}\langle \iota(2^{54}\omega), 2^{54} \rangle$ t

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

reveals that the point $K \in E_2$ with

$$x(K) = 86739268981076750i + 692$$

generates a 2^{54}-isogeny$\varphi : E_2 \to E_1$ with

Thank you for you