On the module-Lattice Isomorphism Problem,
based on a joint work with A. Pellet-Mary, G. Pliatsok and A. Wallet.

Guilhem Mureau, 1st year PhD.

Supervisors : Alice Pellet-Mary, Renaud Coulangeon

INRIA, Université de Bordeaux

Journées C2 2023

What's in this talk ?

- Defining the module-Lattice Isomorphism Problem (module-LIP).

$\rightarrow$ a generalization of an existing problem.

What's in this talk ?

- Defining the module-Lattice Isomorphism Problem (module-LIP).
$\rightarrow$ a generalization of an existing problem.

- An (algebraic) attack on module-LIP in a special case.

(Unstructured) LIP

• Linearly independent vectors $\mathrm{v}_1, \ldots, \mathrm{v}_\mathrm{k} \in \mathbb{R}^n$ form a **basis** of a lattice $\mathcal{L} \subset \mathbb{R}^n$ if

$$\mathcal{L} = \mathcal{L}(\mathrm{v}_1 || \cdots || \mathrm{v}_k) := \left\{ \sum_{i=1}^{k} a_i \mathrm{v}_\mathrm{i} \mid \forall\, i \in \{1, \ldots, k\},\ a_i \in \mathbb{Z} \right\}.$$

(Unstructured) LIP

- Linearly independent vectors $\mathrm{v}_1, \ldots, \mathrm{v}_\mathrm{k} \in \mathbb{R}^n$ form a **basis** of a lattice $\mathcal{L} \subset \mathbb{R}^n$ if

$$\mathcal{L} = \mathcal{L}(\mathrm{v}_1 || \cdots || \mathrm{v}_k) := \left\{ \sum_{i=1}^{k} a_i \mathrm{v}_\mathrm{i} \mid \forall\, i \in \{1, \ldots, k\},\ a_i \in \mathbb{Z} \right\}.$$

We consider full rank lattices *i.e.*, $k = n$.

(Unstructured) LIP

- Linearly independent vectors $\mathrm{v}_1, \ldots, \mathrm{v}_\mathrm{k} \in \mathbb{R}^n$ form a **basis** of a lattice $\mathcal{L} \subset \mathbb{R}^n$ if

$$\mathcal{L} = \mathcal{L}(\mathrm{v}_1 || \cdots || \mathrm{v}_k) := \left\{ \sum_{i=1}^{k} a_i \mathrm{v}_\mathrm{i} \mid \forall\, i \in \{1, \ldots, k\},\ a_i \in \mathbb{Z} \right\}.$$

We consider full rank lattices *i.e.*, $k = n$.

- $\mathcal{L}_1 = \mathcal{L}(\mathrm{B})$ and $\mathcal{L}_2 = \mathcal{L}(\mathrm{B}')$ are **isomorphic** if there exists $\mathrm{O} \in \mathcal{O}_n(\mathbb{R})$ such that $\mathcal{L}_2 = \mathrm{O} \cdot \mathcal{L}_1$.

(Unstructured) LIP

- Linearly independent vectors $\mathrm{v}_1, \dots, \mathrm{v}_\mathrm{k} \in \mathbb{R}^n$ form a **basis** of a lattice $\mathcal{L} \subset \mathbb{R}^n$ if

$$\mathcal{L} = \mathcal{L}(\mathrm{v}_1 || \cdots || \mathrm{v}_k) := \left\{ \sum_{i=1}^{k} a_i \mathrm{v}_\mathrm{i} \mid \forall\, i \in \{1, \dots, k\},\ a_i \in \mathbb{Z} \right\}.$$

We consider full rank lattices *i.e.*, $k = n$.

- $\mathcal{L}_1 = \mathcal{L}(\mathrm{B})$ and $\mathcal{L}_2 = \mathcal{L}(\mathrm{B}')$ are **isomorphic** if there exists $\mathrm{O} \in \mathcal{O}_n(\mathbb{R})$ such that $\mathcal{L}_2 = \mathrm{O} \cdot \mathcal{L}_1$. In terms of bases,

$$\mathrm{O} \cdot \mathrm{B} \text{ is a basis of } \mathcal{L}_2 \Rightarrow \exists\, \mathrm{U} \in \mathrm{GL}_n(\mathbb{Z}) : \mathrm{B}' = \mathrm{OBU}.$$

(Unstructured) LIP

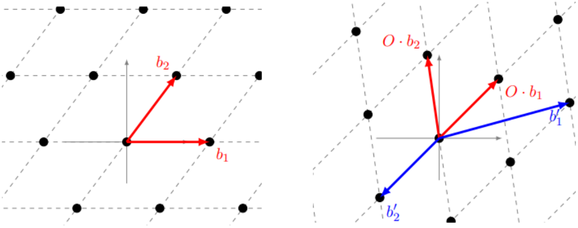
- Linearly independent vectors $\mathrm{v}_1, \ldots, \mathrm{v}_\mathrm{k} \in \mathbb{R}^n$ form a **basis** of a lattice $\mathcal{L} \subset \mathbb{R}^n$ if

$$\mathcal{L} = \mathcal{L}(\mathrm{v}_1 || \cdots || \mathrm{v}_k) := \left\{ \sum_{i=1}^{k} a_i \mathrm{v}_\mathrm{i} \mid \forall\, i \in \{1, \ldots, k\},\, a_i \in \mathbb{Z} \right\}.$$

  We consider full rank lattices $i.e.$, $k = n$.

- $\mathcal{L}_1 = \mathcal{L}(\mathrm{B})$ and $\mathcal{L}_2 = \mathcal{L}(\mathrm{B}')$ are **isomorphic** if there exists $\mathrm{O} \in \mathcal{O}_n(\mathbb{R})$ such that $\mathcal{L}_2 = \mathrm{O} \cdot \mathcal{L}_1$. In terms of bases,

$$\mathrm{O} \cdot \mathrm{B} \text{ is a basis of } \mathcal{L}_2 \Rightarrow \exists\, \mathrm{U} \in \mathrm{GL}_n(\mathbb{Z}) : \mathrm{B}' = \mathrm{OBU}.$$



(a) $\mathcal{L}_1$ with known basis $B = (b_1, b_2)$. (b) $\mathcal{L}_2$ with known basis $B' = (b'_1, b'_2)$.

(Unstructured) LIP

Move to Gram matrices : $G = B^T B$ and $G' = B'^T B'$,

$$B' = OBU \Rightarrow G' = U^T G U \text{ are } \mathrm{GL}_n(\mathbb{Z})\text{-}\textbf{congruent}.$$

(Unstructured) LIP

Move to Gram matrices : $G = B^T B$ and $G' = B'^T B'$,

$$B' = OBU \Rightarrow G' = U^T GU \text{ are } \mathrm{GL}_n(\mathbb{Z})\text{-}\textbf{congruent}.$$

(Unstructured) LIP :

Parameter : $\mathrm{G} \in \mathcal{S}_n^{>0}(\mathbb{R})$.
Input : $\mathrm{G}' \in \mathcal{S}_n^{>0}(\mathbb{R})$ $\mathrm{GL}_n(\mathbb{Z})$-congruent to G.
Goal : Find $\mathrm{U} \in \mathrm{GL}_n(\mathbb{Z})$ such that $\mathrm{G}' = \mathrm{U}^\mathrm{T}\mathrm{GU}$.

(Unstructured) LIP

Move to Gram matrices : $G = B^T B$ and $G' = B'^T B'$,

$$B' = OBU \Rightarrow G' = U^T G U \text{ are } \mathrm{GL}_n(\mathbb{Z})\text{-}\textbf{congruent}.$$

(Unstructured) LIP :

Parameter : $\mathrm{G} \in \mathcal{S}_n^{>0}(\mathbb{R})$.
Input : $\mathrm{G}' \in \mathcal{S}_n^{>0}(\mathbb{R})$ $\mathrm{GL}_n(\mathbb{Z})$-congruent to G.
Goal : Find $\mathrm{U} \in \mathrm{GL}_n(\mathbb{Z})$ such that $\mathrm{G}' = \mathrm{U}^\mathrm{T}\mathrm{GU}$.

LIP in cryptography

- Best known algorithm runs in time $n^{O(n)}$ (Haviv and Regev, 2013 [1]). Needs to enumerate (possibly many) short vectors.

LIP in cryptography

- Best known algorithm runs in time $n^{O(n)}$ (Haviv and Regev, 2013 [1]). Needs to enumerate (possibly many) short vectors.

- Recently, LIP to build cryptographic schemes.

- Best known algorithm runs in time $n^{O(n)}$ (Haviv and Regev, 2013 [1]). Needs to enumerate (possibly many) short vectors.

- Recently, LIP to build cryptographic schemes.
  - LIP with unstructured lattices ([3] and [4] $e.g., \mathcal{L} = \mathbb{Z}^n$).

LIP in cryptography

- Best known algorithm runs in time $n^{O(n)}$ (Haviv and Regev, 2013 [1]). Needs to enumerate (possibly many) short vectors.

- Recently, LIP to build cryptographic schemes.
  - LIP with unstructured lattices ([3] and [4] $e.g., \mathcal{L} = \mathbb{Z}^n$).
  - Signature scheme Hawk (Ducas, Postlethwaite, Pulles, van Woerden, 2023 [2]). Instantiated on the module $\mathcal{O}_K^2$ (a structured lattice).

LIP in cryptography

- Best known algorithm runs in time $n^{O(n)}$ (Haviv and Regev, 2013 [1]). Needs to enumerate (possibly many) short vectors.

- Recently, LIP to build cryptographic schemes.
  - LIP with unstructured lattices ([3] and [4] $e.g., \mathcal{L} = \mathbb{Z}^n$).
  - Signature scheme Hawk (Ducas, Postlethwaite, Pulles, van Woerden, 2023 [2]). Instantiated on the module $\mathcal{O}_K^2$ (a structured lattice).

- Generalize LIP for any module ?

LIP in cryptography

- Best known algorithm runs in time $n^{O(n)}$ (Haviv and Regev, 2013 [1]). Needs to enumerate (possibly many) short vectors.

- Recently, LIP to build cryptographic schemes.
  - LIP with unstructured lattices ([3] and [4] $e.g., \mathcal{L} = \mathbb{Z}^n$).
  - Signature scheme Hawk (Ducas, Postlethwaite, Pulles, van Woerden, 2023 [2]). Instantiated on the module $\mathcal{O}_K^2$ (a structured lattice).

- Generalize LIP for any module ?

- Use the algebraic structure to solve LIP more efficiently ?

K a number field, $d = [K : \mathbb{Q}]$ and ring of integers $\mathcal{O}_K$.

Modules and module-LIP

K a number field, $d = [K : \mathbb{Q}]$ and ring of integers $\mathcal{O}_K$.

- A (free) **module** of rank ℓ is any set

$$M = \mathcal{O}_K b_1 + \cdots + \mathcal{O}_K b_\ell \subset K^\ell,$$

with $b_1, \ldots, b_\ell \in K^\ell$ which are K-linearly independent.

Modules and module-LIP

K a number field, $d = [K : \mathbb{Q}]$ and ring of integers $\mathcal{O}_K$.

- A (free) **module** of rank ℓ is any set

$$M = \mathcal{O}_K b_1 + \cdots + \mathcal{O}_K b_\ell \subset K^\ell,$$

with $b_1, \ldots, b_\ell \in K^\ell$ which are K-linearly independent.

- Analogy with unstructured lattices :
  - With Minkowski embedding $\sigma : K \hookrightarrow \mathbb{R}^d$, see M as $\mathcal{L} \subset \mathbb{R}^{d\ell}$.

Modules and module-LIP

K a number field, $d = [K : \mathbb{Q}]$ and ring of integers $\mathcal{O}_K$.

- A (free) **module** of rank ℓ is any set

$$M = \mathcal{O}_K b_1 + \cdots + \mathcal{O}_K b_\ell \subset K^\ell,$$

with $b_1, \ldots, b_\ell \in K^\ell$ which are K-linearly independent.

- Analogy with unstructured lattices :
  - With Minkowski embedding $\sigma : K \hookrightarrow \mathbb{R}^d$, see M as $\mathcal{L} \subset \mathbb{R}^{d\ell}$.
  - $B := (b_1 || \cdots || b_\ell)$ is a basis of M.

Modules and module-LIP

K a number field, $d = [K : \mathbb{Q}]$ and ring of integers $\mathcal{O}_K$.

- A (free) **module** of rank ℓ is any set

$$M = \mathcal{O}_K b_1 + \cdots + \mathcal{O}_K b_\ell \subset K^\ell,$$

with $b_1, \ldots, b_\ell \in K^\ell$ which are K-linearly independent.

- Analogy with unstructured lattices :
  - With Minkowski embedding $\sigma : K \hookrightarrow \mathbb{R}^d$, see M as $\mathcal{L} \subset \mathbb{R}^{d\ell}$.
  - $B := (b_1 || \cdots || b_\ell)$ is a basis of M.
  - $G := B^* B$ is the Gram matrix associated.

Modules and module-LIP

K a number field, $d = [K : \mathbb{Q}]$ and ring of integers $\mathcal{O}_K$.

- A (free) **module** of rank ℓ is any set

$$M = \mathcal{O}_K b_1 + \cdots + \mathcal{O}_K b_\ell \subset K^\ell,$$

with $b_1, \ldots, b_\ell \in K^\ell$ which are K-linearly independent.

- Analogy with unstructured lattices :
  - With Minkowski embedding $\sigma : K \hookrightarrow \mathbb{R}^d$, see M as $\mathcal{L} \subset \mathbb{R}^{d\ell}$.
  - $B := (b_1 || \cdots || b_\ell)$ is a basis of M.
  - $G := B^* B$ is the Gram matrix associated.
  - Gram matrices G, G' are congruent if there is $U \in \mathrm{GL}_\ell(\mathcal{O}_K)$ such that $G' = U^* G U$.

Modules and module-LIP

K a number field, $d = [K : \mathbb{Q}]$ and ring of integers $\mathcal{O}_K$.

- A (free) **module** of rank ℓ is any set

$$M = \mathcal{O}_K b_1 + \cdots + \mathcal{O}_K b_\ell \subset K^\ell,$$

with $b_1, \ldots, b_\ell \in K^\ell$ which are K-linearly independent.

- Analogy with unstructured lattices :
  - With Minkowski embedding $\sigma : K \hookrightarrow \mathbb{R}^d$, see M as $\mathcal{L} \subset \mathbb{R}^{d\ell}$.
  - $B := (b_1 || \cdots || b_\ell)$ is a basis of M.
  - $G := B^* B$ is the Gram matrix associated.
  - Gram matrices G, G' are congruent if there is $U \in \mathrm{GL}_\ell(\mathcal{O}_K)$ such that $G' = U^* G U$.

- More generally (for non-free modules), one can use pseudo-bases and pseudo-Gram matrices.

Modules and module-LIP

Module-Lattice Isomorphism Problem

Parameters : K, a basis B of a (free) module M, Gram matrix G.
Input : Any G' congruent to G.
Goal : Find $U \in \mathrm{GL}_\ell(\mathcal{O}_K)$ such that $G' = U^* G U$.

Module-Lattice Isomorphism Problem

Parameters : K, a basis B of a (free) module M, Gram matrix G.
Input : Any G' congruent to G.
Goal : Find $U \in \mathrm{GL}_\ell(\mathcal{O}_K)$ such that $G' = U^* G U$.

Solving module-LIP for rank 2 modules ?

Module-Lattice Isomorphism Problem

Parameters : K, a basis B of a (free) module M, Gram matrix G.
Input : Any G' congruent to G.
Goal : Find $U \in \mathrm{GL}_\ell(\mathcal{O}_K)$ such that $G' = U^* G U$.

Solving module-LIP for rank 2 modules ?
e.g., when $M = \mathcal{O}_K^2$ (as in Hawk) then $B = G = I_2$ and

$$G' = U^* U = \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix} \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} a\overline{a} + b\overline{b} & \star \\ \star & c\overline{c} + d\overline{d} \end{pmatrix}$$

Module-Lattice Isomorphism Problem

Parameters : K, a basis B of a (free) module M, Gram matrix G.
Input : Any G' congruent to G.
Goal : Find $U \in \mathrm{GL}_\ell(\mathcal{O}_K)$ such that $G' = U^* G U$.

Solving module-LIP for rank 2 modules ?
e.g., when $M = \mathcal{O}_K^2$ (as in Hawk) then $B = G = I_2$ and

$$G' = U^* U = \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix} \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} a\overline{a} + b\overline{b} & \star \\ \star & c\overline{c} + d\overline{d} \end{pmatrix}$$

When K is totally real, the diagonal coefficients are sums of two squares in K. Finding those squares allows to reconstruct U.

Module-Lattice Isomorphism Problem

Parameters : K, a basis B of a (free) module M, Gram matrix G.
Input : Any G' congruent to G.
Goal : Find $U \in \mathrm{GL}_\ell(\mathcal{O}_K)$ such that $G' = U^* G U$.

Solving module-LIP for rank 2 modules ?
e.g., when $M = \mathcal{O}_K^2$ (as in Hawk) then $B = G = I_2$ and

$$G' = U^* U = \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix} \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} a\overline{a} + b\overline{b} & \star \\ \star & c\overline{c} + d\overline{d} \end{pmatrix}$$

When K is totally real, the diagonal coefficients are sums of two squares in K. Finding those squares allows to reconstruct U.
Writing elements as sums of two squares in K is equivalent to solve a norm equation (in the appropriate extension).

First attack on module-LIP

$\rightarrow$ Using arithmetic of ideals (factorization, splittings) and algorithmic tools (variants of Gentry Szydlo algorithm) we can solve module-LIP for rank two modules when K is totally real !

$\rightarrow$ Using arithmetic of ideals (factorization, splittings) and algorithmic tools (variants of Gentry Szydlo algorithm) we can solve module-LIP for rank two modules when K is totally real !

Breaking module-LIP on $\mathcal{O}_K^2$.

Suppose K is totally real and $M = \mathcal{O}_K^2$. There exists a polynomial time algorithm that, given any G' congruent to I_2, returns **all** $U \in \mathrm{GL}_2(\mathcal{O}_K)$ such that $G' = U^* U$.

First attack on module-LIP

$\rightarrow$ Using arithmetic of ideals (factorization, splittings) and algorithmic tools (variants of Gentry Szydlo algorithm) we can solve module-LIP for rank two modules when K is totally real !

Breaking module-LIP on $\mathcal{O}_K^2$.

Suppose K is totally real and $M = \mathcal{O}_K^2$. There exists a polynomial time algorithm that, given any G' congruent to I_2, returns **all** $U \in \mathrm{GL}_2(\mathcal{O}_K)$ such that $G' = U^* U$.

We proved a more general statement : for K totally real and most of rank two modules $M \subset K^2$, there exists a probabilistic and heuristic polynomial time algorithm that solves module-LIP on M (G. M., A. Pellet-Mary, G. Pliatsok, A. Wallet).

Ok that's nice, and after ?

First attack on module-LIP

Ok that's nice, and after ?

- Generalize to any field ? (would break Hawk)

First attack on module-LIP

Ok that's nice, and after ?

- Generalize to any field ? (would break Hawk)
- Decide algorithmically if two module lattices are isomorphic ? (distinguishing variant of module-LIP)

First attack on module-LIP

Ok that's nice, and after ?

- Generalize to any field ? (would break Hawk)
- Decide algorithmically if two module lattices are isomorphic ? (distinguishing variant of module-LIP)

Thank you !

[1] On the Lattice Isomorphism Problem, I. Haviv, O. Regev, 2013.

[2] HAWK : Module LIP makes Lattice Signatures Fast, Compact and Simple, L. Ducas, E.W. Postlethwaite, L. N. Pulles. W. van Woerden, 2023.

[3] Just how hard are rotations of $\mathbb{Z}^n$? H. Bennett, A. Ganju, P. Peetathawatchai, N. Sthephens-Davidowitz, 2023.

[4] On the lattice isomorphism problem, quadratic forms, remarkable lattices and cryptography, L. Ducas, W. van Woerden.