IMPERIAL

On the Spinor Genus and the Distinguishing Lattice Isomorphism Problem

Cong Ling & Jingbo Liu & Andrew Mendelsohn
13/12/2024

Introduction

Lattice Isomorphism Problem: decide if two lattices are isomorphic and if so, find an isomorphism.

Introduction

Lattice Isomorphism Problem: decide if two lattices are isomorphic and if so, find an isomorphism.

'Arithmetic Invariants': (efficiently computable) properties of lattices preserved under isomorphism.

Means: $\mathcal{L}$ and $\mathsf{f}(\mathcal{L})$ share an efficiently computable property.

Introduction

Lattice Isomorphism Problem: decide if two lattices are isomorphic and if so, find an isomorphism.

'Arithmetic Invariants': (efficiently computable) properties of lattices preserved under isomorphism.

Means: $\mathcal{L}$ and f$(\mathcal{L})$ share an efficiently computable property.

Examples:
Class: $\mathcal{L} \sim \mathcal{L}'$ if related by a global isomorphism.
Genus: $\mathcal{L} \sim \mathcal{L}'$ if related by local isomorphisms.

Introduction

Lattice Isomorphism Problem: decide if two lattices are isomorphic and if so, find an isomorphism.

'Arithmetic Invariants': (efficiently computable) properties of lattices preserved under isomorphism.

Means: $\mathcal{L}$ and f$(\mathcal{L})$ share an efficiently computable property.

Examples:
Class: $\mathcal{L} \sim \mathcal{L}'$ if related by a global isomorphism.
Genus: $\mathcal{L} \sim \mathcal{L}'$ if related by local isomorphisms.

Are there more relations? Yes!

In this talk: we discuss when a certain invariant (the 'spinor genus') is useful for solving LIP.

Why? vWD21 developed a KEM and signature scheme from LIP. ALW24 developed PKE.
DPPvW22 developed an optimised signature scheme, HAWK, based on search LIP on rank-2 Hermitian module lattices. Submitted to NIST's PQC standardisation process.

Lattices and their Isomorphisms

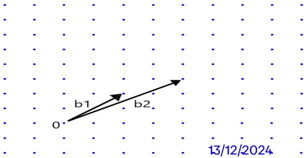
$$\mathcal{L} = \mathcal{L}(B) = \{x : x = \sum_{i=1}^{n} a_i \mathbf{b}_i, a_i \in \mathbb{Z}\}$$

Lattices and their Isomorphisms

$\mathcal{L} = \mathcal{L}(B) = \{x : x = \sum_{i=1}^{n} a_i \mathbf{b}_i, a_i \in \mathbb{Z}\}$

$GL_n(\mathbb{Z}) = \{M \in M_n(\mathbb{Z}) : \det(M) = \pm 1\}$
$O_n(\mathbb{R}) = \{M \in M_n(\mathbb{R}) : M^T M = I_n\}$

Lattice isomorphism: $\mathcal{L} \cong \mathcal{L}' \Leftrightarrow$ there exists $O \in O_n(\mathbb{R}) : \mathcal{L}' = O \cdot \mathcal{L}$.



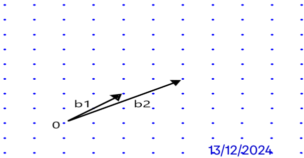
Lattices and their Isomorphisms

$\mathcal{L} = \mathcal{L}(B) = \{x : x = \sum_{i=1}^{n} a_i \mathbf{b}_i, a_i \in \mathbb{Z}\}$

$GL_n(\mathbb{Z}) = \{M \in M_n(\mathbb{Z}) : \det(M) = \pm 1\}$
$O_n(\mathbb{R}) = \{M \in M_n(\mathbb{R}) : M^T M = I_n\}$

Lattice isomorphism: $\mathcal{L} \cong \mathcal{L}' \Leftrightarrow$ there exists $O \in O_n(\mathbb{R}) : \mathcal{L}' = O \cdot \mathcal{L}$.

Classes: $\mathcal{L} \sim \mathcal{L}' \Leftrightarrow \mathcal{L}' \cong \mathcal{L}$.
Then $\{\text{Integer Lattices}\}/\sim$ partitions the set into equivalence classes.
Write $\mathcal{L} \in [\mathcal{L}']$.



Lattices and their Isomorphisms

$\mathcal{L} = \mathcal{L}(B) = \{x : x = \sum_{i=1}^{n} a_i \mathbf{b}_i, a_i \in \mathbb{Z}\}$

$GL_n(\mathbb{Z}) = \{M \in M_n(\mathbb{Z}) : \det(M) = \pm 1\}$
$O_n(\mathbb{R}) = \{M \in M_n(\mathbb{R}) : M^T M = I_n\}$

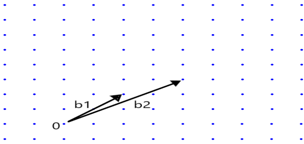
Lattice isomorphism: $\mathcal{L} \cong \mathcal{L}' \Leftrightarrow$ there exists $O \in O_n(\mathbb{R}) : \mathcal{L}' = O \cdot \mathcal{L}$.

Classes: $\mathcal{L} \sim \mathcal{L}' \Leftrightarrow \mathcal{L}' \cong \mathcal{L}$.
Then $\{\text{Integer Lattices}\}/\sim$ partitions the set into equivalence classes.
Write $\mathcal{L} \in [\mathcal{L}']$.

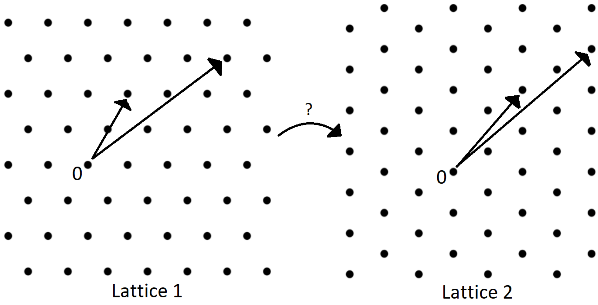
Search LIP: find $U \in GL_n(\mathbb{Z})$ and $O \in O_n(\mathbb{R})$ with $B' = OBU$.
Ask for U since $OB = B' \Rightarrow O = B'B^{-1}$.

Decision LIP: decide if a pair (U, O) exists for $\mathcal{L}, \mathcal{L}'$.

Distinguish LIP: Given $\mathcal{L}_0, \mathcal{L}_1$, and $\mathcal{L} \in [\mathcal{L}_b]$ for uniform $b \in \{0, 1\}$, find b.



Lattice Isomorphism Problems
Pictorially



Quadratic Forms

Quadratic forms/$\mathbb{Z}$: $f(\mathbf{x}) = \sum_{i,j}^{n} f_{ij} x_i x_j$ with $f_{ij} \in \mathbb{Z}$, $f_{ij} = f_{ji}$.
Then $f(\mathbf{x}) = f_{11} x_1^2 + f_{12} x_1 x_2 + \ldots + f_{nn} x_n^2$.

Quadratic Forms

Quadratic forms/$\mathbb{Z}$: $f(\mathbf{x}) = \sum_{i,j}^{n} f_{ij} x_i x_j$ with $f_{ij} \in \mathbb{Z}$, $f_{ij} = f_{ji}$.
Then $f(\mathbf{x}) = f_{11}x_1^2 + f_{12}x_1x_2 + \ldots + f_{nn}x_n^2$.

Alternatively: $f(\mathbf{x}) = \mathbf{x}^T F \mathbf{x}$, with F a symmetric matrix of f.

f and g are equivalent over $\mathbb{Z}$ if $\exists\, U \in GL_n(\mathbb{Z}) : F = U^T G U$.
Then $f \sim_{\mathbb{Z}} g$ or $f \in [g]$ or $f \in \mathrm{class}\, g$.

Quadratic Forms

Quadratic forms/$\mathbb{Z}$: $f(\mathbf{x}) = \sum_{i,j}^{n} f_{ij} x_i x_j$ with $f_{ij} \in \mathbb{Z}$, $f_{ij} = f_{ji}$.
Then $f(\mathbf{x}) = f_{11} x_1^2 + f_{12} x_1 x_2 + \ldots + f_{nn} x_n^2$.

Alternatively: $f(\mathbf{x}) = \mathbf{x}^T F \mathbf{x}$, with F a symmetric matrix of f.

f and g are equivalent over $\mathbb{Z}$ if $\exists\, U \in GL_n(\mathbb{Z}) : F = U^T G U$.
Then $f \sim_{\mathbb{Z}} g$ or $f \in [g]$ or $f \in \mathrm{class}\, g$.

If $B' = OBU$: ${B'}^T B' = (OBU)^T OBU = U^T B^T B U$.
$B^T B$ is symmetric, integral, so corresponds to a quadratic form.
If f a quad. form: $f(\mathbf{x}) = \mathbf{x}^T F \mathbf{x}$; Cholesky $\Rightarrow$ factor $F = B^T B$.

So we can move between quadratic forms and lattices over the integers.

Solving Lattice Isomorphism Problems

Arithmetic Invariants

Decision/Distinguish LIP is easy **if** there are efficiently computable invariants of quadratic forms which differ for forms in distinct classes (i.e. non-isomorphic lattices).

Determinants: $F = U^T G U \Rightarrow \det F = \det U^T \det G \det U = \det G$.

Solving Lattice Isomorphism Problems
Arithmetic Invariants

Decision/Distinguish LIP is easy **if** there are efficiently computable invariants of quadratic forms which differ for forms in distinct classes (i.e. non-isomorphic lattices).

Determinants: $F = U^T G U \Rightarrow \det F = \det U^T \det G \det U = \det G$.

So f, g share 'fingerprint': $(\det, \mathrm{par}, \gcd, \text{equivalence}/\{\mathbb{Q}, \mathbb{R}, \mathbb{Z}_p\})$.

So to instantiate LIP in cryptography, make sure forms have matching fingerprints!

Solving Lattice Isomorphism Problems
Arithmetic Invariants

Decision/Distinguish LIP is easy **if** there are efficiently computable invariants of quadratic forms which differ for forms in distinct classes (i.e. non-isomorphic lattices).

Determinants: $F = U^T G U \Rightarrow \det F = \det U^T \det G \det U = \det G$.

So f, g share 'fingerprint': $(\det, \mathrm{par}, \gcd,$ equivalence/$\{\mathbb{Q}, \mathbb{R}, \mathbb{Z}_p\})$.

So to instantiate LIP in cryptography, make sure forms have matching fingerprints!

We care about the notions of equivalence.

The Genus

Definition: let $\mathbb{Z}_{(p)} = \{\frac{a}{b} | a \in \mathbb{Z}, b \neq 0, \gcd(b, p) = 1\}$.

$$f \in \operatorname{gen} g \text{ iff } F = U_p G U_p^t \text{ for } U_p \in Gl_n(\mathbb{Z}_{(p)}) \text{ for all } p \text{ (and over } \mathbb{R}).^1$$

[1] Alternatively, $U_p \in \mathbb{Z}_p$.

The Genus

Definition: let $\mathbb{Z}_{(p)} = \{\frac{a}{b} | a \in \mathbb{Z}, b \neq 0, \gcd(b, p) = 1\}$.

$$f \in \operatorname{gen} g \text{ iff } F = U_p G U_p^t \text{ for } U_p \in Gl_n(\mathbb{Z}_{(p)}) \text{ for all } p \text{ (and over } \mathbb{R}).$$ [1]

Each genus is a disjoint union of classes. So given f, we have

$$\operatorname{class} f \subset \operatorname{gen} f$$

So given f, g, test if $\operatorname{gen} f = \operatorname{gen} g$; if not, then $\operatorname{class} f \neq \operatorname{class} g$.

[1] Alternatively, $U_p \in \mathbb{Z}_p$.

The Genus

Definition: let $\mathbb{Z}_{(p)} = \{\frac{a}{b} | a \in \mathbb{Z}, b \neq 0, \gcd(b, p) = 1\}$.

$$f \in \operatorname{gen} g \text{ iff } F = U_p G U_p^t \text{ for } U_p \in Gl_n(\mathbb{Z}_{(p)}) \text{ for all } p \text{ (and over } \mathbb{R}).^1$$

Each genus is a disjoint union of classes. So given f, we have

$$\operatorname{class} f \subset \operatorname{gen} f$$

So given f, g, test if $\operatorname{gen} f = \operatorname{gen} g$; if not, then $\operatorname{class} f \neq \operatorname{class} g$.

[BDG23] studies the genus in a cryptographic context.

Q: Are there more equivalence relations on the space of quadratic forms?

[1] Alternatively, $U_p \in \mathbb{Z}_p$.

The Spinor Genus
Overview

There is another equivalence relation on spaces of quadratic forms!

The Spinor Genus
Overview

There is another equivalence relation on spaces of quadratic forms!

Informal description: let V/K be a vector space over a field. Then there is a homomorphism

$$\text{Group of Rotations of } V \to K^\times/(K^\times)^2$$

The kernel is thus a proper normal subgroup of the group of rotations of V.

We can use this normal subgroup applied to V_p to define an equivalence relation on lattices in V.

The Spinor Genus
Overview

There is another equivalence relation on spaces of quadratic forms!

Informal description: let V/K be a vector space over a field. Then there is a homomorphism

$$\text{Group of Rotations of } V \to K^\times/(K^\times)^2$$

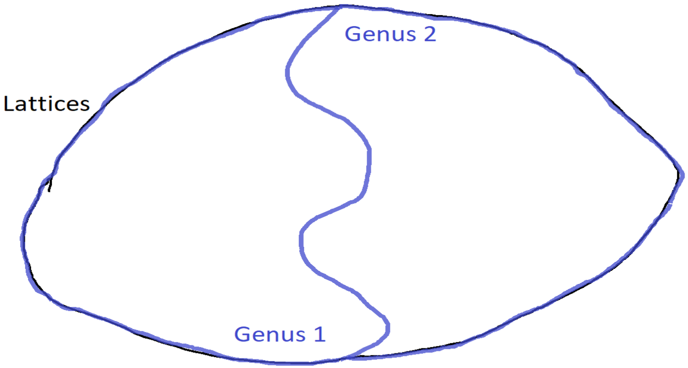
The kernel is thus a proper normal subgroup of the group of rotations of V.

We can use this normal subgroup applied to V_p to define an equivalence relation on lattices in V.

This relation gives a partition finer than the genus but coarser than the class.

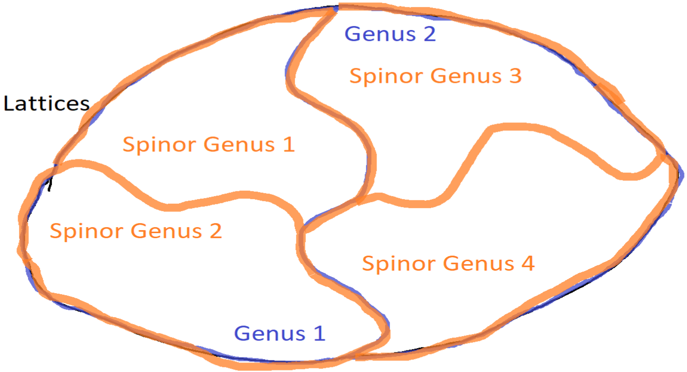
The Spinor Genus

Via Bad Paint Drawings



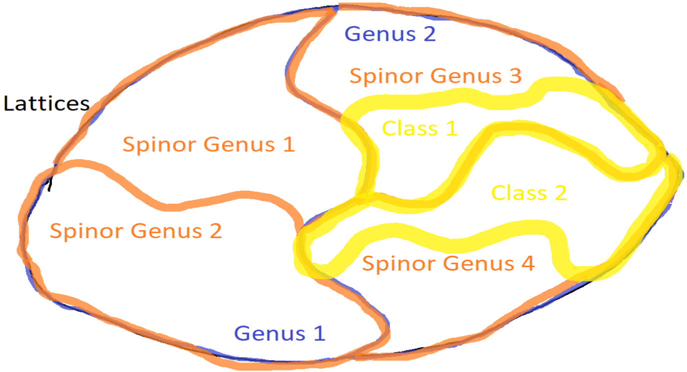
The Spinor Genus

Via Bad Paint Drawings



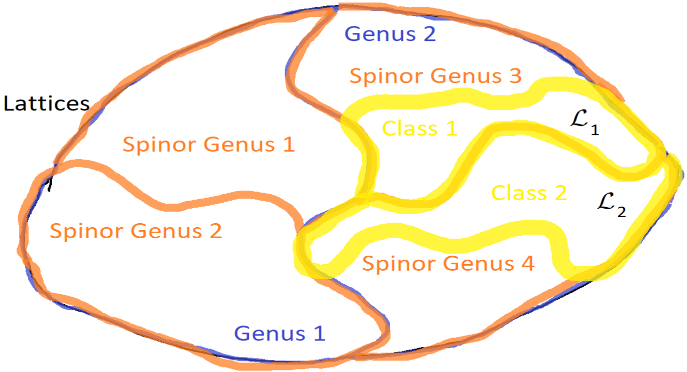
The Spinor Genus

Via Bad Paint Drawings



The Spinor Genus

Via Bad Paint Drawings



The Spinor Genus
Setup

Let K be a number field. Let V/K be a vector space. Lattices live on V, i.e. $\mathcal{L} \subset V$.

The Spinor Genus
Setup

Let K be a number field. Let V/K be a vector space. Lattices live on V, i.e. $\mathcal{L} \subset$ V.

V is equipped with a quadratic form ϕ : V $\to$ K (a ‘quadratic space’).
$\mathsf{O}(\mathsf{V}) = \{\sigma : \mathsf{V} \to \mathsf{V} : \phi(\sigma \mathsf{x}) = \phi(\mathsf{x})\}$
$\mathsf{O}^{+}(\mathsf{V}) = \{\sigma \in \mathsf{O}(\mathsf{V}) : \det \sigma = 1\}$.

The Spinor Genus
Setup

Let K be a number field. Let V/K be a vector space. Lattices live on V, i.e. $\mathcal{L} \subset$ V.

V is equipped with a quadratic form ϕ : V $\to$ K (a 'quadratic space').
$\mathsf{O}(\mathsf{V}) = \{\sigma : \mathsf{V} \to \mathsf{V} : \phi(\sigma \mathsf{x}) = \phi(\mathsf{x})\}$
$\mathsf{O}^+(\mathsf{V}) = \{\sigma \in \mathsf{O}(\mathsf{V}) : \det \sigma = 1\}$.

ϕ is regular if $\det \phi \neq 0$.

ϕ is anisotropic if there is no x $\in$ V $\setminus 0$ such that $\phi(\mathsf{x}) = 0$.

The Spinor Genus
Setup

Let K be a number field. Let V/K be a vector space. Lattices live on V, i.e. $\mathcal{L} \subset V$.

V is equipped with a quadratic form $\phi : V \to K$ (a 'quadratic space').
$O(V) = \{\sigma : V \to V : \phi(\sigma x) = \phi(x)\}$
$O^+(V) = \{\sigma \in O(V) : \det \sigma = 1\}$.

ϕ is regular if $\det \phi \neq 0$.

ϕ is anisotropic if there is no $x \in V \setminus 0$ such that $\phi(x) = 0$.

$\mathcal{L}$ and $\mathcal{L}'$ lie in the same class iff there exists some $\beta \in O(V)$ such that $\mathcal{L}' = \beta\mathcal{L}$.

$\mathcal{L}$ and $\mathcal{L}'$ lie in the same genus iff there exist $\beta_p \in O(V_p)$ such that $\mathcal{L}' = \beta_p\mathcal{L}$ for all primes p.

The Spinor Genus

The Spinor Norm

Set $b(x, y) = \frac{1}{2}\left(\phi(x + y) - \phi(x) - \phi(y)\right)$.
Reflections: an involution τ is a reflection if for all $x \in V$ there is an anisotropic vector $y \in V$ such that

$$\tau(x) = \tau_y(x) := x - \frac{b(x, y)}{\phi(y)} y$$

The Spinor Genus

The Spinor Norm

Set $b(x, y) = \frac{1}{2}(\phi(x + y) - \phi(x) - \phi(y))$.
Reflections: an involution τ is a reflection if for all $x \in V$ there is an anisotropic vector $y \in V$ such that

$$\tau(x) = \tau_y(x) := x - \frac{b(x, y)}{\phi(y)} y$$

Theorem (Cartan-Dieudonné)

If V, ϕ is an n-d regular quadratic space, every element of $O(V)$ is a product of at most n reflections.

The Spinor Genus

The Spinor Norm

Set $b(x, y) = \frac{1}{2}(\phi(x + y) - \phi(x) - \phi(y))$.
Reflections: an involution τ is a reflection if for all $x \in V$ there is an anisotropic vector $y \in V$ such that

$$\tau(x) = \tau_y(x) := x - \frac{b(x, y)}{\phi(y)} y$$

Theorem (Cartan-Dieudonné)

If V, ϕ is an n-d regular quadratic space, every element of $O(V)$ is a product of at most n reflections.

Spinor Norm: Let $\sigma \in O^+(V)$. Then by Cartan-Dieudonné, $\sigma = \prod_i \tau_{y_i}$. The map

$$\theta : O^+(V) \to K^\times/(K^\times)^2, \ \sigma \mapsto \prod_i \phi(y_i)$$

is a multiplicative homomorphism called the spinor norm. Let $\Theta(V) := \ker \theta \trianglelefteq O^+(V)$.

The Spinor Genus

The Spinor Norm

Set $b(x, y) = \frac{1}{2}(\phi(x + y) - \phi(x) - \phi(y))$.
Reflections: an involution τ is a reflection if for all $x \in V$ there is an anisotropic vector $y \in V$ such that

$$\tau(x) = \tau_y(x) := x - \frac{b(x, y)}{\phi(y)}y$$

Theorem (Cartan-Dieudonné)

If V, ϕ is an n-d regular quadratic space, every element of $O(V)$ is a product of at most n reflections.

Spinor Norm: Let $\sigma \in O^+(V)$. Then by Cartan-Dieudonné, $\sigma = \prod_i \tau_{y_i}$. The map

$$\theta : O^+(V) \to K^\times/(K^\times)^2,\ \sigma \mapsto \prod_i \phi(y_i)$$

is a multiplicative homomorphism called the spinor norm. Let $\Theta(V) := \ker \theta \trianglelefteq O^+(V)$.

We will apply this to define an equivalence relation using localisations V_p, like the genus.

The Spinor Genus

Equivalence using $\ker\theta = \Theta(\mathsf{V}_\mathsf{p}) \trianglelefteq \mathsf{O}^+(\mathsf{V}_\mathsf{p})$

Definition: $\mathcal{L}$ and $\mathcal{L}'$ satisfy $\mathsf{S}(\mathcal{L}, \mathcal{L}')$ if there exist $\gamma \in \mathsf{O}^+(\mathsf{V})$ and $\delta_\mathsf{p} \in \Theta(\mathsf{V}_\mathsf{p})$: $\mathcal{L}' = \gamma\delta_\mathsf{p}\mathcal{L} \,\forall\, \mathsf{p}$.

This relation is an equivalence relation intermediate to the class and genus.

The Spinor Genus

Equivalence using $\ker\theta = \Theta(\mathsf{V_p}) \trianglelefteq \mathsf{O}^+(\mathsf{V_p})$

Definition: $\mathcal{L}$ and $\mathcal{L}'$ satisfy $\mathsf{S}(\mathcal{L}, \mathcal{L}')$ if there exist $\gamma \in \mathsf{O}^+(\mathsf{V})$ and $\delta_\mathsf{p} \in \Theta(\mathsf{V_p})$: $\mathcal{L}' = \gamma\delta_\mathsf{p}\mathcal{L}\ \forall$ p.

This relation is an equivalence relation intermediate to the class and genus.

Transitivity: suppose $\mathcal{L}, \mathcal{L}', \mathcal{L}''$ satisfy $\mathsf{S}(\mathcal{L}, \mathcal{L}')$ and $\mathsf{S}(\mathcal{L}', \mathcal{L}'')$. Then there are $\gamma_1, \gamma_2 \in \mathsf{O}^+(\mathsf{V})$ and $\beta_{1\mathsf{p}}, \beta_{2\mathsf{p}} \in \Theta(\mathsf{V_p})$ such that $\mathcal{L} = \gamma_1\beta_{1\mathsf{p}}\mathcal{L}'$ and $\mathcal{L}' = \gamma_2\beta_{2\mathsf{p}}\mathcal{L}''$ for each prime p. Combining these,

$$\mathcal{L} = \gamma_1\beta_{1\mathsf{p}}\gamma_2\beta_{2\mathsf{p}}\mathcal{L}'' = (\gamma_1\gamma_2)(\gamma_2^{-1}\beta_{1\mathsf{p}}\gamma_2\beta_{2\mathsf{p}})\mathcal{L}''$$

for each prime p. Since $\gamma_1\gamma_2 \in \mathsf{O}^+(\mathsf{V})$ and $\gamma_2^{-1}\beta_{1\mathsf{p}}\gamma_2\beta_{2\mathsf{p}} \in \Theta(\mathsf{V_p})$, $\mathsf{S}(\mathcal{L}, \mathcal{L}'')$ holds.

The Spinor Genus

Equivalence using $\ker\theta = \Theta(\mathsf{V_p}) \trianglelefteq \mathsf{O}^+(\mathsf{V_p})$

Definition: $\mathcal{L}$ and $\mathcal{L}'$ satisfy $\mathsf{S}(\mathcal{L}, \mathcal{L}')$ if there exist $\gamma \in \mathsf{O}^+(\mathsf{V})$ and $\delta_\mathsf{p} \in \Theta(\mathsf{V_p})$: $\mathcal{L}' = \gamma\delta_\mathsf{p}\mathcal{L} \,\forall$ p.

This relation is an equivalence relation intermediate to the class and genus.

Transitivity: suppose $\mathcal{L}, \mathcal{L}', \mathcal{L}''$ satisfy $\mathsf{S}(\mathcal{L}, \mathcal{L}')$ and $\mathsf{S}(\mathcal{L}', \mathcal{L}'')$. Then there are $\gamma_1, \gamma_2 \in \mathsf{O}^+(\mathsf{V})$ and $\beta_{1\mathsf{p}}, \beta_{2\mathsf{p}} \in \Theta(\mathsf{V_p})$ such that $\mathcal{L} = \gamma_1\beta_{1\mathsf{p}}\mathcal{L}'$ and $\mathcal{L}' = \gamma_2\beta_{2\mathsf{p}}\mathcal{L}''$ for each prime p. Combining these,

$$\mathcal{L} = \gamma_1\beta_{1\mathsf{p}}\gamma_2\beta_{2\mathsf{p}}\mathcal{L}'' = (\gamma_1\gamma_2)(\gamma_2^{-1}\beta_{1\mathsf{p}}\gamma_2\beta_{2\mathsf{p}})\mathcal{L}''$$

for each prime p. Since $\gamma_1\gamma_2 \in \mathsf{O}^+(\mathsf{V})$ and $\gamma_2^{-1}\beta_{1\mathsf{p}}\gamma_2\beta_{2\mathsf{p}} \in \Theta(\mathsf{V_p})$, $\mathsf{S}(\mathcal{L}, \mathcal{L}'')$ holds.

Spinor Genera: the equivalence classes $\{\text{Lattices on V}\}/\mathsf{S}$. If $\mathsf{S}(\mathcal{L}, \mathcal{L}')$ holds, write $\mathcal{L} \in \operatorname{spn}(\mathcal{L}')$.

The Spinor Genus

Equivalence using $\ker\theta = \Theta(\mathsf{V_p}) \trianglelefteq \mathsf{O}^+(\mathsf{V_p})$

Definition: $\mathcal{L}$ and $\mathcal{L}'$ satisfy $\mathsf{S}(\mathcal{L}, \mathcal{L}')$ if there exist $\gamma \in \mathsf{O}^+(\mathsf{V})$ and $\delta_\mathsf{p} \in \Theta(\mathsf{V_p})$: $\mathcal{L}' = \gamma\delta_\mathsf{p}\mathcal{L} \,\forall$ p.

This relation is an equivalence relation intermediate to the class and genus.

Transitivity: suppose $\mathcal{L}, \mathcal{L}', \mathcal{L}''$ satisfy $\mathsf{S}(\mathcal{L}, \mathcal{L}')$ and $\mathsf{S}(\mathcal{L}', \mathcal{L}'')$. Then there are $\gamma_1, \gamma_2 \in \mathsf{O}^+(\mathsf{V})$ and $\beta_{1\mathsf{p}}, \beta_{2\mathsf{p}} \in \Theta(\mathsf{V_p})$ such that $\mathcal{L} = \gamma_1\beta_{1\mathsf{p}}\mathcal{L}'$ and $\mathcal{L}' = \gamma_2\beta_{2\mathsf{p}}\mathcal{L}''$ for each prime p. Combining these,

$$\mathcal{L} = \gamma_1\beta_{1\mathsf{p}}\gamma_2\beta_{2\mathsf{p}}\mathcal{L}'' = (\gamma_1\gamma_2)(\gamma_2^{-1}\beta_{1\mathsf{p}}\gamma_2\beta_{2\mathsf{p}})\mathcal{L}''$$

for each prime p. Since $\gamma_1\gamma_2 \in \mathsf{O}^+(\mathsf{V})$ and $\gamma_2^{-1}\beta_{1\mathsf{p}}\gamma_2\beta_{2\mathsf{p}} \in \Theta(\mathsf{V_p})$, $\mathsf{S}(\mathcal{L}, \mathcal{L}'')$ holds.

Spinor Genera: the equivalence classes $\{$Lattices on V$\}/\mathsf{S}$. If $\mathsf{S}(\mathcal{L}, \mathcal{L}')$ holds, write $\mathcal{L} \in \mathrm{spn}(\mathcal{L}')$.

Lemma (Cassels)

1. The number of spinor genera in any genus is finite and a power of 2.
2. For all $\mathsf{n} \geq 3$ there exist lattices whose genus contains multiple spinor genera.
3. If (V, ϕ) has dimension $\mathsf{n} \geq 3$, $\mathcal{L} \subset$ V, ϕ takes integral values on $\mathcal{L}$, and $\mathrm{gen}(\mathcal{L})$ contains multiple spinor genera, then either there exists $\mathsf{p} > 2$: $\mathsf{p}^{\frac{\mathsf{n}(\mathsf{n}-1)}{2}} \mid \det(\mathcal{L})$, or $2^{\mathsf{n}(\mathsf{n}-3)/2+\lfloor(\mathsf{n}+1)/2\rfloor} \mid \det(\mathcal{L})$.

The Spinor Genus: Binary Case over the Integers

Consider primitive integral binary quadratic forms f, g over $\mathbb{Z}$.

EstesPall73, Theorem: If f and g are in the same genus, f and g are in the same spinor genus if and only if $\mathsf{f} = \mathsf{g}\mathsf{k}^4$ for some k, under Gauss composition.

Equivalently for lattices, $\mathcal{L}$ and $\mathcal{L}'$ are in the same spinor genus iff $\mathcal{L}'^{-1}\mathcal{L} \in \mathcal{C}(\mathcal{O}_{\mathsf{l}}(\mathcal{L}'))^4$.

The Spinor Genus: Binary Case over the Integers

Consider primitive integral binary quadratic forms f, g over $\mathbb{Z}$.

EstesPall73, Theorem: If f and g are in the same genus, f and g are in the same spinor genus if and only if $\mathsf{f} = \mathsf{g}\mathsf{k}^4$ for some k, under Gauss composition.

Equivalently for lattices, $\mathcal{L}$ and $\mathcal{L}'$ are in the same spinor genus iff $\mathcal{L}'^{-1}\mathcal{L} \in \mathcal{C}(\mathcal{O}_{\mathsf{l}}(\mathcal{L}'))^4$.

Q: can we extend this to forms over number fields? And can it be computed efficiently?

The Spinor Genus: Binary Case over the Integers

Consider primitive integral binary quadratic forms f, g over $\mathbb{Z}$.

EstesPall73, Theorem: If f and g are in the same genus, f and g are in the same spinor genus if and only if $\mathsf{f} = \mathsf{g}\mathsf{k}^4$ for some k, under Gauss composition.

Equivalently for lattices, $\mathcal{L}$ and $\mathcal{L}'$ are in the same spinor genus iff $\mathcal{L}'^{-1}\mathcal{L} \in \mathcal{C}(\mathcal{O}_\mathsf{l}(\mathcal{L}'))^4$.

Q: can we extend this to forms over number fields? And can it be computed efficiently?

Theorem (BiasseSong16, Class Group Quantum Computation)

Under GRH there is a quantum algorithm for computing the class group of an order $\mathcal{O}$ in a number field K which runs in polynomial time in $\mathsf{n} = \deg(\mathsf{K})$ and $\log(|\Delta|)$, where Δ is the discriminant of $\mathcal{O}$.

The Spinor Genus: Binary Case over Number Fields

Ingredients for a Quantum Algorithm

f, g anisotropic binary quadratic forms over $\mathcal{O}_F \Rightarrow f, g$ correspond to lattices of rank 2 over $\mathcal{O}_F$ in V.
V is a regular binary quadratic space over a number field F.
Fix a basis such that $V \cong F(\sqrt{-d})$ for some d. Write $\mathcal{O}_V$ for the ring of integers of $F(\sqrt{-d})$.

The Spinor Genus: Binary Case over Number Fields

Ingredients for a Quantum Algorithm

f, g anisotropic binary quadratic forms over $\mathcal{O}_F \Rightarrow f, g$ correspond to lattices of rank 2 over $\mathcal{O}_F$ in V.
V is a regular binary quadratic space over a number field F.
Fix a basis such that $V \cong F(\sqrt{-d})$ for some d. Write $\mathcal{O}_V$ for the ring of integers of $F(\sqrt{-d})$.
Recall the left order is $\mathcal{O}_l(\mathcal{L}_2) := \{x \in V : x\mathcal{L}_2 \subset \mathcal{L}_2\} \subset V$, and a lattice is a left ideal in its left order.

The Spinor Genus: Binary Case over Number Fields

Ingredients for a Quantum Algorithm

f, g anisotropic binary quadratic forms over $\mathcal{O}_F \Rightarrow f, g$ correspond to lattices of rank 2 over $\mathcal{O}_F$ in V.
V is a regular binary quadratic space over a number field F.
Fix a basis such that $V \cong F(\sqrt{-d})$ for some d. Write $\mathcal{O}_V$ for the ring of integers of $F(\sqrt{-d})$.
Recall the left order is $\mathcal{O}_l(\mathcal{L}_2) := \{x \in V : x\mathcal{L}_2 \subset \mathcal{L}_2\} \subset V$, and a lattice is a left ideal in its left order.

Lemma (EarnestEstes80)

A necessary and sufficient condition that $\mathcal{L}_1$ be in $\mathrm{spn}(\mathcal{L}_2)$ is that $\mathcal{L}_1\mathcal{L}_2^{-1}$ be in $\mathrm{spn}\left(\mathcal{O}_l(\mathcal{L}_2)\right)$.

The Spinor Genus: Binary Case over Number Fields

Ingredients for a Quantum Algorithm

f, g anisotropic binary quadratic forms over $\mathcal{O}_F \Rightarrow f, g$ correspond to lattices of rank 2 over $\mathcal{O}_F$ in V.
V is a regular binary quadratic space over a number field F.
Fix a basis such that $V \cong F(\sqrt{-d})$ for some d. Write $\mathcal{O}_V$ for the ring of integers of $F(\sqrt{-d})$.
Recall the left order is $\mathcal{O}_l(\mathcal{L}_2) := \{x \in V : x\mathcal{L}_2 \subset \mathcal{L}_2\} \subset V$, and a lattice is a left ideal in its left order.

Lemma (EarnestEstes80)

A necessary and sufficient condition that $\mathcal{L}_1$ be in $\operatorname{spn}(\mathcal{L}_2)$ is that $\mathcal{L}_1\mathcal{L}_2^{-1}$ be in $\operatorname{spn}(\mathcal{O}_l(\mathcal{L}_2))$.

Set $\mathcal{H}(\mathcal{O}) = \operatorname{gen}(\mathcal{O})/\operatorname{spn}(\mathcal{O})$. For an $\mathcal{O}_F$-order $\mathcal{O} \subset V$, let $\mathcal{I}(\mathcal{O}) =$ group of invertible frac. $\mathcal{O}$-ideals, and $\mathcal{P}(\mathcal{O}) =$ subgroup of principal invertible frac. ideals. Set $\mathcal{C}(\mathcal{O}) = \mathcal{I}(\mathcal{O})/\mathcal{P}(\mathcal{O})$.

The Spinor Genus: Binary Case over Number Fields

Ingredients for a Quantum Algorithm

f, g anisotropic binary quadratic forms over $\mathcal{O}_F \Rightarrow f, g$ correspond to lattices of rank 2 over $\mathcal{O}_F$ in V.
V is a regular binary quadratic space over a number field F.
Fix a basis such that $V \cong F(\sqrt{-d})$ for some d. Write $\mathcal{O}_V$ for the ring of integers of $F(\sqrt{-d})$.
Recall the left order is $\mathcal{O}_l(\mathcal{L}_2) := \{x \in V : x\mathcal{L}_2 \subset \mathcal{L}_2\} \subset V$, and a lattice is a left ideal in its left order.

Lemma (EarnestEstes80)

A necessary and sufficient condition that $\mathcal{L}_1$ be in $\mathrm{spn}(\mathcal{L}_2)$ is that $\mathcal{L}_1\mathcal{L}_2^{-1}$ be in $\mathrm{spn}\left(\mathcal{O}_l(\mathcal{L}_2)\right)$.

Set $\mathcal{H}(\mathcal{O}) = \mathrm{gen}(\mathcal{O})/\mathrm{spn}(\mathcal{O})$. For an $\mathcal{O}_F$-order $\mathcal{O} \subset V$, let $\mathcal{I}(\mathcal{O}) =$ group of invertible frac. $\mathcal{O}$-ideals, and $\mathcal{P}(\mathcal{O}) =$ subgroup of principal invertible frac. ideals. Set $\mathcal{C}(\mathcal{O}) = \mathcal{I}(\mathcal{O})/\mathcal{P}(\mathcal{O})$.

Lemma (EarnestEstes81)

Let F be a number field and $\mathcal{O}_F$ a PID. Let $\mathcal{O}$ be a degree 2 order over $\mathcal{O}_F$. Then $\mathcal{H}(\mathcal{O}) \cong \mathcal{C}(\mathcal{O})^2/\mathcal{C}(\mathcal{O})^4$.

The Spinor Genus: Binary Case over Number Fields

Ingredients for a Quantum Algorithm

f, g anisotropic binary quadratic forms over $\mathcal{O}_\mathsf{F} \Rightarrow \mathsf{f}, \mathsf{g}$ correspond to lattices of rank 2 over $\mathcal{O}_\mathsf{F}$ in V.
V is a regular binary quadratic space over a number field F.
Fix a basis such that $\mathsf{V} \cong \mathsf{F}(\sqrt{-\mathsf{d}})$ for some d. Write $\mathcal{O}_\mathsf{V}$ for the ring of integers of $\mathsf{F}(\sqrt{-\mathsf{d}})$.
Recall the left order is $\mathcal{O}_\mathsf{l}(\mathcal{L}_2) := \{\mathsf{x} \in \mathsf{V} : \mathsf{x}\mathcal{L}_2 \subset \mathcal{L}_2\} \subset \mathsf{V}$, and a lattice is a left ideal in its left order.

Lemma (EarnestEstes80)

A necessary and sufficient condition that $\mathcal{L}_1$ be in $\mathrm{spn}(\mathcal{L}_2)$ is that $\mathcal{L}_1\mathcal{L}_2^{-1}$ be in $\mathrm{spn}\left(\mathcal{O}_\mathsf{l}(\mathcal{L}_2)\right)$.

Set $\mathcal{H}(\mathcal{O}) = \mathrm{gen}(\mathcal{O})/\mathrm{spn}(\mathcal{O})$. For an $\mathcal{O}_\mathsf{F}$-order $\mathcal{O} \subset \mathsf{V}$, let $\mathcal{I}(\mathcal{O}) =$ group of invertible frac. $\mathcal{O}$-ideals, and $\mathcal{P}(\mathcal{O}) =$ subgroup of principal invertible frac. ideals. Set $\mathcal{C}(\mathcal{O}) = \mathcal{I}(\mathcal{O})/\mathcal{P}(\mathcal{O})$.

Lemma (EarnestEstes81)

Let F be a number field and $\mathcal{O}_\mathsf{F}$ a PID. Let $\mathcal{O}$ be a degree 2 order over $\mathcal{O}_\mathsf{F}$. Then $\mathcal{H}(\mathcal{O}) \cong \mathcal{C}(\mathcal{O})^2/\mathcal{C}(\mathcal{O})^4$.

So $\mathrm{spn}(\mathcal{O})/\mathrm{cls}^+(\mathcal{O}) \cong \mathcal{C}(\mathcal{O})^4$, and lattices $\mathcal{L}_1, \mathcal{L}_2 \subset \mathsf{V}$ in the same genus are in the same proper spinor genus iff $\mathcal{L}_1\mathcal{L}_2^{-1}$ is a quartic residue in the class group of the left order of $\mathcal{L}_2$ in V.

The Spinor Genus: Binary Case over Number Fields

Theorem

Let $\mathcal{O}_{\mathsf{F}}$ be a PID. Let f, g be anisotropic integral binary quadratic forms over $\mathcal{O}_{\mathsf{F}}$ in the same genus. Let V be the quadratic space containing $\mathcal{L}_{\mathsf{f}}$, $\mathcal{L}_{\mathsf{g}}$. Then $\mathcal{L}_{\mathsf{f}} \cdot \mathcal{L}_{\mathsf{g}}^{-1}$ generates an ideal coprime to the conductor of $\mathcal{O}_{\mathsf{l}}(\mathcal{L}_{\mathsf{g}})$ in $\mathcal{O}_{\mathsf{V}} \Rightarrow$ a quantum poly. time algorithm to decide if f $\in \mathrm{spn}(\mathsf{g})$.

The Spinor Genus: Binary Case over Number Fields

Theorem

Let $\mathcal{O}_\mathsf{F}$ be a PID. Let f, g be anisotropic integral binary quadratic forms over $\mathcal{O}_\mathsf{F}$ in the same genus. Let V be the quadratic space containing $\mathcal{L}_\mathsf{f}$, $\mathcal{L}_\mathsf{g}$. Then $\mathcal{L}_\mathsf{f} \cdot \mathcal{L}_\mathsf{g}^{-1}$ generates an ideal coprime to the conductor of $\mathcal{O}_\mathsf{l}(\mathcal{L}_\mathsf{g})$ in $\mathcal{O}_\mathsf{V}$ $\Rightarrow$ a quantum poly. time algorithm to decide if f $\in \mathrm{spn}(\mathsf{g})$.

Proof, simple case: $\mathcal{O}_\mathsf{l}(\mathcal{L}_\mathsf{g})$ is a maximal order.

1. f, g are anisotropic $\Rightarrow$ V is isomorphic to a quadratic field extension of F.
Compute a basis of $\mathcal{O}_\mathsf{l}(\mathcal{L}_\mathsf{g})$ and so compute the class group, obtaining a generating set of prime ideals for $\mathcal{C}(\mathcal{O}_\mathsf{l}(\mathcal{L}_\mathsf{g}))$ in quantum poly. time + their defining relations.

The Spinor Genus: Binary Case over Number Fields

Theorem

Let $\mathcal{O}_F$ be a PID. Let f, g be anisotropic integral binary quadratic forms over $\mathcal{O}_F$ in the same genus. Let V be the quadratic space containing $\mathcal{L}_f$, $\mathcal{L}_g$. Then $\mathcal{L}_f \cdot \mathcal{L}_g^{-1}$ generates an ideal coprime to the conductor of $\mathcal{O}_l(\mathcal{L}_g)$ in $\mathcal{O}_V \Rightarrow$ a quantum poly. time algorithm to decide if f $\in \mathrm{spn}(g)$.

Proof, simple case: $\mathcal{O}_l(\mathcal{L}_g)$ is a maximal order.

1. f, g are anisotropic $\Rightarrow$ V is isomorphic to a quadratic field extension of F.
Compute a basis of $\mathcal{O}_l(\mathcal{L}_g)$ and so compute the class group, obtaining a generating set of prime ideals for $\mathcal{C}(\mathcal{O}_l(\mathcal{L}_g))$ in quantum poly. time + their defining relations.
2. The relations form a lattice Λ, and $\mathcal{C}(\mathcal{O}_l(\mathcal{L}_g)) \cong \mathbb{Z}^n/\Lambda$ via $\mathcal{I} \mapsto (e_1, \ldots, e_n) + \Lambda$ for $\mathcal{I} = \prod_{i=1}^n \mathfrak{p}_i^{e_i}$.

The Spinor Genus: Binary Case over Number Fields

Theorem

Let $\mathcal{O}_F$ be a PID. Let f, g be anisotropic integral binary quadratic forms over $\mathcal{O}_F$ in the same genus. Let V be the quadratic space containing $\mathcal{L}_f, \mathcal{L}_g$. Then $\mathcal{L}_f \cdot \mathcal{L}_g^{-1}$ generates an ideal coprime to the conductor of $\mathcal{O}_l(\mathcal{L}_g)$ in $\mathcal{O}_V \Rightarrow$ a quantum poly. time algorithm to decide if $f \in \mathrm{spn}(g)$.

Proof, simple case: $\mathcal{O}_l(\mathcal{L}_g)$ is a maximal order.

1. f, g are anisotropic $\Rightarrow$ V is isomorphic to a quadratic field extension of F. Compute a basis of $\mathcal{O}_l(\mathcal{L}_g)$ and so compute the class group, obtaining a generating set of prime ideals for $\mathcal{C}(\mathcal{O}_l(\mathcal{L}_g))$ in quantum poly. time + their defining relations.
2. The relations form a lattice Λ, and $\mathcal{C}(\mathcal{O}_l(\mathcal{L}_g)) \cong \mathbb{Z}^n/\Lambda$ via $\mathcal{I} \mapsto (e_1, ..., e_n) + \Lambda$ for $\mathcal{I} = \prod_{i=1}^n \mathfrak{p}_i^{e_i}$.
3. $\mathbb{Z}^n/\Lambda$ is an abelian group $\Rightarrow \mathcal{C}(\mathcal{O}_l(\mathcal{L}_g)) \cong \oplus_i \mathbb{Z}/d_i\mathbb{Z}$ for some integers d_i, where the factors d_i are obtained by the quantum algorithm. We want the image of $\mathcal{L}_f \cdot \mathcal{L}_g^{-1}$ in $\oplus_i \mathbb{Z}/d_i\mathbb{Z}$.

The Spinor Genus: Binary Case over Number Fields

Theorem

Let $\mathcal{O}_F$ be a PID. Let f, g be anisotropic integral binary quadratic forms over $\mathcal{O}_F$ in the same genus. Let V be the quadratic space containing $\mathcal{L}_f$, $\mathcal{L}_g$. Then $\mathcal{L}_f \cdot \mathcal{L}_g^{-1}$ generates an ideal coprime to the conductor of $\mathcal{O}_l(\mathcal{L}_g)$ in $\mathcal{O}_V \Rightarrow$ a quantum poly. time algorithm to decide if $f \in \mathrm{spn}(g)$.

Proof, simple case: $\mathcal{O}_l(\mathcal{L}_g)$ is a maximal order.

1. f, g are anisotropic $\Rightarrow$ V is isomorphic to a quadratic field extension of F.
Compute a basis of $\mathcal{O}_l(\mathcal{L}_g)$ and so compute the class group, obtaining a generating set of prime ideals for $\mathcal{C}(\mathcal{O}_l(\mathcal{L}_g))$ in quantum poly. time + their defining relations.
2. The relations form a lattice Λ, and $\mathcal{C}(\mathcal{O}_l(\mathcal{L}_g)) \cong \mathbb{Z}^n/\Lambda$ via $\mathcal{I} \mapsto (e_1, ..., e_n) + \Lambda$ for $\mathcal{I} = \prod_{i=1}^n \mathfrak{p}_i^{e_i}$.
3. $\mathbb{Z}^n/\Lambda$ is an abelian group $\Rightarrow \mathcal{C}(\mathcal{O}_l(\mathcal{L}_g)) \cong \oplus_i \mathbb{Z}/d_i\mathbb{Z}$ for some integers d_i, where the factors d_i are obtained by the quantum algorithm. We want the image of $\mathcal{L}_f \cdot \mathcal{L}_g^{-1}$ in $\oplus_i \mathbb{Z}/d_i\mathbb{Z}$.
4. $\mathcal{O}_l(\mathcal{L}_g)$ a maximal order $\Rightarrow$ can write $\mathcal{L}_f \cdot \mathcal{L}_g^{-1}$ as a product of primes in our generating set, reduced mod the relations between the prime ideals. Map $\mathcal{L}_f \cdot \mathcal{L}_g^{-1} \mapsto (f_1, ..., f_n) + \Lambda$ for some exponents f_i.

The Spinor Genus: Binary Case over Number Fields

Theorem

Let $\mathcal{O}_F$ be a PID. Let f, g be anisotropic integral binary quadratic forms over $\mathcal{O}_F$ in the same genus. Let V be the quadratic space containing $\mathcal{L}_f$, $\mathcal{L}_g$. Then $\mathcal{L}_f \cdot \mathcal{L}_g^{-1}$ generates an ideal coprime to the conductor of $\mathcal{O}_l(\mathcal{L}_g)$ in $\mathcal{O}_V \Rightarrow$ a quantum poly. time algorithm to decide if $f \in \mathrm{spn}(g)$.

Proof, simple case: $\mathcal{O}_l(\mathcal{L}_g)$ is a maximal order.

1. f, g are anisotropic $\Rightarrow$ V is isomorphic to a quadratic field extension of F.
Compute a basis of $\mathcal{O}_l(\mathcal{L}_g)$ and so compute the class group, obtaining a generating set of prime ideals for $\mathcal{C}(\mathcal{O}_l(\mathcal{L}_g))$ in quantum poly. time + their defining relations.
2. The relations form a lattice Λ, and $\mathcal{C}(\mathcal{O}_l(\mathcal{L}_g)) \cong \mathbb{Z}^n/\Lambda$ via $\mathcal{I} \mapsto (e_1, ..., e_n) + \Lambda$ for $\mathcal{I} = \prod_{i=1}^{n} \mathfrak{p}_i^{e_i}$.
3. $\mathbb{Z}^n/\Lambda$ is an abelian group $\Rightarrow \mathcal{C}(\mathcal{O}_l(\mathcal{L}_g)) \cong \oplus_i \mathbb{Z}/d_i\mathbb{Z}$ for some integers d_i, where the factors d_i are obtained by the quantum algorithm. We want the image of $\mathcal{L}_f \cdot \mathcal{L}_g^{-1}$ in $\oplus_i \mathbb{Z}/d_i\mathbb{Z}$.
4. $\mathcal{O}_l(\mathcal{L}_g)$ a maximal order $\Rightarrow$ can write $\mathcal{L}_f \cdot \mathcal{L}_g^{-1}$ as a product of primes in our generating set, reduced mod the relations between the prime ideals. Map $\mathcal{L}_f \cdot \mathcal{L}_g^{-1} \mapsto (f_1, ..., f_n) + \Lambda$ for some exponents f_i.
5. The algorithm also outputs vectors $\overline{g}_i$ of order d_i which form a basis of $\mathbb{Z}^n/\Lambda \cong \oplus_i \mathbb{Z}/d_i\mathbb{Z}$ [Cohen].

The Spinor Genus: Binary Case over Number Fields

Theorem

Let $\mathcal{O}_F$ be a PID. Let f, g be anisotropic integral binary quadratic forms over $\mathcal{O}_F$ in the same genus. Let V be the quadratic space containing $\mathcal{L}_f$, $\mathcal{L}_g$. Then $\mathcal{L}_f \cdot \mathcal{L}_g^{-1}$ generates an ideal coprime to the conductor of $\mathcal{O}_l(\mathcal{L}_g)$ in $\mathcal{O}_V$ $\Rightarrow$ a quantum poly. time algorithm to decide if $f \in \mathrm{spn}(g)$.

Proof, simple case: $\mathcal{O}_l(\mathcal{L}_g)$ is a maximal order.

1. f, g are anisotropic $\Rightarrow$ V is isomorphic to a quadratic field extension of F. Compute a basis of $\mathcal{O}_l(\mathcal{L}_g)$ and so compute the class group, obtaining a generating set of prime ideals for $\mathcal{C}(\mathcal{O}_l(\mathcal{L}_g))$ in quantum poly. time + their defining relations.
2. The relations form a lattice Λ, and $\mathcal{C}(\mathcal{O}_l(\mathcal{L}_g)) \cong \mathbb{Z}^n/\Lambda$ via $\mathcal{I} \mapsto (e_1, \ldots, e_n) + \Lambda$ for $\mathcal{I} = \prod_{i=1}^n \mathfrak{p}_i^{e_i}$.
3. $\mathbb{Z}^n/\Lambda$ is an abelian group $\Rightarrow$ $\mathcal{C}(\mathcal{O}_l(\mathcal{L}_g)) \cong \oplus_i \mathbb{Z}/d_i\mathbb{Z}$ for some integers d_i, where the factors d_i are obtained by the quantum algorithm. We want the image of $\mathcal{L}_f \cdot \mathcal{L}_g^{-1}$ in $\oplus_i \mathbb{Z}/d_i\mathbb{Z}$.
4. $\mathcal{O}_l(\mathcal{L}_g)$ a maximal order $\Rightarrow$ can write $\mathcal{L}_f \cdot \mathcal{L}_g^{-1}$ as a product of primes in our generating set, reduced mod the relations between the prime ideals. Map $\mathcal{L}_f \cdot \mathcal{L}_g^{-1} \mapsto (f_1, \ldots, f_n) + \Lambda$ for some exponents f_i.
5. The algorithm also outputs vectors $\overline{g}_i$ of order d_i which form a basis of $\mathbb{Z}^n/\Lambda \cong \oplus_i \mathbb{Z}/d_i\mathbb{Z}$ [Cohen].
6. To test for quartic residuosity: write $(f_1, \ldots, f_n) = \sum_i \lambda_i \overline{g}_i$ for some $\lambda_i \in \mathbb{Z}/d_i\mathbb{Z}$, $i = 1, \ldots, n$. As a matrix-vector equation: $(f_1, \ldots, f_n)^T = G \cdot \lambda$. Compute $G^{-1} \cdot (f_1, \ldots, f_n)^T = \lambda$; if $\lambda_i = 4\gamma_i \mod d_i$ for some $\gamma_i \in \mathbb{Z}/d_i\mathbb{Z}$ and all $i = 1, \ldots, n$, conclude that $\mathcal{L}_f \cdot \mathcal{L}_g^{-1}$ is a quartic residue in $\mathcal{C}(\mathcal{O}_l(\mathcal{L}_g))$.

The Spinor Genus: Binary Case over Number Fields

Theorem

Let $\mathcal{O}_F$ be a PID. Let f, g be anisotropic integral binary quadratic forms over $\mathcal{O}_F$ in the same genus. Let V be the quadratic space containing $\mathcal{L}_f$, $\mathcal{L}_g$. Then $\mathcal{L}_f \cdot \mathcal{L}_g^{-1}$ generates an ideal coprime to the conductor of $\mathcal{O}_l(\mathcal{L}_g)$ in $\mathcal{O}_V \Rightarrow$ a quantum poly. time algorithm to decide if $f \in \mathrm{spn}(g)$.

Proof, simple case: $\mathcal{O}_l(\mathcal{L}_g)$ is a maximal order.

1. f, g are anisotropic $\Rightarrow$ V is isomorphic to a quadratic field extension of F. Compute a basis of $\mathcal{O}_l(\mathcal{L}_g)$ and so compute the class group, obtaining a generating set of prime ideals for $\mathcal{C}(\mathcal{O}_l(\mathcal{L}_g))$ in quantum poly. time + their defining relations.
2. The relations form a lattice Λ, and $\mathcal{C}(\mathcal{O}_l(\mathcal{L}_g)) \cong \mathbb{Z}^n/\Lambda$ via $\mathcal{I} \mapsto (e_1, \ldots, e_n) + \Lambda$ for $\mathcal{I} = \prod_{i=1}^n \mathfrak{p}_i^{e_i}$.
3. $\mathbb{Z}^n/\Lambda$ is an abelian group $\Rightarrow \mathcal{C}(\mathcal{O}_l(\mathcal{L}_g)) \cong \oplus_i \mathbb{Z}/d_i\mathbb{Z}$ for some integers d_i, where the factors d_i are obtained by the quantum algorithm. We want the image of $\mathcal{L}_f \cdot \mathcal{L}_g^{-1}$ in $\oplus_i \mathbb{Z}/d_i\mathbb{Z}$.
4. $\mathcal{O}_l(\mathcal{L}_g)$ a maximal order $\Rightarrow$ can write $\mathcal{L}_f \cdot \mathcal{L}_g^{-1}$ as a product of primes in our generating set, reduced mod the relations between the prime ideals. Map $\mathcal{L}_f \cdot \mathcal{L}_g^{-1} \mapsto (f_1, \ldots, f_n) + \Lambda$ for some exponents f_i.
5. The algorithm also outputs vectors $\bar{g}_i$ of order d_i which form a basis of $\mathbb{Z}^n/\Lambda \cong \oplus_i \mathbb{Z}/d_i\mathbb{Z}$ [Cohen].
6. To test for quartic residuosity: write $(f_1, \ldots, f_n) = \sum_i \lambda_i \bar{g}_i$ for some $\lambda_i \in \mathbb{Z}/d_i\mathbb{Z}$, $i = 1, \ldots, n$. As a matrix-vector equation: $(f_1, \ldots, f_n)^T = G \cdot \lambda$. Compute $G^{-1} \cdot (f_1, \ldots, f_n)^T = \lambda$; if $\lambda_i = 4\gamma_i \bmod d_i$ for some $\gamma_i \in \mathbb{Z}/d_i\mathbb{Z}$ and all $i = 1, \ldots, n$, conclude that $\mathcal{L}_f \cdot \mathcal{L}_g^{-1}$ is a quartic residue in $\mathcal{C}(\mathcal{O}_l(\mathcal{L}_g))$.
7. If $\mathcal{L}_f \cdot \mathcal{L}_g^{-1}$ is a quartic residue in $\mathcal{C}(\mathcal{O}_l(\mathcal{L}_g))$, then $f \in \mathrm{spn}(g)$; otherwise, $f \notin \mathrm{spn}(g)$. $\square$

The Spinor Genus: Binary Case over Number Fields
Consequences

Let f, g be anisotropic integral binary quadratic forms over $\mathcal{O}_\mathsf{F}$ in the same genus; V be the quadratic space containing $\mathcal{L}_\mathsf{f}$, $\mathcal{L}_\mathsf{g}$; and $\mathcal{L}_\mathsf{f} \cdot \mathcal{L}_\mathsf{g}^{-1}$ generate an ideal coprime to the conductor of $\mathcal{O}_\mathsf{l}(\mathcal{L}_\mathsf{g})$ in $\mathcal{O}_\mathsf{V}$.

The Spinor Genus: Binary Case over Number Fields
Consequences

Let f, g be anisotropic integral binary quadratic forms over $\mathcal{O}_\mathsf{F}$ in the same genus; V be the quadratic space containing $\mathcal{L}_\mathsf{f}$, $\mathcal{L}_\mathsf{g}$; and $\mathcal{L}_\mathsf{f} \cdot \mathcal{L}_\mathsf{g}^{-1}$ generate an ideal coprime to the conductor of $\mathcal{O}_\mathsf{l}(\mathcal{L}_\mathsf{g})$ in $\mathcal{O}_\mathsf{V}$.

Corollary

Suppose $\gcd(|\mathcal{C}(\mathcal{O}_\mathsf{l}(\mathcal{L}_\mathsf{g}))|, 2) = 1$. Then $\mathsf{f} \in \operatorname{spn}(\mathsf{g})$.

The Spinor Genus: Binary Case over Number Fields
Consequences

Let f, g be anisotropic integral binary quadratic forms over $\mathcal{O}_F$ in the same genus; V be the quadratic space containing $\mathcal{L}_f$, $\mathcal{L}_g$; and $\mathcal{L}_f \cdot \mathcal{L}_g^{-1}$ generate an ideal coprime to the conductor of $\mathcal{O}_l(\mathcal{L}_g)$ in $\mathcal{O}_V$.

Corollary

Suppose $\gcd(|\mathcal{C}(\mathcal{O}_l(\mathcal{L}_g))|, 2) = 1$. Then $f \in \mathrm{spn}(g)$.

Corollary

Let F be the maximal totally real subfield of $\mathbb{Q}(\zeta_n)$ and $n \in S := \{4, 8, 16, 32, 64, 128, 256\}$ (and assuming GRH, $n \in S \cup \{512\}$). Then there is a quantum poly. time algorithm to decide if $f \in \mathrm{spn}(g)$.

The Spinor Genus: Binary Case over Number Fields
Consequences

Let f, g be anisotropic integral binary quadratic forms over $\mathcal{O}_F$ in the same genus; V be the quadratic space containing $\mathcal{L}_f$, $\mathcal{L}_g$; and $\mathcal{L}_f \cdot \mathcal{L}_g^{-1}$ generate an ideal coprime to the conductor of $\mathcal{O}_l(\mathcal{L}_g)$ in $\mathcal{O}_V$.

Corollary

Suppose $\gcd(|\mathcal{C}(\mathcal{O}_l(\mathcal{L}_g))|, 2) = 1$. Then $f \in \mathrm{spn}(g)$.

Corollary

Let F be the maximal totally real subfield of $\mathbb{Q}(\zeta_n)$ and $n \in S := \{4, 8, 16, 32, 64, 128, 256\}$ (and assuming GRH, $n \in S \cup \{512\}$). Then there is a quantum poly. time algorithm to decide if $f \in \mathrm{spn}(g)$.

Corollary

Let $F = \mathbb{Q}(\zeta_n)$ be a cyclotomic field and

$$n \in \{1, 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84\}$$

Then there is a quantum poly. time algorithm to decide if $f \in \mathrm{spn}(g)$.

IMPERIAL

Thank you.
Questions?