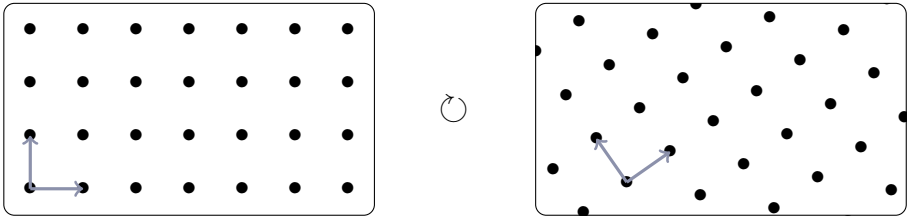
Algorithms for the module lattice isomorphism problem in certain fields

Alice Pellet-Mary

based on joint works with Guilhem Mureau, Clémence Chevignard, Pierre-Alain Fouque, Georges Pliatsok, Alexandre Wallet and Wessel van Woerden

CAIPI Symposium, Limoges

The module lattice isomorphism problem



Number fields

Number field: $K = \mathbb{Q}[X]/P(X)$ (P irreducible, $\deg(P) = d$)

- $K = \mathbb{Q}$
- $K = \mathbb{Q}[X]/(X^d + 1)$ with $d = 2^\ell \rightsquigarrow$ power-of-two cyclotomic field
- $K = \mathbb{Q}[X]/(X^d - X - 1)$ with d prime $\rightsquigarrow$ NTRUPrime field

Ring of integers: $\mathcal{O}_K \subset K$, for this talk $\mathcal{O}_K = \mathbb{Z}[X]/P(X)$

(more generally $\mathbb{Z}[X]/P(X) \subseteq \mathcal{O}_K$ but $\mathcal{O}_K$ can be larger)

- $\mathcal{O}_K = \mathbb{Z}$
- $\mathcal{O}_K = \mathbb{Z}[X]/(X^d + 1)$ with $d = 2^\ell \rightsquigarrow$ power-of-two cyclotomic ring
- $\mathcal{O}_K = \mathbb{Z}[X]/(X^d - X - 1)$ with d prime $\rightsquigarrow$ NTRUPrime ring of integers

The canonical embedding

($K = \mathbb{Q}[X]/P(X)$, $\alpha_1, \cdots, \alpha_d$ complex roots of $P(X)$)

Canonical embedding: $\sigma : \begin{array}{ccc} K & \to & \mathbb{C}^d \\ a(X) & \mapsto & (a(\alpha_1), \cdots, a(\alpha_d)) \end{array}$

- σ is injective
- σ is a ring morphism (addition and multiplication in $\mathbb{C}^d$ performed coefficient-wise)

$\Rightarrow$ we can see K as a subset of $\mathbb{C}^d$

This induces a geometry on K (using the hermitian norm in $\mathbb{C}^d$): for $a \in K$

$$\|a\| := \|\sigma(a)\|_2 = \sqrt{\overline{\sigma(a)}^T \sigma(a)}.$$

We extend $\sigma : K^k \to \mathbb{C}^{dk}$ coordinate-wise, and similarly $\|v\| := \|\sigma(v)\|_2$ for $v \in K^k$

Module lattices

(Free) module:

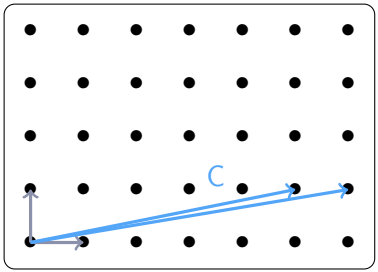
$$M = \{B \cdot x \,|\, x \in {\mathcal{O}_K}^k\} \text{ for some matrix } B \in {\mathcal{O}_K}^{k \times k} \text{ with } \det_K(B) \neq 0$$

- k is the module rank
- B is a module basis of M

Example: $M = {\mathcal{O}_K}^2$ is a module of rank 2, with basis $B = I_2$ (or any $B \in {\mathcal{O}_K}^{2\times 2}$ with $\det(B) \in {\mathcal{O}_K}^\times$)

$\sigma(M)$ is a lattice: of $\mathbb{Z}$-rank $n := d \cdot k$, included in $\mathbb{C}^n$

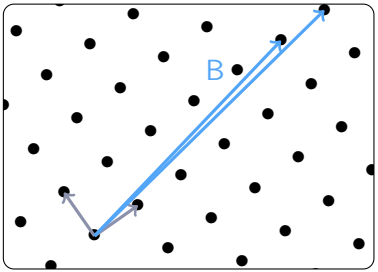
The lattice isomorphism problem [DW22,BGPS23]



$\mathcal{L}_0 = \mathbb{Z}^n$

rotate

(choose O orthogonal matrix)

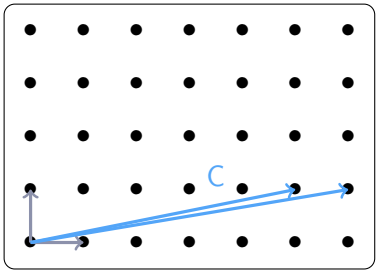


$\mathcal{L} = O \cdot \mathbb{Z}^n$

B bad basis of $\mathcal{L}$

Lattice Isomorphism Problem (LIP):
Given B, recover O (or C)

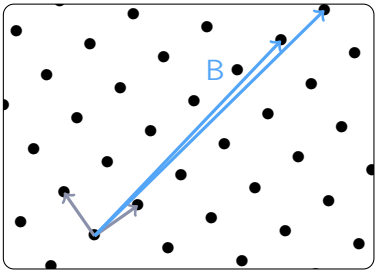
The lattice isomorphism problem [DW22,BGPS23]



$\mathcal{L}_0 = \mathbb{Z}^n$

rotate

(choose O orthogonal matrix)



$\mathcal{L} = O \cdot \mathbb{Z}^n$

B bad basis of $\mathcal{L}$

Lattice Isomorphism Problem (LIP):
Given B, recover O (or C)

Equivalent formulation with Gram matrices

Lattice isomorphism problem: Given $B = O \cdot C$ with
- $O \in O_n(\mathbb{R})$ orthogonal
- C a basis of $\mathbb{Z}^n$

Find O (equivalently: find C)

Gram matrix associated to B:

$$G = B^T B = C^T (O^T O) C = C^T C$$

Lattice isomorphism problem (Gram matrix formulation):
Given $G = C^T C$ with C a (secret) basis of $\mathbb{Z}^n$, find C.

Example:
- $C = \begin{pmatrix} 1 & 1 \\ 4 & 5 \end{pmatrix}$
- $O = \begin{pmatrix} 0.5 & 0.87 \\ 0.87 & -0.5 \end{pmatrix}$
- $B = \begin{pmatrix} 3.96 & 4.83 \\ -1.13 & -1.63 \end{pmatrix}$
- $G = \begin{pmatrix} 17 & 21 \\ 21 & 26 \end{pmatrix}$
  $= C^T C = B^T B$

Given G, recover $C \in \mathbb{Z}^{2\times 2}$ with $\det(C) = \pm 1$ such that $C^T C = G$

The module lattice isomorphism problem

Lattice isomorphism problem:
Given $G = C^T C$ with C a basis of $\mathbb{Z}^n$, find C

The module lattice isomorphism problem

Lattice isomorphism problem:
Given $G = C^T C$ with C a basis of $\mathbb{Z}^n$, find C

Module lattice isomorphism problem:
Given $G = \overline{\sigma(C)}^T \sigma(C)$ with C a basis of ${\mathcal{O}_K}^2$, find C

The module lattice isomorphism problem

Lattice isomorphism problem:
Given $G = C^T C$ with C a basis of $\mathbb{Z}^n$, find C

Module lattice isomorphism problem:
Given $G = \overline{\sigma(C)^T}\sigma(C)$ with C a basis of ${\mathcal{O}_K}^2$, find C

Remarks.

- we consider $\overline{\sigma(C)}$ because we use hermitian norm in $\mathbb{C}^{2d}$
- only rank 2 modules in this talk (and even only ${\mathcal{O}_K}^2$)

The module lattice isomorphism problem

Lattice isomorphism problem:
Given $G = C^T C$ with C a basis of $\mathbb{Z}^n$, find C

Module lattice isomorphism problem:
Given $G = \overline{\sigma(C)}^T \sigma(C)$ with C a basis of ${\mathcal{O}_K}^2$, find C

Remarks.

- we consider $\overline{\sigma(C)}$ because we use hermitian norm in $\mathbb{C}^{2d}$
- only rank 2 modules in this talk (and even only ${\mathcal{O}_K}^2$)

Hawk signature: (submitted to the NIST)
Relies on module-LIP for the module ${\mathcal{O}_K}^2$, in a power-of-two cyclotomic field
($K = \mathbb{Q}[X]/(X^d + 1)$ with $d = 512$ or $d = 1024$)

Algorithms for module-LIP over certain fields

Conclusion

Summing up

Hardness of module-LIP for various fields: (for modules of rank 2)

- Totally real fields: polynomial time attack

Summing up

Hardness of module-LIP for various fields: (for modules of rank 2)

- Totally real fields: polynomial time attack
- NTRUPrime fields: heuristic polynomial time attack
  - relies heavily on the presence of one real embedding
  - relies (less heavily) of the 2-transitivity of the Galois group

Summing up

Hardness of module-LIP for various fields: (for modules of rank 2)

- Totally real fields: polynomial time attack
- NTRUPrime fields: heuristic polynomial time attack
  - relies heavily on the presence of one real embedding
  - relies (less heavily) of the 2-transitivity of the Galois group
- Cyclotomic fields: polynomial time reduction to a problem in ideals of a quaternion algebra
  - How hard is this problem in ideals of quaternion algebras?

Summing up

Hardness of module-LIP for various fields: (for modules of rank 2)

- Totally real fields: polynomial time attack
- NTRUPrime fields: heuristic polynomial time attack
  - relies heavily on the presence of one real embedding
  - relies (less heavily) of the 2-transitivity of the Galois group
- Cyclotomic fields: polynomial time reduction to a problem in ideals of a quaternion algebra
  - How hard is this problem in ideals of quaternion algebras?
  - At first we thought it would be easy (analogy with similar problems in number fields)...

Summing up

Hardness of module-LIP for various fields: (for modules of rank 2)

- Totally real fields: polynomial time attack
- NTRUPrime fields: heuristic polynomial time attack
  - relies heavily on the presence of one real embedding
  - relies (less heavily) of the 2-transitivity of the Galois group
- Cyclotomic fields: polynomial time reduction to a problem in ideals of a quaternion algebra
  - How hard is this problem in ideals of quaternion algebras?
  - At first we thought it would be easy (analogy with similar problems in number fields)...
  - ... but now I am much less convinced

Conclusion

Hardness of module-LIP in $\mathcal{O}_K{}^2$ seems quite dependent on the choice of K

I used beamer theme begles (https://framagit.org/squirrrr/beamerthemebegles)

Conclusion

Hardness of module-LIP in $\mathcal{O}_K{}^2$ seems quite dependent on the choice of K

- luckily, Hawk uses cyclotomic fields $\Rightarrow$ unbroken so far

I used beamer theme begles (https://framagit.org/squirrrr/beamerthemebegles)

Conclusion

Hardness of module-LIP in $\mathcal{O}_K{}^2$ seems quite dependent on the choice of K

- luckily, Hawk uses cyclotomic fields $\Rightarrow$ unbroken so far
- is there really a difference in hardness, or is it only a matter of time?

I used beamer theme begles (https://framagit.org/squirrrr/beamerthemebegles)

Conclusion

Hardness of module-LIP in $\mathcal{O}_K{}^2$ seems quite dependent on the choice of K

- luckily, Hawk uses cyclotomic fields $\Rightarrow$ unbroken so far
- is there really a difference in hardness, or is it only a matter of time?
- for other lattice problems (e.g., computing a short basis), we do not have such a difference between number fields

I used beamer theme begles (https://framagit.org/squirrrr/beamerthemebegles)

Conclusion

Hardness of module-LIP in $\mathcal{O}_K{}^2$ seems quite dependent on the choice of K

- luckily, Hawk uses cyclotomic fields $\Rightarrow$ unbroken so far
- is there really a difference in hardness, or is it only a matter of time?
- for other lattice problems (e.g., computing a short basis), we do not have such a difference between number fields

Thank you

I used beamer theme begles (https://framagit.org/squirrrr/beamerthemebegles)