Are these lattices isomorphic? A quest for finer invariants

April 3rd, Journées Codage et Cryptographie, Calais

Guilhem Mureau

Inria de Bordeaux, IMB, France

The Lattice Isomorphism Problem (LIP)

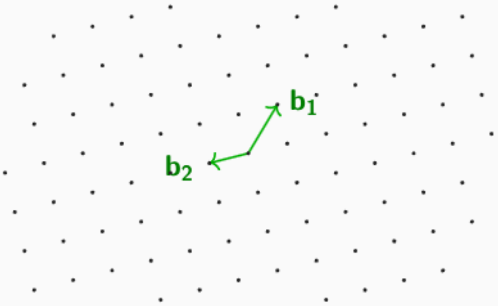
Let $\mathbf{b_1}, \ldots, \mathbf{b_n} \in \mathbb{R}^n$ which are $\mathbb{R}$-linearly independant.

$\mathcal{L} := \{\sum_i x_i \mathbf{b_i} \,|\, x_i \in \mathbb{Z}\}$ is a **lattice** in $\mathbb{R}^n$ and $\mathbf{B} = (\mathbf{b_1}| \cdots |\mathbf{b_n})$ is a **basis** of $\mathcal{L}$.

The Lattice Isomorphism Problem (LIP)

Let $\mathbf{b_1}, \ldots, \mathbf{b_n} \in \mathbb{R}^n$ which are $\mathbb{R}$-linearly independant.

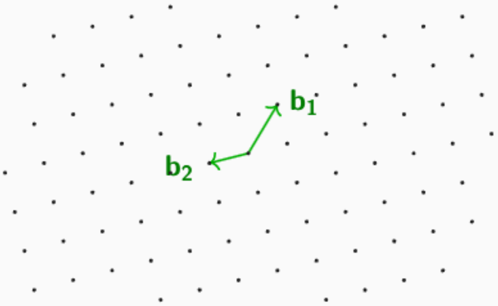
$\mathcal{L} := \{\sum_i x_i \mathbf{b_i} \mid x_i \in \mathbb{Z}\}$ is a **lattice** in $\mathbb{R}^n$ and $\mathbf{B} = (\mathbf{b_1}|\cdots|\mathbf{b_n})$ is a **basis** of $\mathcal{L}$.

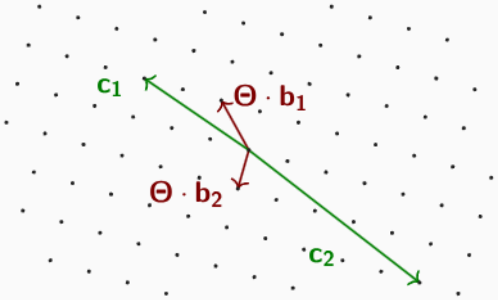


The Lattice Isomorphism Problem (LIP)

Let $\mathbf{b_1}, \ldots, \mathbf{b_n} \in \mathbb{R}^n$ which are $\mathbb{R}$-linearly independant.

$\mathcal{L} := \{\sum_i x_i \mathbf{b_i} \mid x_i \in \mathbb{Z}\}$ is a **lattice** in $\mathbb{R}^n$ and $\mathbf{B} = (\mathbf{b_1} | \cdots | \mathbf{b_n})$ is a **basis** of $\mathcal{L}$.





Lattices $\mathcal{L}_1$ and $\mathcal{L}_2$ are **isomorphic** if $\mathcal{L}_2 = \mathbf{\Theta}(\mathcal{L}_1)$ for some $\mathbf{\Theta} \in \mathcal{O}_n(\mathbb{R})$ orthogonal.

The Lattice Isomorphism Problem (LIP)

Given two lattices $\mathcal{L}_1$ and $\mathcal{L}_2$, define:

search LIP: $\mathcal{L}_1$ and $\mathcal{L}_2$ are isomorphic, compute $\mathbf{\Theta} \in \mathcal{O}_n(\mathbb{R})$ s.t. $\mathcal{L}_2 = \mathbf{\Theta}(\mathcal{L}_1)$.

The Lattice Isomorphism Problem (LIP)

Given two lattices $\mathcal{L}_1$ and $\mathcal{L}_2$, define:

search LIP: $\mathcal{L}_1$ and $\mathcal{L}_2$ are isomorphic, compute $\mathbf{\Theta} \in \mathcal{O}_n(\mathbb{R})$ s.t. $\mathcal{L}_2 = \mathbf{\Theta}(\mathcal{L}_1)$.
decision LIP: Decide whether $\mathcal{L}_1$ and $\mathcal{L}_2$ are isomorphic or not.

The Lattice Isomorphism Problem (LIP)

Given two lattices $\mathcal{L}_1$ and $\mathcal{L}_2$, define:

search LIP: $\mathcal{L}_1$ and $\mathcal{L}_2$ are isomorphic, compute $\mathbf{\Theta} \in \mathcal{O}_n(\mathbb{R})$ s.t. $\mathcal{L}_2 = \mathbf{\Theta}(\mathcal{L}_1)$.
decision LIP: Decide whether $\mathcal{L}_1$ and $\mathcal{L}_2$ are isomorphic or not.

Very old questions (Gauss, classification of binary integral quadratic forms).

The Lattice Isomorphism Problem (LIP)

Given two lattices $\mathcal{L}_1$ and $\mathcal{L}_2$, define:

search LIP: $\mathcal{L}_1$ and $\mathcal{L}_2$ are isomorphic, compute $\mathbf{\Theta} \in \mathcal{O}_n(\mathbb{R})$ s.t. $\mathcal{L}_2 = \mathbf{\Theta}(\mathcal{L}_1)$.
decision LIP: Decide whether $\mathcal{L}_1$ and $\mathcal{L}_2$ are isomorphic or not.

Very old questions (Gauss, classification of binary integral quadratic forms).

Hard algorithmic problems in high dimension: Plesken & Souvignier (1997), Haviv & Regev (2013). Best algorithms require to compute short vectors.

The Lattice Isomorphism Problem (LIP)

Given two lattices $\mathcal{L}_1$ and $\mathcal{L}_2$, define:

search LIP: $\mathcal{L}_1$ and $\mathcal{L}_2$ are isomorphic, compute $\mathbf{\Theta} \in \mathcal{O}_n(\mathbb{R})$ s.t. $\mathcal{L}_2 = \mathbf{\Theta}(\mathcal{L}_1)$.
decision LIP: Decide whether $\mathcal{L}_1$ and $\mathcal{L}_2$ are isomorphic or not.

Very old questions (Gauss, classification of binary integral quadratic forms).

Hard algorithmic problems in high dimension: Plesken & Souvignier (1997), Haviv & Regev (2013). Best algorithms require to compute short vectors.

Use in cryptography :

1. Ducas & van Woerden (2021): primitives based on decision LIP.
2. Ducas *et. al.* (2022): signature scheme **HAWK**, security related to **module**-LIP.

The module-Lattice Isomorphism Problem (module-LIP)

Module lattices are lattices with additional algebraic structure (symmetries).
They admit a compact representation: good candidates for crypto!

The module-Lattice Isomorphism Problem (module-LIP)

Module lattices are lattices with additional algebraic structure (symmetries). They admit a compact representation: good candidates for crypto!

module-LIP is LIP restricted to module lattices (and where the isomorphism must preserve the structure). Several attempts to break **search** module-LIP.

The module-Lattice Isomorphism Problem (module-LIP)

Module lattices are lattices with additional algebraic structure (symmetries).
They admit a compact representation: good candidates for crypto!

module-LIP is LIP restricted to module lattices (and where the isomorphism must preserve the structure). Several attempts to break **search** module-LIP.

van Gent & van Woerden (2025): For a certain family of module lattices, search module-LIP reduces to **decision** module-LIP.
$\rightsquigarrow$ HAWK reduces to several instances of decision module-LIP.

State-of-the-art and contribution

Target decision module-LIP for specific module lattices, as those in the reduction.

State-of-the-art and contribution

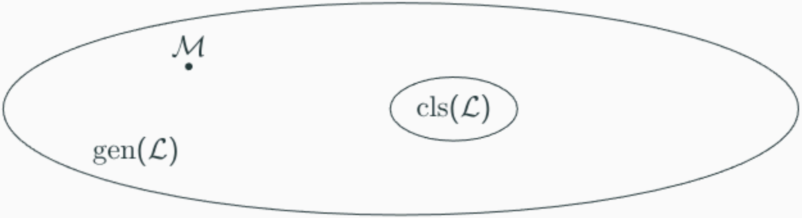
Target decision module-LIP for specific module lattices, as those in the reduction.

Goal: Decide if $\mathcal{M}$ belongs to $\mathrm{cls}(\mathcal{L})$, the isomorphism class of $\mathcal{L}$.

State-of-the-art and contribution

Target decision module-LIP for specific module lattices, as those in the reduction.

Goal: Decide if $\mathcal{M}$ belongs to cls($\mathcal{L}$), the isomorphism class of $\mathcal{L}$.

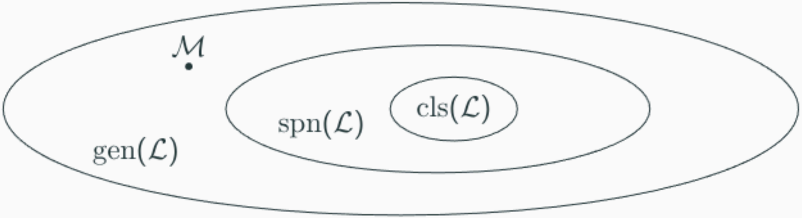


Genus: Can test efficiently if $\mathcal{L}$, $\mathcal{M}$ are in the same **genus** (necessary but not sufficient!). Are there finer and efficiently computable invariants?

State-of-the-art and contribution

Target decision module-LIP for specific module lattices, as those in the reduction.

Goal: Decide if $\mathcal{M}$ belongs to cls($\mathcal{L}$), the isomorphism class of $\mathcal{L}$.

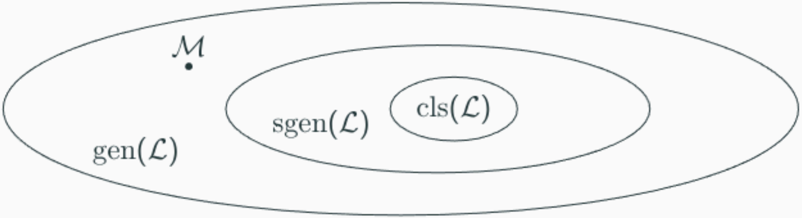


Spinor genus: Ling, Liu and Mendelsohn (2024) gave a poly-time algorithm to determine if $\mathcal{L}$, $\mathcal{M}$ are in the same **spinor genus**. **Limitations:** very strong conditions on the parameters + only defined for quadratic lattices $\Rightarrow$ No impact on HAWK.

State-of-the-art and contribution

Target decision module-LIP for specific module lattices, as those in the reduction.

Goal: Decide if $\mathcal{M}$ belongs to cls($\mathcal{L}$), the isomorphism class of $\mathcal{L}$.



My contribution: An algorithm to determine if $\mathcal{L}, \mathcal{M}$ are in the same **special genus**. Works for all parameters + poly-time for many module lattices, including those in the reduction.

Background on number theory (1)

Let $n = 2^\ell$ and $K = \mathbb{Q}[X]/(X^n + 1)$ is a (power-of-two) **cyclotomic number field**.
Its **ring of integers** is $\mathbb{Z}_K = \mathbb{Z}[X]/(X^n + 1)$. $\exists$ a **complex conjugation** $a \mapsto \overline{a}$ on K.

Background on number theory (1)

Let $n = 2^\ell$ and $K = \mathbb{Q}[X]/(X^n + 1)$ is a (power-of-two) **cyclotomic number field**.
Its **ring of integers** is $\mathbb{Z}_K = \mathbb{Z}[X]/(X^n + 1)$. $\exists$ a **complex conjugation** $a \mapsto \overline{a}$ on K.

An **ideal** of $\mathbb{Z}_K$ is a subgroup $\mathfrak{a} \subseteq \mathbb{Z}_K$ s.t. $\mathbb{Z}_K \cdot \mathfrak{a} \subseteq \mathfrak{a}$.

Background on number theory (1)

Let $n = 2^\ell$ and $K = \mathbb{Q}[X]/(X^n + 1)$ is a (power-of-two) **cyclotomic number field**.
Its **ring of integers** is $\mathbb{Z}_K = \mathbb{Z}[X]/(X^n + 1)$. $\exists$ a **complex conjugation** $a \mapsto \overline{a}$ on K.

An **ideal** of $\mathbb{Z}_K$ is a subgroup $\mathfrak{a} \subseteq \mathbb{Z}_K$ s.t. $\mathbb{Z}_K \cdot \mathfrak{a} \subseteq \mathfrak{a}$. If for all $x, y \in \mathbb{Z}_K$,

$$xy \in \mathfrak{a} \Rightarrow x \in \mathfrak{a} \text{ or } y \in \mathfrak{a},$$

it is a **prime ideal** (denote $\mathfrak{p} = \mathfrak{a}$).

Background on number theory (1)

Let $n = 2^\ell$ and $K = \mathbb{Q}[X]/(X^n + 1)$ is a (power-of-two) **cyclotomic number field**. Its **ring of integers** is $\mathbb{Z}_K = \mathbb{Z}[X]/(X^n + 1)$. $\exists$ a **complex conjugation** $a \mapsto \overline{a}$ on K.

An **ideal** of $\mathbb{Z}_K$ is a subgroup $\mathfrak{a} \subseteq \mathbb{Z}_K$ s.t. $\mathbb{Z}_K \cdot \mathfrak{a} \subseteq \mathfrak{a}$. If for all $x, y \in \mathbb{Z}_K$,

$$xy \in \mathfrak{a} \Rightarrow x \in \mathfrak{a} \text{ or } y \in \mathfrak{a},$$

it is a **prime ideal** (denote $\mathfrak{p} = \mathfrak{a}$). Example: $\ell = 2, K = \mathbb{Q}, \mathbb{Z}_K = \mathbb{Z}$ and $\mathfrak{p} = 2\mathbb{Z}$.

Background on number theory (1)

Let $n = 2^\ell$ and $K = \mathbb{Q}[X]/(X^n + 1)$ is a (power-of-two) **cyclotomic number field**.
Its **ring of integers** is $\mathbb{Z}_K = \mathbb{Z}[X]/(X^n + 1)$. $\exists$ a **complex conjugation** $a \mapsto \overline{a}$ on K.

An **ideal** of $\mathbb{Z}_K$ is a subgroup $\mathfrak{a} \subseteq \mathbb{Z}_K$ s.t. $\mathbb{Z}_K \cdot \mathfrak{a} \subseteq \mathfrak{a}$. If for all $x, y \in \mathbb{Z}_K$,

$$xy \in \mathfrak{a} \Rightarrow x \in \mathfrak{a} \text{ or } y \in \mathfrak{a},$$

it is a **prime ideal** (denote $\mathfrak{p} = \mathfrak{a}$). Example: $\ell = 2, K = \mathbb{Q}, \mathbb{Z}_K = \mathbb{Z}$ and $\mathfrak{p} = 2\mathbb{Z}$.

K **embeds** into larger fields. Two types of embeddings:

1. **Complex**: $K \hookrightarrow \mathbb{C}$, by sending X to a root of $X^n + 1$ in $\mathbb{C}$.
2. **Local**: $K \hookrightarrow K_\mathfrak{p}$, for any prime ideal $\mathfrak{p}$.

Background on number theory (2)

Let $\mathbf{b_1}, \ldots, \mathbf{b}_\ell \in K^\ell$ which are K-linearly independant. $\mathcal{L} := \{\sum_i x_i \mathbf{b_i} \,|\, x_i \in \mathbb{Z}_K\}$ is a **module lattice** in K^ℓ.

Background on number theory (2)

Let $\mathbf{b_1}, \ldots, \mathbf{b}_\ell \in K^\ell$ which are K-linearly independant. $\mathcal{L} := \{\sum_i x_i \mathbf{b_i} \,|\, x_i \in \mathbb{Z}_K\}$ is a **module lattice** in K^ℓ. It can be seen as a lattice in $\mathbb{R}^{n\ell}$, through complex embeddings.

Background on number theory (2)

Let $\mathbf{b_1}, \ldots, \mathbf{b}_\ell \in K^\ell$ which are K-linearly independant. $\mathcal{L} := \{\sum_i x_i \mathbf{b_i} \mid x_i \in \mathbb{Z}_K\}$ is a **module lattice** in K^ℓ. It can be seen as a lattice in $\mathbb{R}^{n\ell}$, through complex embeddings.

Example: $\ell = 2$, $\mathbf{b_1} = \binom{1}{0}$ and $\mathbf{b_2} = \binom{0}{1}$, then $\mathcal{L} = \mathbb{Z}_K^2$ as in **HAWK**.

Background on number theory (2)

Let $\mathbf{b_1}, \ldots, \mathbf{b}_\ell \in K^\ell$ which are K-linearly independant. $\mathcal{L} := \{\sum_i x_i \mathbf{b_i} \,|\, x_i \in \mathbb{Z}_K\}$ is a **module lattice** in K^ℓ. It can be seen as a lattice in $\mathbb{R}^{n\ell}$, through complex embeddings.

Example: $\ell = 2$, $\mathbf{b_1} = \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$ and $\mathbf{b_2} = \left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)$, then $\mathcal{L} = \mathbb{Z}_K^2$ as in **HAWK**.

For $\mathcal{L}, \mathcal{M} \subset K^\ell$, the **module index** $[\mathcal{L} : \mathcal{M}]$ is an ideal of $\mathbb{Z}_K$.

Background on number theory (2)

Let $\mathbf{b_1}, \ldots, \mathbf{b}_\ell \in K^\ell$ which are K-linearly independant. $\mathcal{L} := \{\sum_i x_i \mathbf{b_i} \mid x_i \in \mathbb{Z}_K\}$ is a **module lattice** in K^ℓ. It can be seen as a lattice in $\mathbb{R}^{n\ell}$, through complex embeddings.

Example: $\ell = 2$, $\mathbf{b_1} = \binom{1}{0}$ and $\mathbf{b_2} = \binom{0}{1}$, then $\mathcal{L} = \mathbb{Z}_K^2$ as in **HAWK**.

For $\mathcal{L}, \mathcal{M} \subset K^\ell$, the **module index** $[\mathcal{L} : \mathcal{M}]$ is an ideal of $\mathbb{Z}_K$. It is the "covolume of $\mathcal{M}$ in $\mathcal{L}$":

$$\text{For } \mathcal{L} = \mathbb{Z}_K + \mathbb{Z}_K \text{ and } \mathcal{M} = \mathbb{Z}_K + 2\mathbb{Z}_K, \quad [\mathcal{L} : \mathcal{M}] = 2\mathbb{Z}_K.$$

Background on number theory (2)

Let $\mathbf{b_1}, \ldots, \mathbf{b}_\ell \in K^\ell$ which are K-linearly independant. $\mathcal{L} := \{\sum_i x_i \mathbf{b_i} \,|\, x_i \in \mathbb{Z}_K\}$ is a **module lattice** in K^ℓ. It can be seen as a lattice in $\mathbb{R}^{n\ell}$, through complex embeddings.

Example: $\ell = 2$, $\mathbf{b_1} = \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$ and $\mathbf{b_2} = \left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)$, then $\mathcal{L} = \mathbb{Z}_K^2$ as in **HAWK**.

For $\mathcal{L}, \mathcal{M} \subset K^\ell$, the **module index** $[\mathcal{L} : \mathcal{M}]$ is an ideal of $\mathbb{Z}_K$. It is the "covolume of $\mathcal{M}$ in $\mathcal{L}$":

$$\text{For } \mathcal{L} = \mathbb{Z}_K + \mathbb{Z}_K \text{ and } \mathcal{M} = \mathbb{Z}_K + 2\mathbb{Z}_K, \quad [\mathcal{L} : \mathcal{M}] = 2\mathbb{Z}_K.$$

For any prime ideal $\mathfrak{p}$, a module lattice $\mathcal{L} \subset K^\ell$ extends to $\mathcal{L}_\mathfrak{p} \subset K_\mathfrak{p}^\ell$ via $K \hookrightarrow K_\mathfrak{p}$.

Background on number theory (2)

Let $\mathbf{b_1}, \ldots, \mathbf{b}_\ell \in K^\ell$ which are K-linearly independant. $\mathcal{L} := \{\sum_i x_i \mathbf{b_i} \,|\, x_i \in \mathbb{Z}_K\}$ is a **module lattice** in K^ℓ. It can be seen as a lattice in $\mathbb{R}^{n\ell}$, through complex embeddings.

Example: $\ell = 2$, $\mathbf{b_1} = \binom{1}{0}$ and $\mathbf{b_2} = \binom{0}{1}$, then $\mathcal{L} = \mathbb{Z}_K^2$ as in **HAWK**.

For $\mathcal{L}, \mathcal{M} \subset K^\ell$, the **module index** $[\mathcal{L} : \mathcal{M}]$ is an ideal of $\mathbb{Z}_K$. It is the "covolume of $\mathcal{M}$ in $\mathcal{L}$":

$$\text{For } \mathcal{L} = \mathbb{Z}_K + \mathbb{Z}_K \text{ and } \mathcal{M} = \mathbb{Z}_K + 2\mathbb{Z}_K, \quad [\mathcal{L} : \mathcal{M}] = 2\mathbb{Z}_K.$$

For any prime ideal $\mathfrak{p}$, a module lattice $\mathcal{L} \subset K^\ell$ extends to $\mathcal{L}_\mathfrak{p} \subset K_\mathfrak{p}^\ell$ via $K \hookrightarrow K_\mathfrak{p}$.
It is **easy** to check if $\mathcal{L}_\mathfrak{p}$ and $\mathcal{M}_\mathfrak{p}$ are **locally** isomorphic at $\mathfrak{p}$, *i.e.*, if there exists

$$\mathbf{\Theta}_\mathfrak{p} \in \mathcal{U}_\ell(K_\mathfrak{p}) \text{ s.t. } \mathcal{M}_\mathfrak{p} = \mathbf{\Theta}_\mathfrak{p}(\mathcal{L}_\mathfrak{p}), \quad \text{where } \mathcal{U}_\ell \text{ means unitary} : \overline{\mathbf{\Theta}}_\mathfrak{p}^T \cdot \mathbf{\Theta}_\mathfrak{p} = \mathbf{Id}.$$

Genus and special genus

$\mathcal{L}$ and $\mathcal{M}$ belongs to the same **genus** if they are locally isomorphic at any $\mathfrak{p}$,

Genus and special genus

$\mathcal{L}$ and $\mathcal{M}$ belongs to the same **genus** if they are locally isomorphic at any $\mathfrak{p}$, *i.e.*, if

$$\forall\, \mathfrak{p}, \exists\, \mathbf{\Theta}_{\mathfrak{p}} \in \mathcal{U}_\ell(K_{\mathfrak{p}}) \text{ s.t. } \mathcal{M}_{\mathfrak{p}} = \mathbf{\Theta}_{\mathfrak{p}}(\mathcal{L}_{\mathfrak{p}}).$$

Genus and special genus

$\mathcal{L}$ and $\mathcal{M}$ belongs to the same **genus** if they are locally isomorphic at any $\mathfrak{p}$, *i.e.*, if

$$\forall\, \mathfrak{p}, \exists\, \mathbf{\Theta}_\mathfrak{p} \in \mathcal{U}_\ell(K_\mathfrak{p}) \text{ s.t. } \mathcal{M}_\mathfrak{p} = \mathbf{\Theta}_\mathfrak{p}(\mathcal{L}_\mathfrak{p}).$$

$\mathcal{L}$ and $\mathcal{M}$ belongs to the same **special genus** if

$$(\exists\, \mathbf{\Sigma} \in \mathcal{U}_\ell(K), \forall\, \mathfrak{p}, \exists\, \mathbf{\Theta}_\mathfrak{p} \in \mathcal{U}_\ell(K_\mathfrak{p}) \text{ with } \det \mathbf{\Theta}_\mathfrak{p} = 1) \text{ s.t. } \mathcal{M}_\mathfrak{p} = \mathbf{\Sigma} \circ \mathbf{\Theta}_\mathfrak{p}(\mathcal{L}_\mathfrak{p}).$$

Genus and special genus

$\mathcal{L}$ and $\mathcal{M}$ belongs to the same **genus** if they are locally isomorphic at any $\mathfrak{p}$, *i.e.*, if

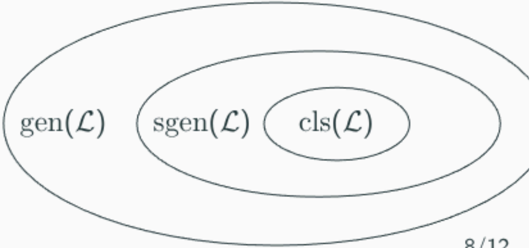
$$\forall\, \mathfrak{p}, \exists\, \mathbf{\Theta}_\mathfrak{p} \in \mathcal{U}_\ell(K_\mathfrak{p}) \text{ s.t. } \mathcal{M}_\mathfrak{p} = \mathbf{\Theta}_\mathfrak{p}(\mathcal{L}_\mathfrak{p}).$$

$\mathcal{L}$ and $\mathcal{M}$ belongs to the same **special genus** if

$$(\exists\, \mathbf{\Sigma} \in \mathcal{U}_\ell(K), \forall\, \mathfrak{p}, \exists\, \mathbf{\Theta}_\mathfrak{p} \in \mathcal{U}_\ell(K_\mathfrak{p}) \text{ with } \det \mathbf{\Theta}_\mathfrak{p} = 1) \text{ s.t. } \mathcal{M}_\mathfrak{p} = \mathbf{\Sigma} \circ \mathbf{\Theta}_\mathfrak{p}(\mathcal{L}_\mathfrak{p}).$$

The genus of $\mathcal{L}$ contains the special genus of $\mathcal{L}$, itself containing the isomorphism class of $\mathcal{L}$.

There are **finitely many** classes in a genus.



How to distinguish special genera: Shimura's theorem

Theorem (Shimura, 1964): Fix $\mathcal{L}_0 = \mathbb{Z}_K^2$ and $\mathcal{M} \in \mathrm{gen}(\mathcal{L}_0)$.

How to distinguish special genera: Shimura's theorem

Theorem (Shimura, 1964): Fix $\mathcal{L}_0 = \mathbb{Z}_K^2$ and $\mathcal{M} \in \mathrm{gen}(\mathcal{L}_0)$. Then,

$$\mathcal{M} \in \mathrm{sgen}(\mathcal{L}_0) \ \ \textbf{iff} \ \ [\mathcal{L}_0 : \mathcal{M}] \text{ has the form } g\mathbb{Z}_K \text{ with } g\overline{g} = 1.$$

Theorem (Shimura, 1964): Fix $\mathcal{L}_0 = \mathbb{Z}_K^2$ and $\mathcal{M} \in \mathrm{gen}(\mathcal{L}_0)$. Then,

$$\mathcal{M} \in \mathrm{sgen}(\mathcal{L}_0) \ \textbf{ iff } \ [\mathcal{L}_0 : \mathcal{M}] \text{ has the form } g\mathbb{Z}_K \text{ with } g\overline{g} = 1.$$

This condition can be checked using an algorithm by Lenstra & Silverberg (2019).

How to distinguish special genera: Shimura's theorem

Theorem (Shimura, 1964): Fix $\mathcal{L}_0 = \mathbb{Z}_K^2$ and $\mathcal{M} \in \mathrm{gen}(\mathcal{L}_0)$. Then,

$$\mathcal{M} \in \mathrm{sgen}(\mathcal{L}_0) \ \textbf{ iff } \ [\mathcal{L}_0 : \mathcal{M}] \text{ has the form } g\mathbb{Z}_K \text{ with } g\overline{g} = 1.$$

This condition can be checked using an algorithm by Lenstra & Silverberg (2019).

We obtain a **polynomial-time** algorithm for testing if $\mathcal{M} \in \mathrm{sgen}(\mathcal{L}_0)$.

How to distinguish special genera: Shimura's theorem

Theorem (Shimura, 1964): Fix $\mathcal{L}_0 = \mathbb{Z}_K^2$ and $\mathcal{M} \in \mathrm{gen}(\mathcal{L}_0)$. Then,

$$\mathcal{M} \in \mathrm{sgen}(\mathcal{L}_0) \ \textbf{ iff } \ [\mathcal{L}_0 : \mathcal{M}] \text{ has the form } g\mathbb{Z}_K \text{ with } g\overline{g} = 1.$$

This condition can be checked using an algorithm by Lenstra & Silverberg (2019).

We obtain a **polynomial-time** algorithm for testing if $\mathcal{M} \in \mathrm{sgen}(\mathcal{L}_0)$.

More generally it works for any $\mathcal{L}$ and $\mathcal{M} \in \mathrm{gen}(\mathcal{L})$ but it is harder to analyze.

Impact and gain

Impact on HAWK? Gain compared to the genus?

Impact and gain

Impact on HAWK? Gain compared to the genus?

Impact and gain

Impact on HAWK? Gain compared to the genus?

Let $K = \mathbb{Q}[X]/(X^{512}+1)$ and $\mathcal{L}_0 = \mathbb{Z}_K^2$.

Impact and gain

Impact on HAWK? Gain compared to the genus?

Let $K = \mathbb{Q}[X]/(X^{512}+1)$ and $\mathcal{L}_0 = \mathbb{Z}_K^2$.

Recall the reduction from HAWK to decision module-LIP; the module lattices involved **lie in the same special genus** $\Rightarrow$ no impact on HAWK.

Impact and gain

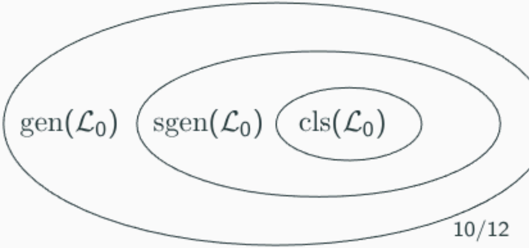
Impact on HAWK? Gain compared to the genus?

Let $K = \mathbb{Q}[X]/(X^{512}+1)$ and $\mathcal{L}_0 = \mathbb{Z}_K^2$.

Recall the reduction from HAWK to decision module-LIP; the module lattices involved **lie in the same special genus** $\Rightarrow$ no impact on HAWK.

$\#\{\text{isomorphism classes in } \mathrm{gen}(\mathcal{L}_0)\} \approx 2^{1000}$.
$\#\{\text{special genera in } \mathrm{gen}(\mathcal{L}_0)\} \approx 2^{200}$.

$\rightsquigarrow$ Still about $\approx 2^{800}$ classes in $\mathrm{sgen}(\mathcal{L}_0)$!



Takeaway

- The special genus is indeed finer than the genus.

- It is computable for several module lattices: To make a hard instance of decision module-LIP, module lattices have to be chosen in the same special genus.

Takeaway

- The special genus is indeed finer than the genus.
- It is computable for several module lattices: To make a hard instance of decision module-LIP, module lattices have to be chosen in the same special genus.
- No practical impact on HAWK.

Takeaway

- The special genus is indeed finer than the genus.
- It is computable for several module lattices: To make a hard instance of decision module-LIP, module lattices have to be chosen in the same special genus.
- No practical impact on HAWK.
- Open question: other efficiently computable invariants?

Takeaway

- The special genus is indeed finer than the genus.
- It is computable for several module lattices: To make a hard instance of decision module-LIP, module lattices have to be chosen in the same special genus.
- No practical impact on HAWK.
- Open question: other efficiently computable invariants?

Thank you for your attention!

References

Léo Ducas, Eamonn W Postlethwaite, Ludo N Pulles, and Wessel van Woerden. Hawk: Module lip makes lattice signatures fast, compact and simple. 2022.

Léo Ducas and Wessel van Woerden. On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography. 2022

Hendrik W Lenstra Jr and Alice Silverberg. Testing isomorphism of lattices over cmorders. 2019

Cong Ling, Jingbo Liu, Andrew Mendelsohn. On the Spinor Genus and the Distinguishing Lattice Isomorphism Problem. 2024.

Goro Shimura. Arithmetic of unitary groups. 1964.