Towards efficient algorithmic aspects of algebraic lattices

Thomas Espitau

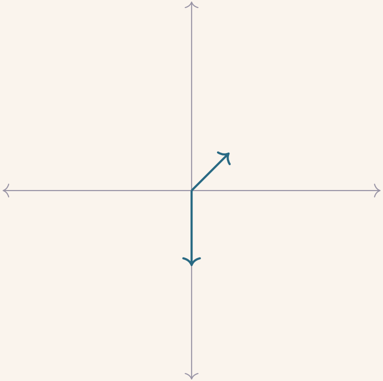
April 3, 2024, Bordeaux

Seminaire CHARM 2024

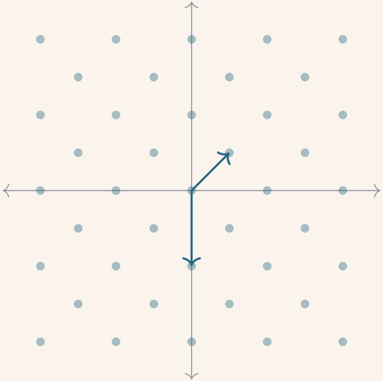
Lattices and their reductions

What is this all about?

What is this all about?



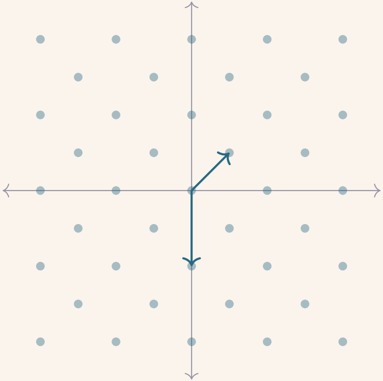
What is this all about?



Lattice

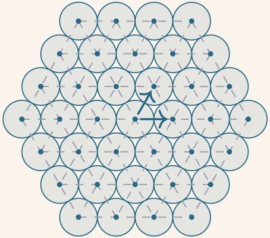
A (Euclidean) lattice Λ is a *discrete* subgroup of an Euclidean space (say $\mathbb{R}^n$).

What is this all about?



Lattice

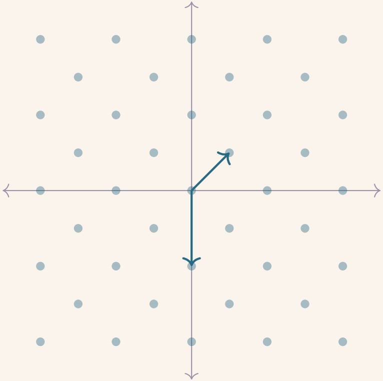
A (Euclidean) lattice Λ is a *discrete* subgroup of an Euclidean space (say $\mathbb{R}^n$).



Sphere Packing problem

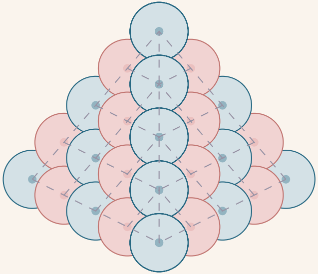
Hexagonal lattice | Lagrange 1773

What is this all about?



Lattice

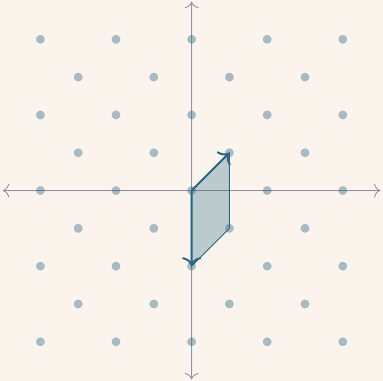
A (Euclidean) lattice Λ is a *discrete* subgroup of an Euclidean space (say $\mathbb{R}^n$).



Sphere Packing problem

Kepler's conjecture | Hales 1999

What is this all about?



Lattice

A (Euclidean) lattice Λ is a *discrete* subgroup of an Euclidean space (say $\mathbb{R}^n$).

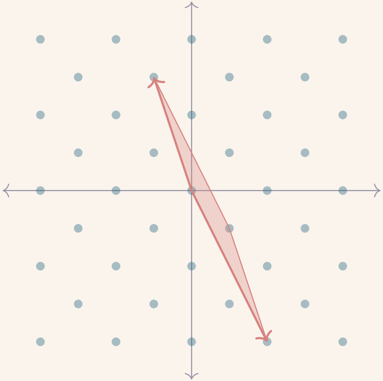
The (co)volume $\mathrm{covol}(\Lambda)$ of Λ is the quantity

$$\mathrm{covol}(\Lambda) = \sqrt{\det \langle v_i, v_j \rangle}$$

Corresponds to the volume of the fundamental domain $\{\sum x_i v_i \mid 0 \leqslant x_i < 1\}$.

(also the volume (no "co") of the variety $\mathbb{R}^n/\Lambda$)

What is this all about?



Lattice

A (Euclidean) lattice Λ is a *discrete* subgroup of an Euclidean space (say $\mathbb{R}^n$).

The (co)volume $\operatorname{covol}(\Lambda)$ of Λ is the quantity

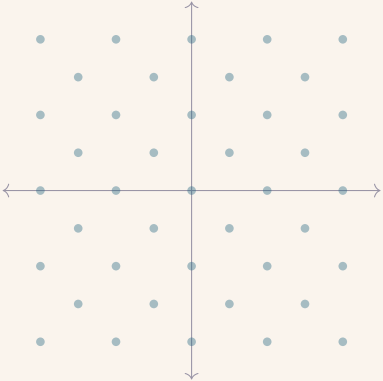
$$\operatorname{covol}(\Lambda) = \sqrt{\det \langle v_i, v_j \rangle}$$

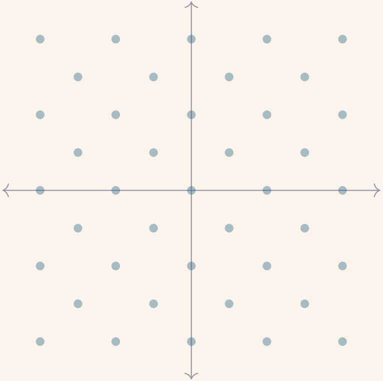
Corresponds to the volume of the fundamental domain $\{\sum x_i v_i \mid 0 \leqslant x_i < 1\}$.

(also the volume (no "co") of the variety $\mathbb{R}^n/\Lambda$)

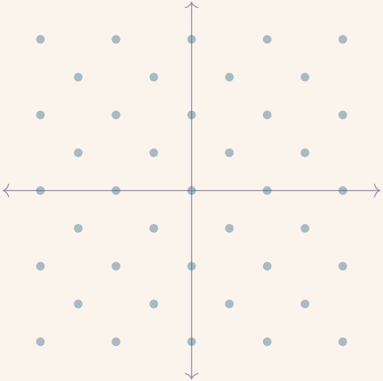
Independent of the basis

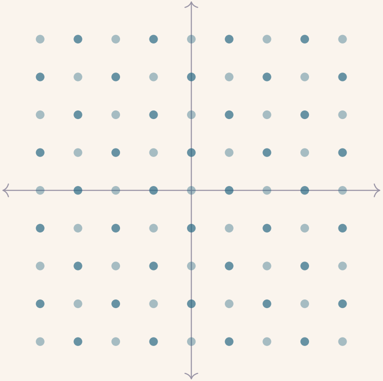
What is this all about?





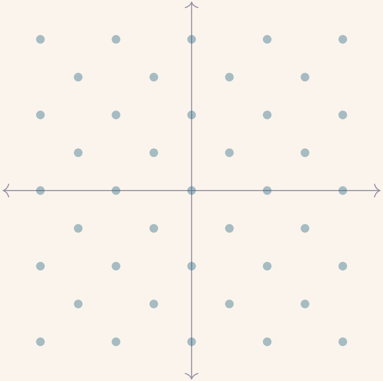
What is this all about?

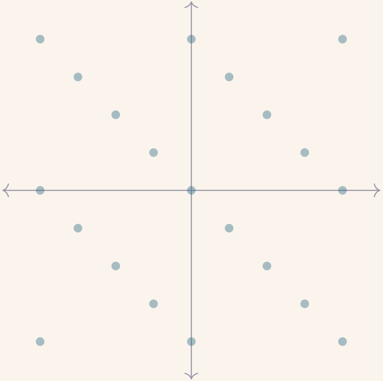




$$\mathrm{covol}(\Lambda) = 2\,\mathrm{covol}(\Lambda')$$

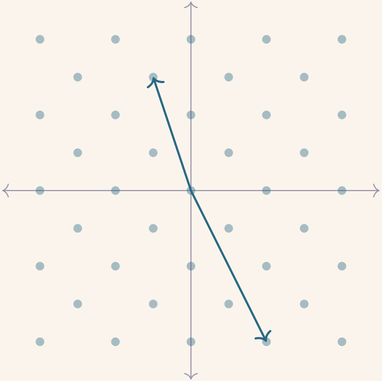
What is this all about?





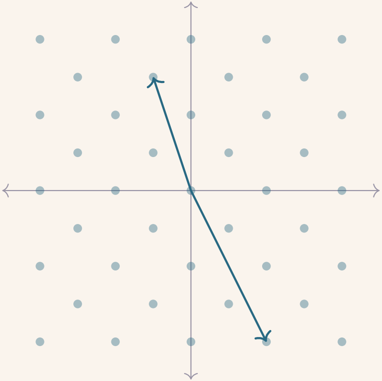
$$\mathrm{covol}(\Lambda) = \tfrac{1}{2}\,\mathrm{covol}(\Lambda')$$

What is this all about?



How to get a shorter basis?

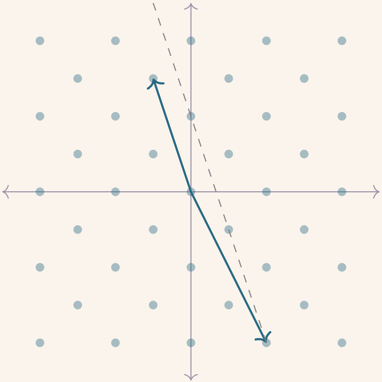
What is this all about?



How to get a shorter basis?

$\rightarrow$ Use the shortest vector to reduce the longest one.

What is this all about?



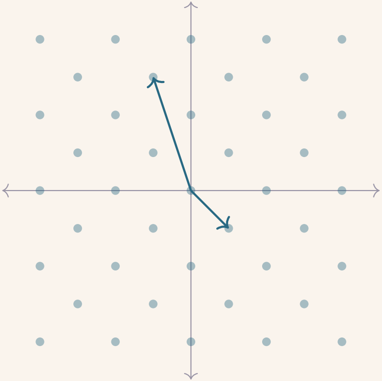
How to get a shorter basis?

$\rightarrow$ Use the shortest vector to reduce the longest one.

---

1. Take the *shortest* element in the coset

What is this all about?



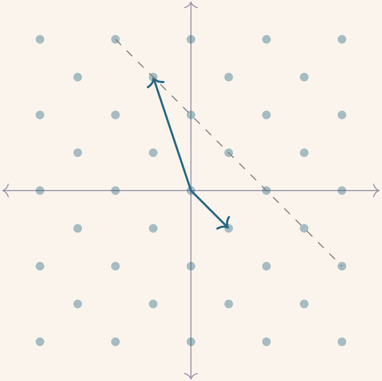
How to get a shorter basis?

$\rightarrow$ Use the shortest vector to reduce the longest one.

---

1. Take the *shortest* element in the coset

What is this all about?



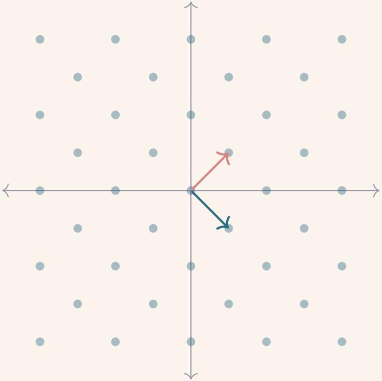
How to get a shorter basis?

$\rightarrow$ Use the shortest vector to reduce the longest one.

---

1. Take the *shortest* element in the coset
2. Repeat

What is this all about?



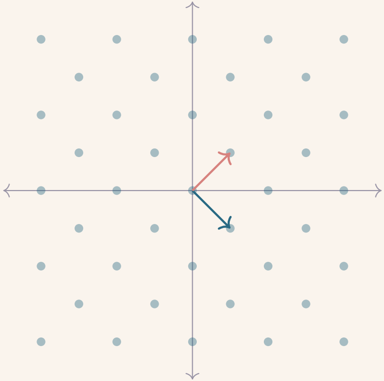
How to get a shorter basis?

$\rightarrow$ Use the shortest vector to reduce the longest one.

---

1. Take the *shortest* element in the coset
2. Repeat

What is this all about?

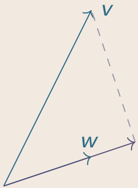


How to get a shorter basis?

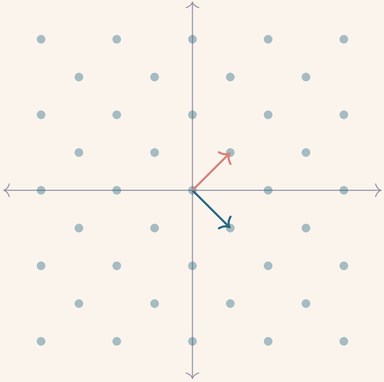
$\rightarrow$ Use the shortest vector to reduce the longest one.

Effective computing of this element:

1. Orthogonal projection $\frac{\langle w,v\rangle}{\langle w,w\rangle} w$



What is this all about?

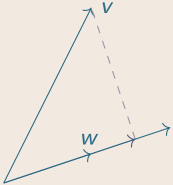


How to get a shorter basis?

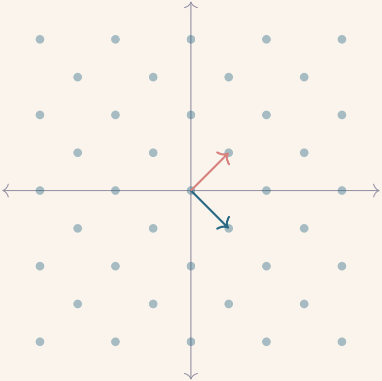
$\rightarrow$ Use the shortest vector to reduce the longest one.

Effective computing of this element:

1. Orthogonal projection $\frac{\langle w,v\rangle}{\langle w,w\rangle} w$
2. Round $\left\lceil \frac{\langle w,v\rangle}{\langle w,w\rangle} \right\rfloor w$



What is this all about?

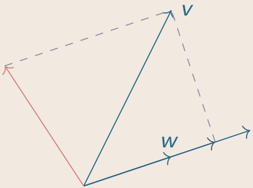


How to get a shorter basis?

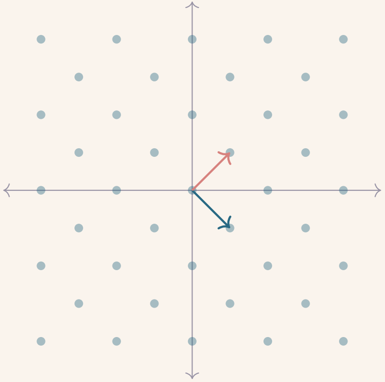
$\rightarrow$ Use the shortest vector to reduce the longest one.

Effective computing of this element:

1. Orthogonal projection $\frac{\langle w,v \rangle}{\langle w,w \rangle} w$
2. Round $\left\lceil \frac{\langle w,v \rangle}{\langle w,w \rangle} \right\rfloor w$
3. Substract $v - \left\lceil \frac{\langle w,v \rangle}{\langle w,w \rangle} \right\rfloor w$



What is this all about?

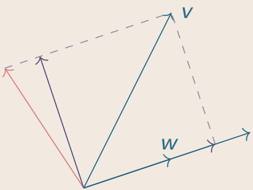


How to get a shorter basis?

→ Use the shortest vector to reduce the longest one.

Effective computing of this element:

1. Orthogonal projection $\frac{\langle w, v\rangle}{\langle w, w\rangle} w$
2. Round $\left\lceil \frac{\langle w, v\rangle}{\langle w, w\rangle} \right\rfloor w$
3. Substract $v - \left\lceil \frac{\langle w, v\rangle}{\langle w, w\rangle} \right\rfloor w$



In dim 2... The Gauss(-Lagrange) reduction algorithm

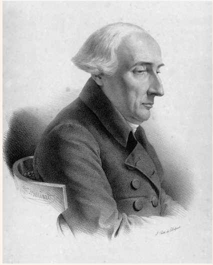
Gauss-Lagrange reduction

if $\|v\| < \|u\|$ **then return** **Gauss**(v, u);
$v' \leftarrow v - \left\lfloor \frac{\langle u,v \rangle}{\|u\|^2} \right\rceil u$;
if $\|v'\| < \|v\|$ **then return** **Gauss**(u, v');
else return (u, v);

In dim 2... The Gauss(-Lagrange) reduction algorithm

Gauss-Lagrange reduction

if $\|v\| < \|u\|$ **then return** **Gauss**(v, u);
$v' \leftarrow v - \left\lfloor \frac{\langle u,v \rangle}{\|u\|^2} \right\rceil u$;
if $\|v'\| < \|v\|$ **then return** **Gauss**(u, v');
else return (u, v);

Properties of a Gauss-reduced basis (u, v)

- $\|u\| \leqslant \|v\|$ and $|\langle u, v \rangle| \leqslant \frac{\|u\|^2}{2}$.

In dim 2… The Gauss(-Lagrange) reduction algorithm

Gauss-Lagrange reduction

if $\|v\| < \|u\|$ **then return**
  Gauss(v, u);
$v' \leftarrow v - \left\lfloor \frac{\langle u,v \rangle}{\|u\|^2} \right\rceil u$;
if $\|v'\| < \|v\|$ **then return**
  Gauss(u, v');
else return (u, v);

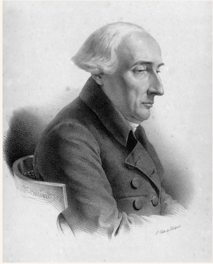
Properties of a Gauss-reduced basis (u, v)

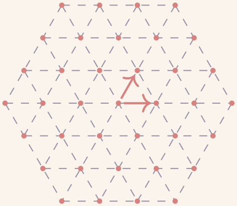
- $\|u\| \leqslant \|v\|$ and $|\langle u, v\rangle| \leqslant \frac{\|u\|^2}{2}$.
- u is a *shortest vector* of Λ

In dim 2… The Gauss(-Lagrange) reduction algorithm

Gauss-Lagrange reduction

if $\|v\| < \|u\|$ **then return** **Gauss**(v, u);
$v' \leftarrow v - \left\lfloor \frac{\langle u, v\rangle}{\|u\|^2} \right\rceil u$;
if $\|v'\| < \|v\|$ **then return** **Gauss**(u, v');
else return (u, v);





Properties of a Gauss-reduced basis (u, v)

- $\|u\| \leqslant \|v\|$ and $|\langle u, v\rangle| \leqslant \frac{\|u\|^2}{2}$.
- u is a *shortest vector* of Λ
- $\|u\|^2 \leqslant (4/3)\,\mathrm{covol}(\Lambda)$

And now what?

Minkowski's theorem for first minima: For any lattice Λ of rank d,

$$\lambda_1(\Lambda) \leqslant \sqrt{d}\,\mathrm{covol}(\Lambda)^{\frac{1}{d}}$$

And now what?

Minkowski-Hermite's theorem for first minima: For any lattice Λ of rank d,

$$\lambda_1(\Lambda) \leqslant \sqrt{\gamma_d}\, \mathrm{covol}(\Lambda)^{\frac{1}{d}}$$

And now what?

Finding the shortest/closest vector in a lattice is **hard**

And now what?

[LLL82] *There exists a* ***polynomial-time algorithm****, which given any lattice Λ, produces a vector in Λ of Euclidean length* ***at most*** *a factor of 2^n longer than the shortest vector.*

And now what?

[LLL82] *There exists a* ***polynomial-time algorithm****, which given any lattice Λ, produces a vector in Λ of Euclidean length* ***at most*** *a factor of 2^n longer than the shortest vector.*

- Simultaneous Diophantine approximation
  $\left| r_i - \frac{p_i}{q} \right| \leqslant \epsilon$

And now what?

[LLL82] *There exists a **polynomial-time algorithm**, which given any lattice Λ, produces a vector in Λ of Euclidean length **at most** a factor of 2^n longer than the shortest vector.*

- Simultaneous Diophantine approximation
  $\left| r_i - \frac{p_i}{q} \right| \leqslant \epsilon$
- Minimal polynomials of algebraic numbers
  $(r_i = r^i)$

And now what?

[LLL82] *There exists a* ***polynomial-time algorithm****, which given any lattice Λ, produces a vector in Λ of Euclidean length* ***at most*** *a factor of 2^n longer than the shortest vector.*

- Simultaneous Diophantine approximation $\left| r_i - \frac{p_i}{q} \right| \leqslant \epsilon$
- Minimal polynomials of algebraic numbers $(r_i = r^i)$
- Polynomial factorization over rationals Approximate a root r, find a minimal g vanishing at r.
- Cryptanalysis Knapsack problem , RSA for small public exponents, lattice-based cryptography...

And now what?

[LLL82] *There exists a* ***polynomial-time algorithm****, which given any lattice Λ, produces a vector in Λ of Euclidean length* ***at most*** *a factor of 2^n longer than the shortest vector.*

- Simultaneous Diophantine approximation $\left|r_i - \frac{p_i}{q}\right| \leqslant \epsilon$
- Minimal polynomials of algebraic numbers $(r_i = r^i)$
- Polynomial factorization over rationals Approximate a root r, find a minimal g vanishing at r.
- Cryptanalysis Knapsack problem , RSA for small public exponents, lattice-based cryptography...
- Computations in algebraic number theory (ideal computations, HNF, control of size of elements...)

What can we do with a reduction in rank 2 ?

Any basis $(v_1, \ldots, v_d)$ of a lattice Λ yields a filtration given by $(\Lambda_i = v_1\mathbb{Z} \oplus \cdots \oplus v_i\mathbb{Z})$

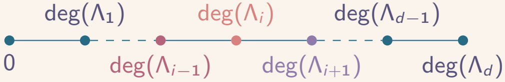
$$\{0\} = \Lambda_0 \subset \Lambda_1 \subset \cdots \subset \Lambda_{i-1} \subset \Lambda_i \subset \Lambda_{i+1} \subset \cdots \subset \Lambda_d = \Lambda$$

What can we do with a reduction in rank 2 ?

Any basis $(v_1, \dots, v_d)$ of a lattice Λ yields a filtration given by $(\Lambda_i = v_1\mathbb{Z} \oplus \cdots \oplus v_i\mathbb{Z})$

$$\{0\} = \Lambda_0 \subset \Lambda_1 \subset \cdots \subset \Lambda_{i-1} \subset \Lambda_i \subset \Lambda_{i+1} \subset \cdots \subset \Lambda_d = \Lambda$$

- Profile (1 dim datum of the filtration):

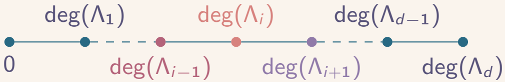


What can we do with a reduction in rank 2 ?

Any basis $(v_1, \ldots, v_d)$ of a lattice Λ yields a filtration given by $(\Lambda_i = v_1\mathbb{Z} \oplus \cdots \oplus v_i\mathbb{Z})$

$$\{0\} = \Lambda_0 \subset \Lambda_1 \subset \cdots \subset \Lambda_{i-1} \subset \Lambda_i \subset \Lambda_{i+1} \subset \cdots \subset \Lambda_d = \Lambda$$

- Profile (1 dim datum of the filtration):



- Where are the natural rank 2 lattices around here?

$$\Lambda^* = {}^{\Lambda_{i+1}}\!/_{\Lambda_{i-1}}$$

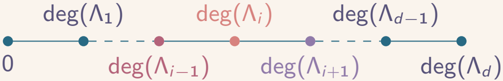
(endowed with the *quotient norm*)

What can we do with a reduction in rank 2 ?

Any basis $(v_1, \ldots, v_d)$ of a lattice Λ yields a filtration given by $(\Lambda_i = v_1\mathbb{Z} \oplus \cdots \oplus v_i\mathbb{Z})$

$$\{0\} = \Lambda_0 \subset \Lambda_1 \subset \cdots \subset \Lambda_{i-1} \subset \Lambda_i \subset \Lambda_{i+1} \subset \cdots \subset \Lambda_d = \Lambda$$

- Profile (1 dim datum of the filtration):



- Where are the natural rank 2 lattices around here?

$$\Lambda^* = {}^{\Lambda_{i+1}}\!/\!_{\Lambda_{i-1}}$$

(endowed with the *quotient norm*)

Reduce this lattice with **Gauss algorithm**:

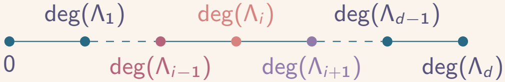
$$\{0\} \subset v\mathbb{Z} = \Lambda' \subset \Lambda^*$$

What can we do with a reduction in rank 2 ?

Any basis $(v_1, \dots, v_d)$ of a lattice Λ yields a filtration given by $(\Lambda_i = v_1\mathbb{Z} \oplus \cdots \oplus v_i\mathbb{Z})$

$$\{0\} = \Lambda_0 \subset \Lambda_1 \subset \cdots \subset \Lambda_{i-1} \subset \Lambda_i \subset \Lambda_{i+1} \subset \cdots \subset \Lambda_d = \Lambda$$

- Profile (1 dim datum of the filtration):



- Where are the natural rank 2 lattices around here?

$$\Lambda^* = {}^{\Lambda_{i+1}}\!/_{\Lambda_{i-1}}$$

(endowed with the *quotient norm*)

Reduce this lattice with **Gauss algorithm**:

$$\{0\} \subset v\mathbb{Z} = \Lambda' \subset \Lambda^*$$

Action of the reduction

$$2\deg(\Lambda') \leqslant \deg(\Lambda^*) + \log\left(\frac{4}{3}\right)$$

(*by Hermite inequality + log*)

Continuing...

Lifting and replacing in the filtration: find Λ_i' s.t.:

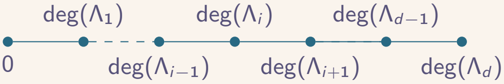
$$\begin{array}{ccccc}
{}^{\Lambda_{i-1}}\!/\!_{\Lambda_{i-1}} & \subset & {}^{\Lambda_i'}\!/\!_{\Lambda_{i-1}} & \subset & {}^{\Lambda_{i+1}}\!/\!_{\Lambda_{i-1}} \\
\| & & \| & & \| \\
\{0\} & \subset & \Lambda' & \subset & \Lambda^*
\end{array}$$

Continuing...

Lifting and replacing in the filtration: find Λ'_i s.t.:

$$\begin{array}{ccccc} {}^{\Lambda_{i-1}}\!/_{\Lambda_{i-1}} & \subset & {}^{\Lambda'_i}\!/_{\Lambda_{i-1}} & \subset & {}^{\Lambda_{i+1}}\!/_{\Lambda_{i-1}} \\ \| & & \| & & \| \\ \{0\} & \subset & \Lambda' & \subset & \Lambda^* \end{array}$$

Result on the profile space:

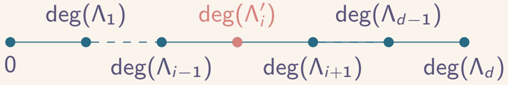


Continuing...

Lifting and replacing in the filtration: find Λ_i' s.t.:

$$\begin{array}{ccccc}
\Lambda_{i-1}/\Lambda_{i-1} & \subset & \Lambda_i'/\Lambda_{i-1} & \subset & \Lambda_{i+1}/\Lambda_{i-1} \\
\| & & \| & & \| \\
\{0\} & \subset & \Lambda' & \subset & \Lambda^*
\end{array}$$

Result on the profile space:

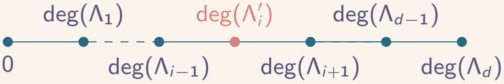


$$\deg(\Lambda_i') \leqslant \deg(\Lambda_i)$$

Lifting and replacing in the filtration: find Λ_i' s.t.:

$$
\begin{array}{ccccc}
\Lambda_{i-1}/\Lambda_{i-1} & \subset & \Lambda_i'/\Lambda_{i-1} & \subset & \Lambda_{i+1}/\Lambda_{i-1} \\
\| & & \| & & \| \\
\{0\} & \subset & \Lambda' & \subset & \Lambda^*
\end{array}
$$

Result on the profile space:



$$\deg(\Lambda_i') \leqslant \deg(\Lambda_i)$$

Gauss's reduction is a *local* tool for densifying the filtration

Effective lifting and size-reduction

Effective lifting

- Boils down to replace v_i by a *small* representative of a basis of $\Lambda' = v + \Lambda_{i-1}$:

CVP instance

Effective lifting and size-reduction

Effective lifting

- Boils down to replace v_i by a *small* representative of a basis of $\Lambda' = v + \Lambda_{i-1}$:

CVP instance

- Perform an *approx*-CVP by using the filtration:

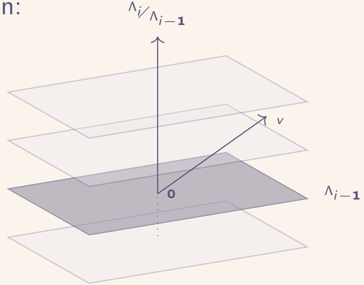
Effective lifting and size-reduction

Effective lifting

- Boils down to replace v_i by a *small* representative of a basis of $\Lambda' = v + \Lambda_{i-1}$:

  CVP instance

- Perform an *approx*-CVP by using the filtration:



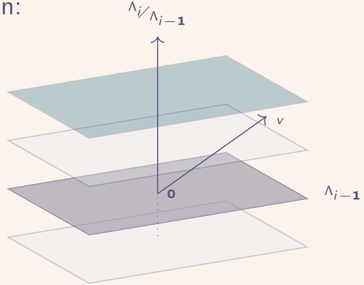
Effective lifting and size-reduction

Effective lifting

- Boils down to replace v_i by a *small* representative of a basis of $\Lambda' = v + \Lambda_{i-1}$:

CVP instance

- Perform an *approx*-CVP by using the filtration:

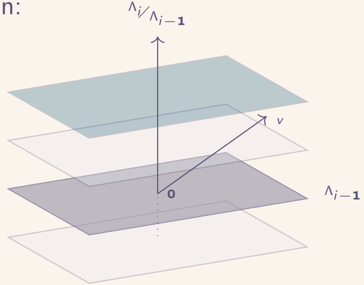


Effective lifting

- Boils down to replace v_i by a *small* representative of a basis of $\Lambda' = v + \Lambda_{i-1}$:

  CVP instance

- Perform an *approx*-CVP by using the filtration:



Lifting

1 **for** $j = k-1$ **down to** 1 **do**
2 $\quad v \leftarrow v - \left\lceil \frac{\langle v_k, \pi_j(v_j)\rangle}{\|\pi_j(v_j)\|^2} \right\rfloor \cdot v_j$
3 **end for**

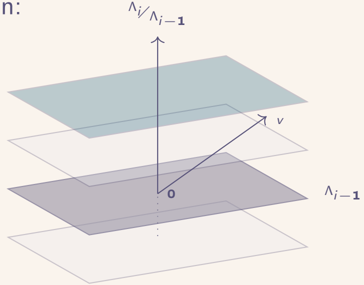
Effective lifting and size-reduction

Effective lifting

- Boils down to replace v_i by a *small* representative of a basis of $\Lambda' = v + \Lambda_{i-1}$:

  CVP instance

- Perform an *approx*-CVP by using the filtration:



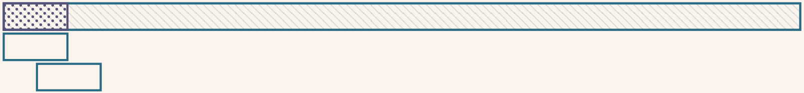
Size-reduction

for $k = 2$ **to** d **do**
  for $j = k-1$ **down to** 1 **do**
    $v_k \leftarrow v_k - \left\lceil \frac{\langle v_k, \pi_j(v_j)\rangle}{\|\pi_j(v_j)\|^2} \right\rfloor \cdot v_j$
  end for
end for
return $(v_1, \ldots, v_d)$

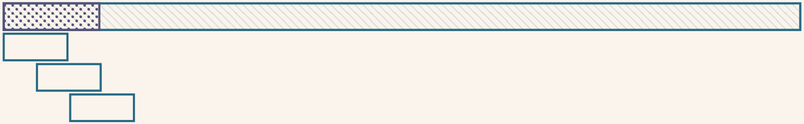
From local to global: an iterative strategy

From local to global: an iterative strategy

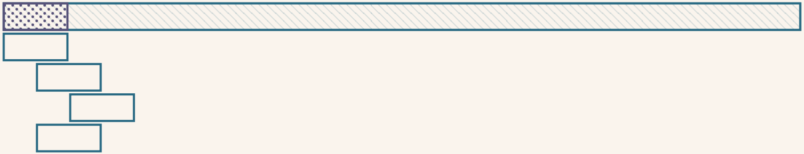
From local to global: an iterative strategy



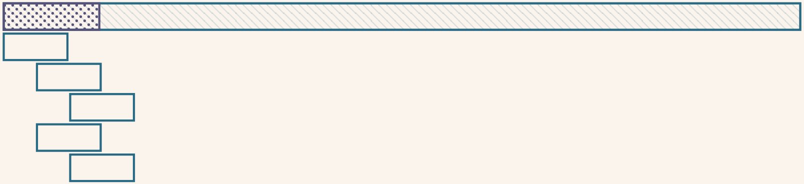
From local to global: an iterative strategy



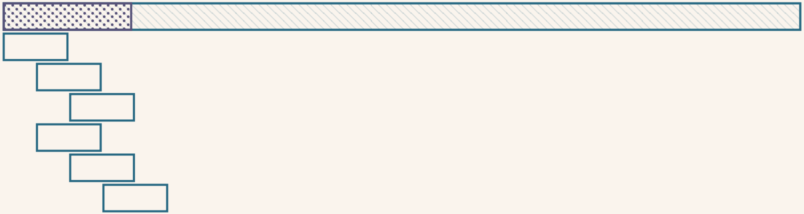
From local to global: an iterative strategy



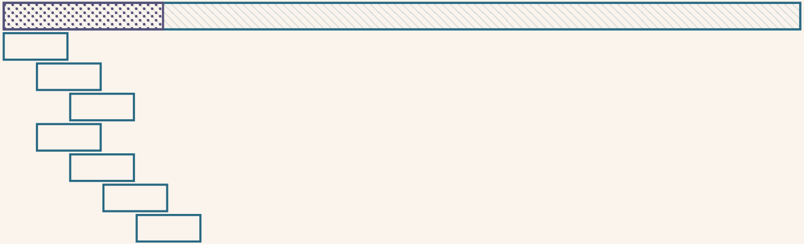
From local to global: an iterative strategy



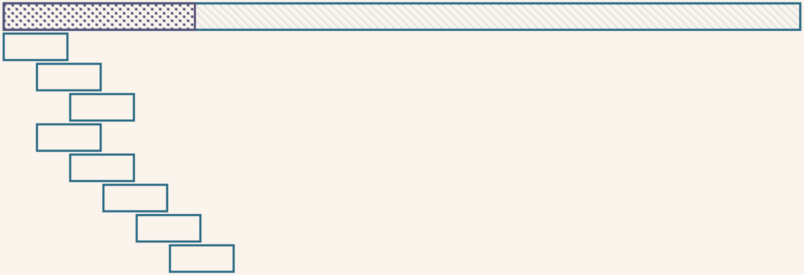
From local to global: an iterative strategy



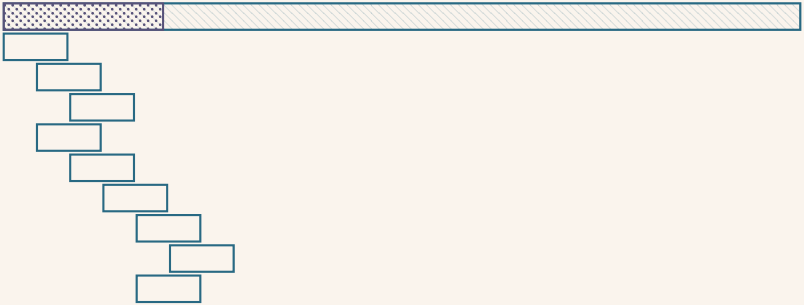
From local to global: an iterative strategy



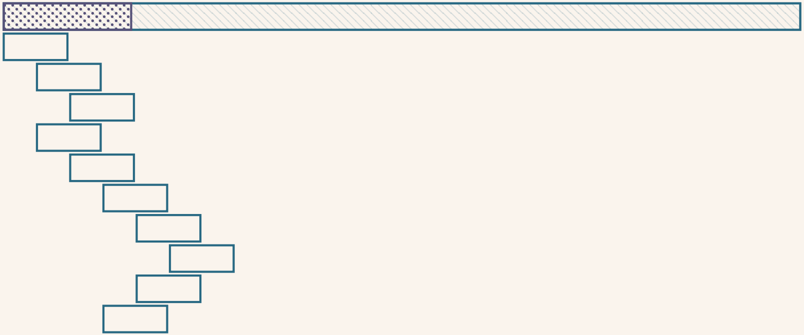
From local to global: an iterative strategy



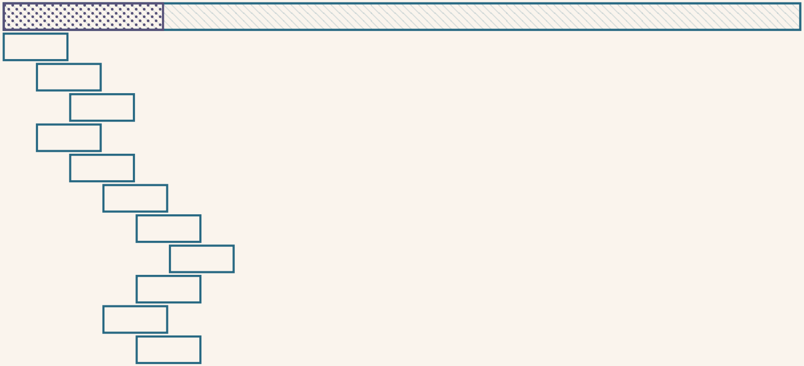
From local to global: an iterative strategy



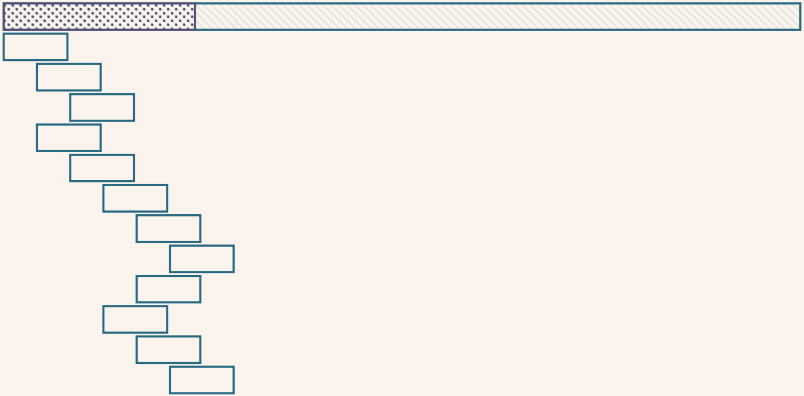
From local to global: an iterative strategy



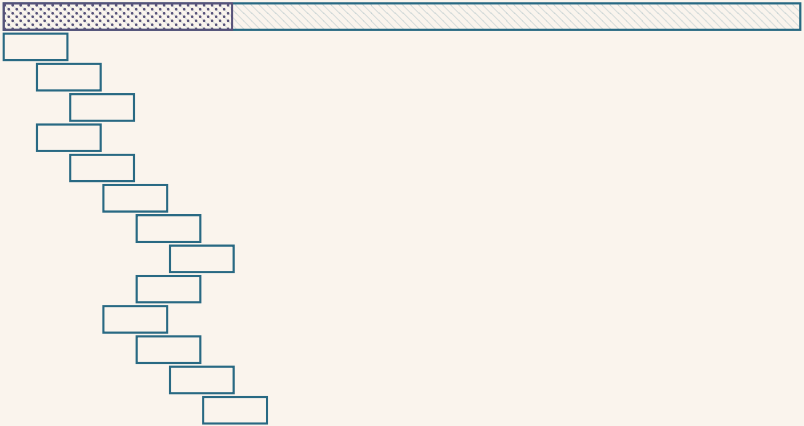
From local to global: an iterative strategy



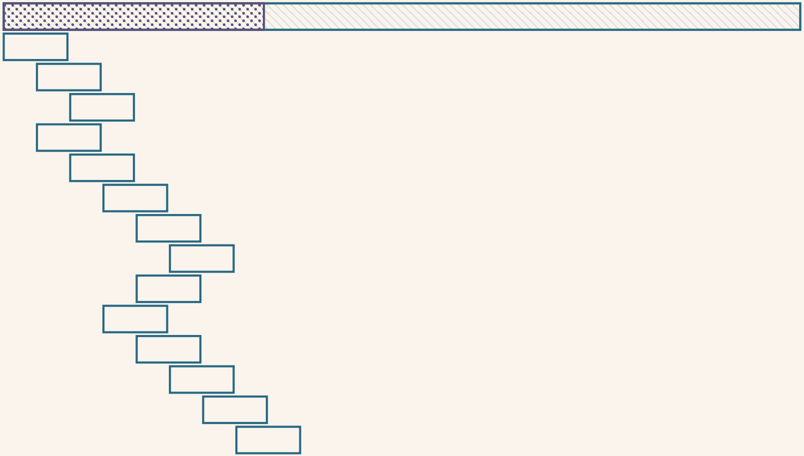
From local to global: an iterative strategy



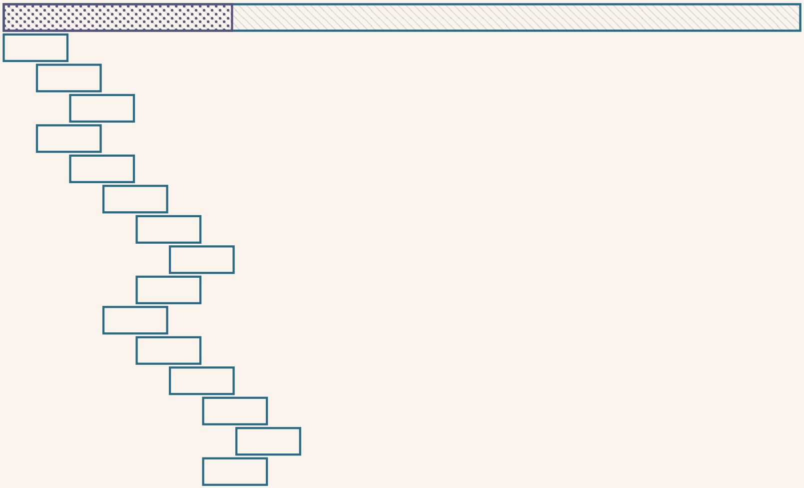
From local to global: an iterative strategy



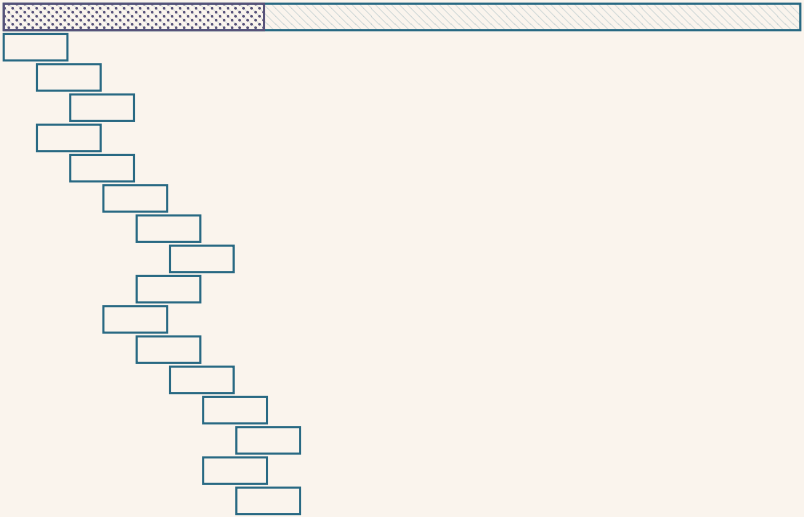
From local to global: an iterative strategy



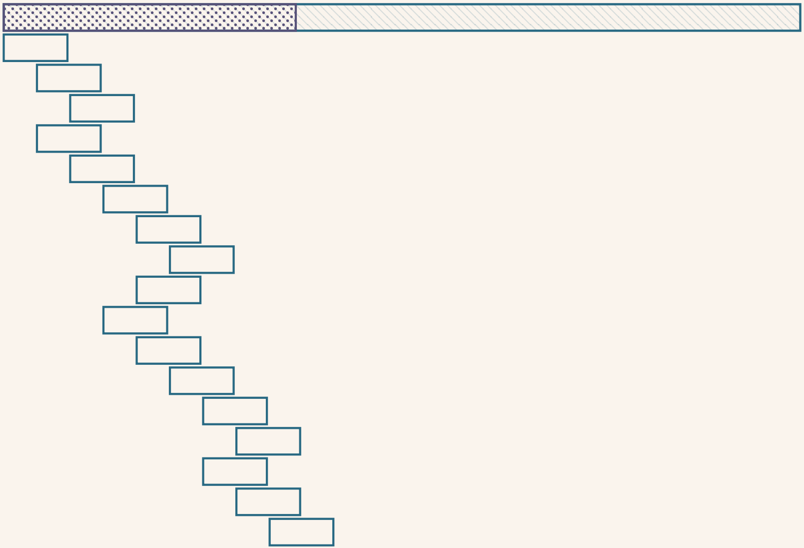
From local to global: an iterative strategy



From local to global: an iterative strategy



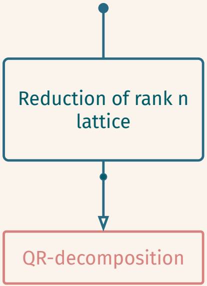
From local to global: an iterative strategy



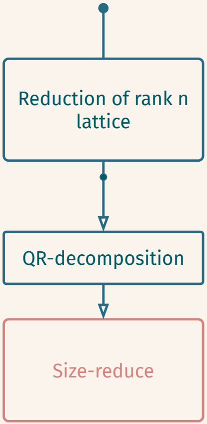
Diagramatically !

Reduction of rank n lattice

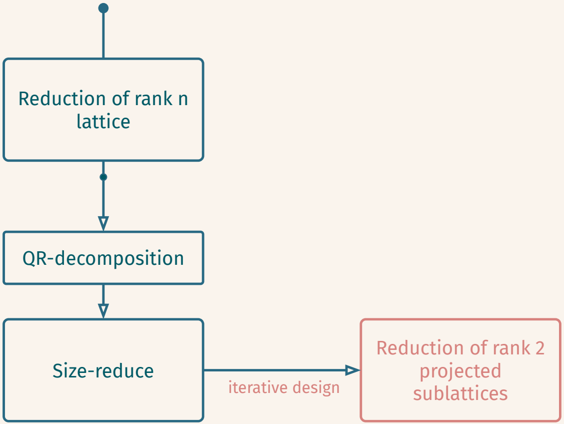
Diagramatically !



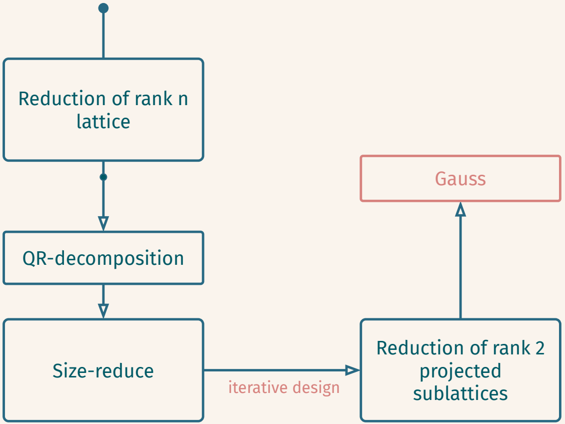
Diagramatically !



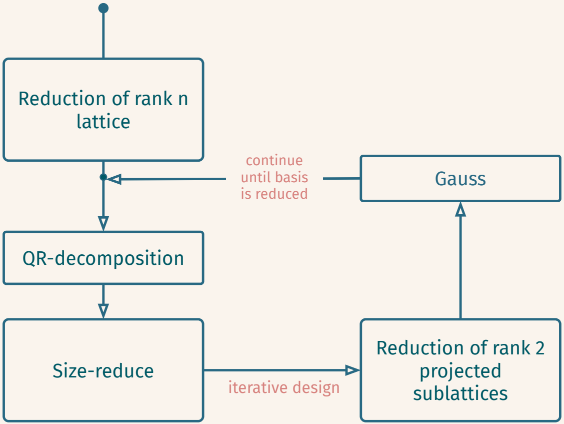
Diagramatically !



Diagramatically !



Diagramatically !



LLL reduced basis

LLL reduced basis

LLL reduced basis

LLL reduced basis

- Size-Reduction condition
  (*lifts is as good as possible*)

$$\forall i < j, \quad |\langle v_j, \pi_i(v_i) \rangle| \leqslant \frac{1}{2} \|\pi_i(v_i)\|^2$$

LLL reduced basis

LLL reduced basis

- Size-Reduction condition
  (*lifts is as good as possible*)

  $$\forall i < j, \quad |\langle v_j, \pi_i(v_i)\rangle| \leqslant \frac{1}{2}\|\pi_i(v_i)\|^2$$

- Lovász condition
  (*Each quotients are reduced*)

  $$\forall i, \;\; \delta\, \mathrm{covol}(\Lambda_i) \leqslant \mathrm{covol}(\Lambda_{i-1} \oplus v_{i+1}\mathbb{Z})$$

LLL reduced basis

LLL reduced basis

- Size-Reduction condition
  (*lifts is as good as possible*)

  $$\forall i < j, \quad |\langle v_j, \pi_i(v_i)\rangle| \leqslant \frac{1}{2}\|\pi_i(v_i)\|^2$$

- Lovász condition
  (*Each quotients are reduced*)

  $$\forall i, \ \delta \operatorname{covol}(\Lambda_i) \leqslant \operatorname{covol}(\Lambda_{i-1} \oplus v_{i+1}\mathbb{Z})$$

Effective version of Hermite's inequality:

$$\gamma_d \leqslant \gamma_2^{d-1}$$

Guarantees offered by LLL

$$\operatorname{covol}(\Lambda_k) \leqslant \left(\delta - \frac{1}{4}\right)^{-\frac{(d-k)k}{4}} \operatorname{covol}(\Lambda)^{\frac{k}{d}}$$

LLL reduced basis

LLL reduced basis

- Size-Reduction condition
  (*lifts is as good as possible*)

$$\forall i < j, \quad |\langle v_j, \pi_i(v_i)\rangle| \leqslant \frac{1}{2}\|\pi_i(v_i)\|^2$$

- Lovász condition
  (*Each quotients are reduced*)

$$\forall i, \;\; \delta \operatorname{covol}(\Lambda_i) \leqslant \operatorname{covol}(\Lambda_{i-1} \oplus v_{i+1}\mathbb{Z})$$

Peter van Emde Boas, László Lovász, Hendrik Lenstra and Arjen Lenstra.
(*Bonn* on 27/02/1982)

But... How fast is this reduction?

	Variant	Complexity	
naive arithmetic	Textbook	$\mathrm{O}\left(d^6 \log^3 \\|B\\|_\infty\right)$	naive
		$\mathrm{O}\left(\frac{d^5 \log^2 \\|B\\|_\infty}{d+\log \\|B\\|_\infty} M(d + \log \\|B\\|_\infty)\right)$	refined
	» Bottleneck: *size* of numerators/denominators in *GSO* computations «		
floating point	Nguyen-Stehlé (2009)	$\mathrm{O}\left(d^5(d + \log(\\|B\\|_\infty)) \log(\\|B\\|_\infty)\right)$	lazy size-reduction
	Neumaier-Stehlé (2016)	$\mathrm{O}\left(d^{4+\epsilon} \log(\\|B\\|_\infty)^{1+\epsilon}\right)$	recursive strategy

Generalization: towards algebraic lattices

Number fields and algebraic lattices

Number field

- Finite extension of $\mathbb{Q}$:

$$L \cong {}^{\mathbb{Q}[X]}\!\big/_{(P)}$$

- Ring of integers:

$$\mathcal{O}_L = \{\alpha \,|\, \exists R \in \mathbb{Z}[X] \text{ monic } , R(\alpha) = 0\}$$

Number field

- Finite extension of $\mathbb{Q}$:

$$L \cong {}^{\mathbb{Q}[X]}\!\diagup_{(P)}$$

- Ring of integers:

$$\mathcal{O}_L = \{\alpha \,|\, \exists R \in \mathbb{Z}[X] \text{ monic }, R(\alpha) = 0\}$$

Examples

$$\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$$
$$\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i] = \{a + ib \,|\, a, b \in \mathbb{Z}\}$$
$$\mathcal{O}_{\mathbb{Q}(i\sqrt{5})} = \left\{\frac{a}{2} + \frac{b}{2} i\sqrt{5} \mid a, b \in \mathbb{Z}\right\}$$
$$\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n] = \left\{\sum_i a_i \zeta^i \mid a_i \in \mathbb{Z}\right\}$$

Number fields and algebraic lattices

Number field

- Finite extension of $\mathbb{Q}$:

$$L \cong \mathbb{Q}[X]/_{(P)}$$

- Ring of integers:

$$\mathcal{O}_L = \{\alpha \mid \exists R \in \mathbb{Z}[X] \text{ monic }, R(\alpha) = 0\}$$

Examples

$$\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$$

$$\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$$

$$\mathcal{O}_{\mathbb{Q}(i\sqrt{5})} = \left\{\frac{a}{2} + \frac{b}{2} i\sqrt{5} \mid a, b \in \mathbb{Z}\right\}$$

$$\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n] = \left\{\sum_i a_i \zeta^i \mid a_i \in \mathbb{Z}\right\}$$

Lattice

A (Euclidean) lattice Λ is a *discrete* subgroup of a Euclidean space (say $\mathbb{R}^n$).

Number fields and algebraic lattices

Number field

- Finite extension of $\mathbb{Q}$:

$$L \cong {}^{\mathbb{Q}[X]}\!\big/\!{}_{(P)}$$

- Ring of integers:

$$\mathcal{O}_L = \{\alpha \mid \exists R \in \mathbb{Z}[X] \text{ monic }, R(\alpha) = 0\}$$

Examples

$$\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$$

$$\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$$

$$\mathcal{O}_{\mathbb{Q}(i\sqrt{5})} = \left\{\frac{a}{2} + \frac{b}{2} i\sqrt{5} \mid a, b \in \mathbb{Z}\right\}$$

$$\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n] = \left\{\sum_i a_i \zeta^i \mid a_i \in \mathbb{Z}\right\}$$

Lattice

A (Euclidean) lattice Λ is a free $\mathbb{Z}$-module of finite rank, endowed with an inner product on $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$.

Number field

- Finite extension of $\mathbb{Q}$:

$$L \cong \mathbb{Q}[X]/(P)$$

- Ring of integers:

$$\mathcal{O}_L = \{\alpha \mid \exists R \in \mathbb{Z}[X] \text{ monic }, R(\alpha) = 0\}$$

Examples

$$\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$$

$$\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$$

$$\mathcal{O}_{\mathbb{Q}(i\sqrt{5})} = \left\{\frac{a}{2} + \frac{b}{2} i\sqrt{5} \mid a, b \in \mathbb{Z}\right\}$$

$$\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n] = \left\{\sum_i a_i \zeta^i \mid a_i \in \mathbb{Z}\right\}$$

Lattice

An (algebraic) lattice Λ is a free $\mathcal{O}_L$-module of finite rank, endowed with an inner product on $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$.

Number fields and algebraic lattices

Number field

- Finite extension of $\mathbb{Q}$:

$$L \cong \mathbb{Q}[X]/(P)$$

- Ring of integers:

$$\mathcal{O}_L = \{\alpha \mid \exists R \in \mathbb{Z}[X] \text{ monic }, R(\alpha) = 0\}$$

Examples

$$\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$$

$$\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$$

$$\mathcal{O}_{\mathbb{Q}(i\sqrt{5})} = \left\{\frac{a}{2} + \frac{b}{2} i\sqrt{5} \mid a, b \in \mathbb{Z}\right\}$$

$$\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n] = \left\{\sum_i a_i \zeta^i \mid a_i \in \mathbb{Z}\right\}$$

Lattice

An (algebraic) lattice Λ is a **free** $\mathcal{O}_L$-module of finite rank, endowed with an inner product on $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$.

Number fields and algebraic lattices

Number field

- Finite extension of $\mathbb{Q}$:

$$L \cong \mathbb{Q}[X]/(P)$$

- Ring of integers:

$$\mathcal{O}_L = \{\alpha \mid \exists R \in \mathbb{Z}[X] \text{ monic }, R(\alpha) = 0\}$$

Examples

$$\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$$

$$\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$$

$$\mathcal{O}_{\mathbb{Q}(i\sqrt{5})} = \left\{\frac{a}{2} + \frac{b}{2} i\sqrt{5} \mid a, b \in \mathbb{Z}\right\}$$

$$\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n] = \left\{\sum_i a_i \zeta^i \mid a_i \in \mathbb{Z}\right\}$$

Lattice

An (algebraic) lattice Λ is a free $\mathcal{O}_L$-module of finite rank, endowed with an inner product on $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$.

Let's look at the trace on $(L \otimes \mathbb{R})^d$

Number fields and algebraic lattices

(Natural?) Hermitian structure

Take your favorite sesquilinear map
$g : \Lambda_{\mathbb{R}} \times \Lambda_{\mathbb{R}} \to L_{\mathbb{R}}$ (for instance as vectors
$g(x, y) = \sum_i \bar{x}_i y_i$)

Lattice

An (algebraic) lattice Λ is a free $\mathcal{O}_L$-module of finite rank, endowed with an inner product on $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$.

Let's look at the trace on $(L \otimes \mathbb{R})^d$

Number fields and algebraic lattices

(Natural?) Hermitian structure

Take your favorite sesquilinear map $g : \Lambda_{\mathbb{R}} \times \Lambda_{\mathbb{R}} \to L_{\mathbb{R}}$ (for instance as vectors $g(x, y) = \sum_i \bar{x}_i y_i$)

- not very *real* ! (distance, etc...)
- How do we go from L to $\mathbb{R}$? Compose with ...

Lattice

An (algebraic) lattice Λ is a free $\mathcal{O}_L$-module of finite rank, endowed with an inner product on $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$.

Let's look at the trace on $(L \otimes \mathbb{R})^d$

Number fields and algebraic lattices

(Natural?) Hermitian structure

Take your favorite sesquilinear map $g : \Lambda_{\mathbb{R}} \times \Lambda_{\mathbb{R}} \to L_{\mathbb{R}}$ (for instance as vectors $g(x, y) = \sum_i \bar{x}_i y_i$)

- not very *real* ! (distance, etc...)
- How do we go from L to $\mathbb{R}$? Compose with ...

Trace tr	Norm N
Additive notion	*Multiplicative notion*
encode the length of the element when seen as a vector in $\mathbb{C}^{\deg(L)}$.	encode the $\deg(L)$ - "volume" of the lattice spanned by the element)
Better for the geometry !	*better with the arithmetic !*

Lattice

An (algebraic) lattice Λ is a free $\mathcal{O}_L$-module of finite rank, endowed with an inner product on $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$.

Let's look at the trace on $(L \otimes \mathbb{R})^d$

Number fields and algebraic lattices

(Natural?) Hermitian structure

Take your favorite sesquilinear map $g : \Lambda_{\mathbb{R}} \times \Lambda_{\mathbb{R}} \to L_{\mathbb{R}}$ (for instance as vectors $g(x, y) = \sum_i \bar{x}_i y_i$)

- not very *real* ! (distance, etc...)
- How do we go from L to $\mathbb{R}$? Compose with ...

Trace tr	Norm N
Additive notion	*Multiplicative notion*
encode the length of the element when seen as a vector in $\mathbb{C}^{\deg(L)}$.	encode the $\deg(L)$ - "volume" of the lattice spanned by the element)
Better for the geometry !	*better with the arithmetic !*

Lattice

An (algebraic) lattice Λ is a free $\mathcal{O}_L$-module of finite rank, endowed with an inner product on $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$.

Let's look at the trace on $(L \otimes \mathbb{R})^d$

For any $x = (x_1, \ldots, x_d) \in (L \otimes \mathbb{R})^d$ and $y = (y_1, \ldots, y_d) \in (L \otimes \mathbb{R})^d$:

$$\langle x, y \rangle =$$

Number fields and algebraic lattices

(Natural?) Hermitian structure

Take your favorite sesquilinear map $g : \Lambda_{\mathbb{R}} \times \Lambda_{\mathbb{R}} \to L_{\mathbb{R}}$ (for instance as vectors $g(x, y) = \sum_i \bar{x}_i y_i$)

- not very *real* ! (distance, etc...)
- How do we go from L to $\mathbb{R}$? Compose with ...

Trace tr	Norm N
Additive notion	*Multiplicative notion*
encode the length of the element when seen as a vector in $\mathbb{C}^{\deg(L)}$.	encode the $\deg(L)$ - "volume" of the lattice spanned by the element)
Better for the geometry !	*better with the arithmetic !*

Lattice

An (algebraic) lattice Λ is a free $\mathcal{O}_L$-module of finite rank, endowed with an inner product on $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$.

Let's look at the trace on $(L \otimes \mathbb{R})^d$

For any $x = (x_1, \ldots, x_d) \in (L \otimes \mathbb{R})^d$ and $y = (y_1, \ldots, y_d) \in (L \otimes \mathbb{R})^d$:

$$\langle x, y \rangle = \sum_{i=1}^{d} \langle x_i, y_i \rangle_\Sigma$$

Number fields and algebraic lattices

(Natural?) Hermitian structure

Take your favorite sesquilinear map $g : \Lambda_{\mathbb{R}} \times \Lambda_{\mathbb{R}} \to L_{\mathbb{R}}$ (for instance as vectors $g(x, y) = \sum_i \bar{x}_i y_i$)

- not very *real* ! (distance, etc...)
- How do we go from L to $\mathbb{R}$? Compose with ...

Trace tr *Additive notion*	Norm N *Multiplicative notion*
encode the length of the element when seen as a vector in $\mathbb{C}^{\deg(L)}$.	encode the $\deg(L)$ - "volume" of the lattice spanned by the element)
Better for the geometry !	*better with the arithmetic !*

Lattice

An (algebraic) lattice Λ is a free $\mathcal{O}_L$-module of finite rank, endowed with an inner product on $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$.

Let's look at the trace on $(L \otimes \mathbb{R})^d$

For any $x = (x_1, \dots, x_d) \in (L \otimes \mathbb{R})^d$ and $y = (y_1, \dots, y_d) \in (L \otimes \mathbb{R})^d$:

$$\langle x, y \rangle = \sum_{\sigma : L \to \mathbb{C}} \langle x, y \rangle_\sigma$$

Number fields and algebraic lattices

(Natural?) Hermitian structure

Take your favorite sesquilinear map $g : \Lambda_{\mathbb{R}} \times \Lambda_{\mathbb{R}} \to L_{\mathbb{R}}$ (for instance as vectors $g(x, y) = \sum_i \bar{x}_i y_i$)

- not very *real* ! (distance, etc...)
- How do we go from L to $\mathbb{R}$? Compose with ...

Trace tr

Additive notion

encode the length of the element when seen as a vector in $\mathbb{C}^{\deg(L)}$.

Better for the geometry !

Norm N

Multiplicative notion

encode the $\deg(L)$ - "volume" of the lattice spanned by the element)

better with the arithmetic !

Lattice

An (algebraic) lattice Λ is a free $\mathcal{O}_L$-module of finite rank, endowed with an inner product on $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$.

Let's look at the trace on $(L \otimes \mathbb{R})^d$

For any $x = (x_1, \ldots, x_d) \in (L \otimes \mathbb{R})^d$ and $y = (y_1, \ldots, y_d) \in (L \otimes \mathbb{R})^d$:

$$\langle x, Hy \rangle = \sum_{\sigma : L \to \mathbb{C}} \langle x, H_\sigma y \rangle_\sigma$$

(Natural?) Hermitian structure

Take your favorite sesquilinear map $g : \Lambda_{\mathbb{R}} \times \Lambda_{\mathbb{R}} \to L_{\mathbb{R}}$ (for instance as vectors $g(x, y) = \sum_i \bar{x}_i y_i$)

- not very *real* ! (distance, etc...)
- How do we go from L to $\mathbb{R}$? Compose with ...

Trace tr	Norm N
Additive notion	*Multiplicative notion*
encode the length of the element when seen as a vector in $\mathbb{C}^{\deg(L)}$.	encode the $\deg(L)$ - "volume" of the lattice spanned by the element)
Better for the geometry !	*better with the arithmetic !*

Lattice

An (algebraic) lattice Λ is a free $\mathcal{O}_L$-module of finite rank, endowed with an inner product on $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$.

Let's look at the trace on $(L \otimes \mathbb{R})^d$

For any $x = (x_1, \ldots, x_d) \in (L \otimes \mathbb{R})^d$ and $y = (y_1, \ldots, y_d) \in (L \otimes \mathbb{R})^d$:

$$\langle x, Hy \rangle = \sum_{\sigma : L \to \mathbb{C}} \langle x, H_\sigma y \rangle_\sigma$$

Corresponds to **Humbert forms** (**"posdef symmetric" matrix over L**)

Algebraic lattice

Algebraic lattice

An algebraic lattice Λ is a projective $\mathcal{O}_L$-module of finite rank, endowed with a Humbert form on the space $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$.

Algebraic lattice

Algebraic lattice

An algebraic lattice Λ is a projective $\mathcal{O}_L$-module of finite rank, endowed with a Humbert form on the space $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$.

Examples I

- $\mathcal{O}_{\mathbb{Q}}^n = \mathbb{Z}^n$ is a rank n lattice for the form Id (!)
- $\mathcal{O}_L$ is a rank 1 lattice for the form $\mathrm{Id}_1 = (1)$
- $\mathcal{O}_L^2$ is a rank 2 lattice for the form Id_2
- $\begin{pmatrix} f \\ g \end{pmatrix} \mathcal{O}_L \oplus \begin{pmatrix} F \\ G \end{pmatrix} \mathcal{O}_L$ is a rank 2 lattice... (if f, g are small it's nothing less than NTRU).

Algebraic lattice

Algebraic lattice

An algebraic lattice Λ is a projective $\mathcal{O}_L$-module of finite rank, endowed with a Humbert form on the space $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$.

Examples II

- More complicated, adding projectivity in the mix:

$$\mathfrak{a} \subset (\mathcal{O}_L, \mathrm{Id}_1) \text{ is a sublattice of rank 1 (not free unless } \mathfrak{a} \text{ is principal)}$$

- As $\mathcal{O}_L$ is a Dedekind domain:

$$\mathcal{O}_L \cong v_1\mathfrak{a}_1 \oplus v_2\mathfrak{a}_2 \oplus \cdots \oplus v_n\mathfrak{a}_n$$

is the general form of a projective module of rank n.

Algebraic lattice

An algebraic lattice Λ is a projective $\mathcal{O}_L$-module of finite rank, endowed with a Humbert form on the space $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$.

Generic form of an algebraic lattice

$$\boxed{\left(v_1\mathfrak{a}_1 \oplus v_2\mathfrak{a}_2 \oplus \cdots \oplus v_n\mathfrak{a}_n \ , \ \left(H_\sigma\right)_{\sigma : L \to \mathbb{C}}\right)}$$

Algebraic lattice

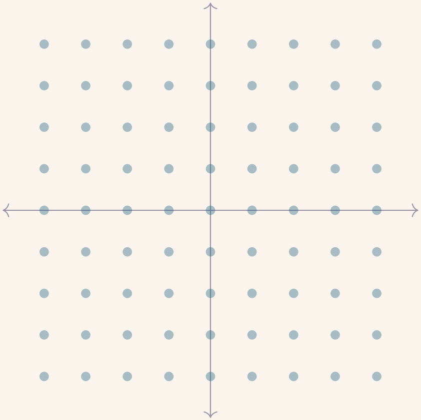
Algebraic lattice

An algebraic lattice Λ is a projective $\mathcal{O}_L$-module of finite rank, endowed with a Humbert form on the space $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$.

Generic form of an algebraic lattice

$$\Big(\underbrace{v_1\mathfrak{a}_1 \oplus v_2\mathfrak{a}_2 \oplus \cdots \oplus v_n\mathfrak{a}_n}_{\text{algebraic datum}} \,,\ \underbrace{(H_\sigma)_{\sigma:L\to\mathbb{C}}}_{\text{metric datum}} \Big)$$

A bit more examples, this time with drawings

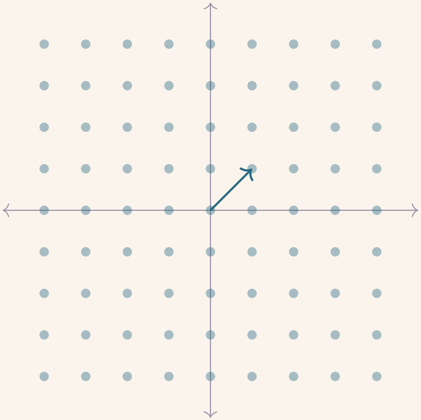


The Gaussian integers

- $\mathcal{O}$, ring of integer of
$$L = \mathbb{Q}(i) = {}^{\mathbb{Z}[T]}\!/_{T^2+1}$$
- $\mathcal{O} = \mathbb{Z}[i] := \{a + ib \mid a, b \in \mathbb{Z}^2\}$
- We take the identity form Id, so that the L-inner product is simply the multiplication: $(x, y) \mapsto \bar{x}y$.

(in dim 2,*already* in $\mathbb{Q}$: unclear *why* we need to norm or trace)

A bit more examples, this time with drawings



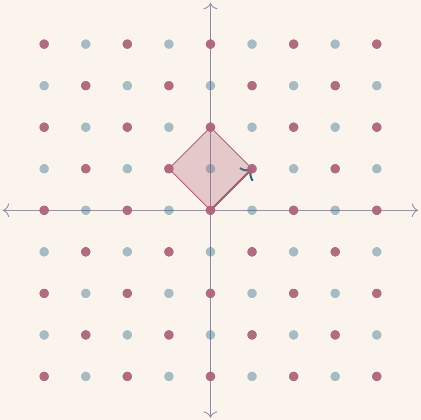
The Gaussian integers

- $\mathcal{O}$, ring of integer of
$$L = \mathbb{Q}(i) = {}^{\mathbb{Z}[T]}\!/\!_{T^2+1}$$
- $\mathcal{O} = \mathbb{Z}[i] := \{a + ib \mid a, b \in \mathbb{Z}^2\}$
- We take the identity form Id, so that the L-inner product is simply the multiplication: $(x, y) \mapsto \bar{x}y$.

(in dim 2,*already* in $\mathbb{Q}$: unclear *why* we need to norm or trace)

tracing vs. norming

A bit more examples, this time with drawings



The Gaussian integers

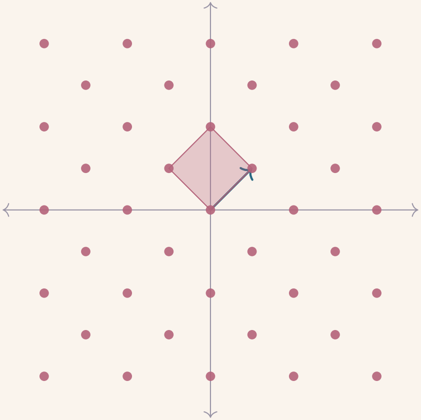
- $\mathcal{O}$, ring of integer of
$$L = \mathbb{Q}(i) = \mathbb{Z}[T]/_{T^2+1}$$
- $\mathcal{O} = \mathbb{Z}[i] := \{a + ib \mid a, b \in \mathbb{Z}^2\}$
- We take the identity form Id, so that the L-inner product is simply the multiplication: $(x, y) \mapsto \bar{x}y$.

(in dim 2, *already* in $\mathbb{Q}$: unclear *why* we need to norm or trace)

tracing vs. norming

- $\mathfrak{a} = (1 + i)\mathcal{O} = \{a + ib \mid a + b = 0[2]\}$

A bit more examples, this time with drawings



$\mathfrak{a}$ is both a dim 1 lattice (over $\mathcal{O}$) and a 2 dimensional lattice (over $\mathbb{Z}$)

The Gaussian integers

- $\mathcal{O}$, ring of integer of
$$L = \mathbb{Q}(i) = {}^{\mathbb{Z}[T]}\!/\!_{T^2+1}$$
- $\mathcal{O} = \mathbb{Z}[i] := \{a + ib \mid a, b \in \mathbb{Z}^2\}$
- We take the identity form Id, so that the L-inner product is simply the multiplication: $(x, y) \mapsto \bar{x}y$.

(in dim 2, *already* in $\mathbb{Q}$: unclear *why* we need to norm or trace)

tracing vs. norming

- $\mathfrak{a} = (1 + i)\mathcal{O} = \{a + ib \mid a + b = 0[2]\}$

Yet another example, without drawings but with sage

- $L = \mathbb{Q}(\zeta_8)$, ζ_8 a primitive 8th root of unity $\to$ cyclotomic field of degree 4

Playing with sagemath

Yet another example, without drawings but with sage

- $L = \mathbb{Q}(\zeta_8)$, ζ_8 a primitive 8th root of unity $\to$ cyclotomic field of degree 4

Playing with sagemath

```
sage:   L.<z> = CyclotomicField(8); L
```

Yet another example, without drawings but with sage

- $L = \mathbb{Q}(\zeta_8)$, ζ_8 a primitive 8th root of unity $\to$ cyclotomic field of degree 4

Playing with sagemath

```
sage:   L.<z> = CyclotomicField(8); L
        Cyclotomic Field of order 8 and degree 4
```

Yet another example, without drawings but with sage

- $L = \mathbb{Q}(\zeta_8)$, ζ_8 a primitive 8th root of unity $\to$ cyclotomic field of degree 4

Playing with sagemath

```
sage:   L.<z> = CyclotomicField(8); L
        Cyclotomic Field of order 8 and degree 4
sage:   O = L. maximal_order(); O.basis()
```

Yet another example, without drawings but with sage

- $L = \mathbb{Q}(\zeta_8)$, ζ_8 a primitive 8th root of unity $\rightarrow$ cyclotomic field of degree 4
- $\mathcal{O}_L = \mathbb{Z}[\zeta_8]$

Playing with sagemath

```
sage:   L.<z> = CyclotomicField(8); L
        Cyclotomic Field of order 8 and degree 4
sage:   O = L. maximal_order(); O.basis()
        [1, z, z**2, z**3]
```

Yet another example, without drawings but with sage

- $L = \mathbb{Q}(\zeta_8)$, ζ_8 a primitive 8th root of unity $\to$ cyclotomic field of degree 4
- $\mathcal{O}_L = \mathbb{Z}[\zeta_8]$
- Take the element $x = 1 + \zeta$. Since $\bar{\zeta} = -\zeta^3$, then $\bar{x}x = -\zeta^3 + \zeta + 2$

Playing with sagemath

```
sage:   L.<z> = CyclotomicField(8); L
        Cyclotomic Field of order 8 and degree 4
sage:   O = L. maximal_order(); O.basis()
        [1, z, z**2, z**3]
sage:   x = 1+z; XbarX =x.conjugate()*x; XbarX
```

Yet another example, without drawings but with sage

- $L = \mathbb{Q}(\zeta_8)$, ζ_8 a primitive 8th root of unity $\to$ cyclotomic field of degree 4
- $\mathcal{O}_L = \mathbb{Z}[\zeta_8]$
- Take the element $x = 1 + \zeta$. Since $\bar{\zeta} = -\zeta^3$, then $\bar{x}x = -\zeta^3 + \zeta + 2$

Playing with sagemath

```
sage:   L.<z> = CyclotomicField(8); L
        Cyclotomic Field of order 8 and degree 4
sage:   O = L. maximal_order(); O.basis()
        [1, z, z**2, z**3]
sage:   x = 1+z; XbarX =x.conjugate()*x; XbarX
        -z**3 + z + 2
```

Yet another example, without drawings but with sage

- $L = \mathbb{Q}(\zeta_8)$, ζ_8 a primitive 8th root of unity $\to$ cyclotomic field of degree 4
- $\mathcal{O}_L = \mathbb{Z}[\zeta_8]$
- Take the element $x = 1 + \zeta$. Since $\bar{\zeta} = -\zeta^3$, then $\bar{x}x = -\zeta^3 + \zeta + 2$

Playing with sagemath

```
sage:   L.<z> = CyclotomicField(8); L
        Cyclotomic Field of order 8 and degree 4
sage:   O = L. maximal_order(); O.basis()
        [1, z, z**2, z**3]
sage:   x = 1+z; XbarX =x.conjugate()*x; XbarX
        -z**3 + z + 2
sage:   XbarX.trace()/4, XbarX.norm()
```

Yet another example, without drawings but with sage

- $L = \mathbb{Q}(\zeta_8)$, ζ_8 a primitive 8th root of unity $\rightarrow$ cyclotomic field of degree 4
- $\mathcal{O}_L = \mathbb{Z}[\zeta_8]$
- Take the element $x = 1 + \zeta$. Since $\bar{\zeta} = -\zeta^3$, then $\bar{x}x = -\zeta^3 + \zeta + 2$
- We can look at the quotient ${}^{\mathcal{O}}\!/_{x\mathcal{O}}$: on the board

Playing with sagemath

```
sage:   L.<z> = CyclotomicField(8); L
        Cyclotomic Field of order 8 and degree 4
sage:   O = L. maximal_order(); O.basis()
        [1, z, z**2, z**3]
sage:   x = 1+z; XbarX =x.conjugate()*x; XbarX
        -z**3 + z + 2
sage:   XbarX.trace()/4, XbarX.norm()
        (2,4)
```

Yet another example, without drawings but with sage

- $L = \mathbb{Q}(\zeta_8)$, ζ_8 a primitive 8th root of unity $\rightarrow$ cyclotomic field of degree 4
- $\mathcal{O}_L = \mathbb{Z}[\zeta_8]$
- Take the element $x = 1 + \zeta$. Since $\bar{\zeta} = -\zeta^3$, then $\bar{x}x = -\zeta^3 + \zeta + 2$
- We can look at the quotient ${}^{\mathcal{O}}\!/_{x\mathcal{O}}$: on the board

Playing with sagemath

```
sage:   L.<z> = CyclotomicField(8); L
        Cyclotomic Field of order 8 and degree 4
sage:   O = L. maximal_order(); O.basis()
        [1, z, z**2, z**3]
sage:   x = 1+z; XbarX =x.conjugate()*x; XbarX
        -z**3 + z + 2
sage:   XbarX.trace()/4, XbarX.norm()
        (2,4)
sage:   G=matrix([[((z**i*x).conj()*z**j*x).trace()/4
               for i in range(4)] for j in range(4)])
```

Yet another example, without drawings but with sage

- $L = \mathbb{Q}(\zeta_8)$, ζ_8 a primitive 8th root of unity $\to$ cyclotomic field of degree 4
- $\mathcal{O}_L = \mathbb{Z}[\zeta_8]$
- Take the element $x = 1 + \zeta$. Since $\bar{\zeta} = -\zeta^3$, then $\bar{x}x = -\zeta^3 + \zeta + 2$
- We can look at the quotient $\mathcal{O}/_{x\mathcal{O}}$: on the board

Playing with sagemath

```
sage:   L.<z> = CyclotomicField(8); L
        Cyclotomic Field of order 8 and degree 4
sage:   O = L. maximal_order(); O.basis()
        [1, z, z**2, z**3]
sage:   x = 1+z; XbarX =x.conjugate()*x; XbarX
        -z**3 + z + 2
sage:   XbarX.trace()/4, XbarX.norm()
        (2,4)
sage:   G=matrix([[((z**i*x).conj()*z**j*x).trace()/4
                for i in range(4)] for j in range(4)])
```

$$\begin{pmatrix} 2 & 1 & 0 & -1 \\ 1 & 2 & 1 & 0 \\ 0 & 1 & 2 & 1 \\ -1 & 0 & 1 & 2 \end{pmatrix}$$

Yet another example, without drawings but with sage

- $L = \mathbb{Q}(\zeta_8)$, ζ_8 a primitive 8th root of unity $\to$ cyclotomic field of degree 4
- $\mathcal{O}_L = \mathbb{Z}[\zeta_8]$
- Take the element $x = 1 + \zeta$. Since $\bar{\zeta} = -\zeta^3$, then $\bar{x}x = -\zeta^3 + \zeta + 2$
- We can look at the quotient $\mathcal{O}/_{x\mathcal{O}}$: on the board

Playing with sagemath

```
sage:  L.<z> = CyclotomicField(8); L
       Cyclotomic Field of order 8 and degree 4
sage:  O = L. maximal_order(); O.basis()
       [1, z, z**2, z**3]
sage:  x = 1+z; XbarX =x.conjugate()*x; XbarX
       -z**3 + z + 2
sage:  XbarX.trace()/4, XbarX.norm()
       (2,4)
sage:  G=matrix([[((z**i*x).conj()*z**j*x).trace()/4
              for i in range(4)] for j in range(4)])
```

$$\begin{pmatrix} 2 & 1 & 0 & -1 \\ 1 & 2 & 1 & 0 \\ 0 & 1 & 2 & 1 \\ -1 & 0 & 1 & 2 \end{pmatrix}$$

```
sage:  G[0], det(G)
```

Yet another example, without drawings but with sage

- $L = \mathbb{Q}(\zeta_8)$, ζ_8 a primitive 8th root of unity $\to$ cyclotomic field of degree 4
- $\mathcal{O}_L = \mathbb{Z}[\zeta_8]$
- Take the element $x = 1 + \zeta$. Since $\bar{\zeta} = -\zeta^3$, then $\bar{x}x = -\zeta^3 + \zeta + 2$
- We can look at the quotient ${}^{\mathcal{O}}\!/\!{}_{x\mathcal{O}}$: on the board

Playing with sagemath

```
sage:  L.<z> = CyclotomicField(8); L
       Cyclotomic Field of order 8 and degree 4
sage:  O = L. maximal_order(); O.basis()
       [1, z, z**2, z**3]
sage:  x = 1+z; XbarX =x.conjugate()*x; XbarX
       -z**3 + z + 2
sage:  XbarX.trace()/4, XbarX.norm()
       (2,4)
sage:  G=matrix([[((z**i*x).conj()*z**j*x).trace()/4
              for i in range(4)] for j in range(4)])
```

$$\begin{pmatrix} 2 & 1 & 0 & -1 \\ 1 & 2 & 1 & 0 \\ 0 & 1 & 2 & 1 \\ -1 & 0 & 1 & 2 \end{pmatrix}$$

```
sage:  G[0], det(G)
       (2,4)
```

On the recursive structure of algebraic lattices: baby Galois descent

$$\begin{tikzcd}
L & \mathcal{O}_L \arrow[rr, dash, dashed] & & \Lambda \\
K \arrow[u] & \mathcal{O}_K \arrow[u] \arrow[urr, dash, dashed] & & \\
\mathbb{Q} \arrow[u] & \mathbb{Z} \arrow[u] \arrow[uurr, dash, dashed] & &
\end{tikzcd}$$

- The structure of an algebraic module is not unique. It depends on the base ring.
- For a tower $\mathbb{Q} \subset K \subset L$, an $\mathcal{O}_L$ lattice can be *descended* to:
  - an $\mathcal{O}_K$ lattice (of rank $\times[L : K]$)
  - a $\mathbb{Z}$ lattice (of rank $\times[L : \mathbb{Q}]$).
- The form is descended *canonically*

On the recursive structure of algebraic lattices: baby Galois descent

$$\begin{tikzcd}
L & \mathcal{O}_L \arrow[rr, dash, dashed] & & \Lambda \\
K \arrow[u] & \mathcal{O}_K \arrow[u] \arrow[urr, dash, dashed] & & \\
\mathbb{Q} \arrow[u] & \mathbb{Z} \arrow[u] \arrow[uurr, dash, dashed] & &
\end{tikzcd}$$

- The structure of an algebraic module is not unique. It depends on the base ring.
- For a tower $\mathbb{Q} \subset K \subset L$, an $\mathcal{O}_L$ lattice can be *descended* to:
  - an $\mathcal{O}_K$ lattice (of rank $\times[L : K]$)
  - a $\mathbb{Z}$ lattice (of rank $\times[L : \mathbb{Q}]$).
- The form is descended *canonically*
- Over $\mathbb{Z}$, recovers the *trace norm* (here we know how to do the reduction !)

How to do reduction at the top level, for the norm?

A very philosophical question

What is the *right* notion of λ_1 ?

A very philosophical question

What is the *right* notion of λ_1 ?

- Is it the shortest vector? (vector taken for trace norm) (in this case use $\mathbb{Z}$-lattice reduction for tr)
- Is it the densest (free? projective?) sublattice of rank 1? (vector/vector+ideal taken by the volume) ... but How?

A very philosophical question

What is the *right* notion of λ_1 ?

"I can't cut the grass until I find the lawnmower and I can't find the lawnmower until I cut the grass"

Reduction of algebraic lattices

How to attack the reduction problem?

$\rightarrow$ **Idea**: Try to keep the core design principles of what we saw.

How to attack the reduction problem?

(Pseudo)-basis $(v_1\mathfrak{a}_1, \ldots, v_d\mathfrak{a}_d)$ gives

$$\Lambda_i = v_1\mathcal{O}_L \oplus \cdots \oplus v_i\mathcal{O}_L$$

$$\{0\} \subset \Lambda_1 \subset \cdots \subset \Lambda_i \subset \cdots \subset \Lambda_d = \Lambda$$

$\rightarrow$ **Idea**: Try to keep the core design principles of what we saw.

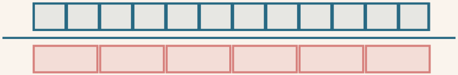
- Work on $\mathcal{O}_L$-filtrations of the lattice

How to attack the reduction problem?

→ **Idea**: Try to keep the core design principles of what we saw.

- Work on $\mathcal{O}_L$-filtrations of the lattice
- Reduce to a rank 2 oracle on projected quotients

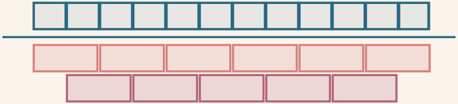
How to attack the reduction problem?



$\rightarrow$ **Idea**: Try to keep the core design principles of what we saw.

- Work on $\mathcal{O}_L$-filtrations of the lattice
- Reduce to a rank 2 oracle on projected quotients

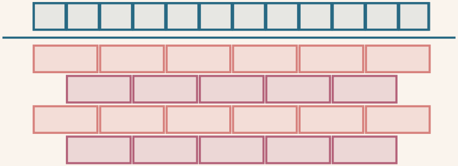
How to attack the reduction problem?



→ **Idea**: Try to keep the core design principles of what we saw.

- Work on $\mathcal{O}_L$-filtrations of the lattice
- Reduce to a rank 2 oracle on projected quotients

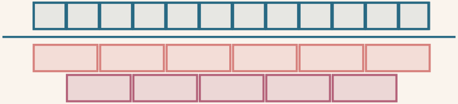
How to attack the reduction problem?



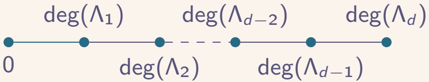
→ **Idea**: Try to keep the core design principles of what we saw.

- Work on $\mathcal{O}_L$-filtrations of the lattice
- Reduce to a rank 2 oracle on projected quotients

How to attack the reduction problem?



A round of local reductions acts as a *discretized* Laplacian operator on the profile space':



- (discrete) *diffusion property* of the solution of the heat equation

$$\frac{\partial u}{\partial t} = \alpha \Delta u$$

- Characteristic time is quadratic in the diameter of the space $\to O(d^2)$ steps

$\to$ **Idea**: Try to keep the core design principles of what we saw.

- Work on $\mathcal{O}_L$-filtrations of the lattice
- Reduce to a rank 2 oracle on projected quotients

How to attack the reduction problem?

- Over $\mathbb{Z}$: requires integral rounding

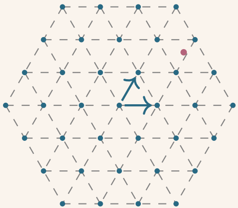
$\rightarrow$ **Idea**: Try to keep the core design principles of what we saw.

- Work on $\mathcal{O}_L$-filtrations of the lattice
- Reduce to a rank 2 oracle on projected quotients
- Size-reduction?

How to attack the reduction problem?

- Over $\mathbb{Z}$: requires integral rounding

- Translated over $\mathcal{O}_L$: find the closest element in the ring: instance of CVP



- Approx-CVP suffices (just do the coefficient-wise rounding!)

$\to$ **Idea**: Try to keep the core design principles of what we saw.

- Work on $\mathcal{O}_L$-filtrations of the lattice
- Reduce to a rank 2 oracle on projected quotients
- Size-reduction?

How to attack the reduction problem?

In $L = \mathbb{Q}[\zeta_{16}]$:

$$x = \frac{65210}{3}\zeta^7 + \frac{78658}{3}\zeta^6 - 41412\zeta^5 + \frac{16567}{3}\zeta^4 + 36970\zeta^3 - \frac{100235}{3}\zeta^2 - \frac{145843}{12}\zeta + \frac{86961}{2}.$$

- We have: $N_{L/\mathbb{Q}}(x)^{\frac{1}{8}} \approx 6.6758$
- Embeddings:

$$|\sigma_1(x)| = |\sigma_{15}(x)| \approx 2771.189$$
$$|\sigma_3(x)| = |\sigma_{13}(x)| \approx 1.558406 \times 10^{-08}$$
$$|\sigma_5(x)| = |\sigma_{11}(x)| \approx 172334.9$$
$$|\sigma_7(x)| = |\sigma_9(x)| \approx 266.8642.$$

$\rightarrow$ **Idea**: Try to keep the core design principles of what we saw.

- Work on $\mathcal{O}_L$-filtrations of the lattice
- Reduce to a rank 2 oracle on projected quotients
- Size-reduction?

How to attack the reduction problem?

In $L = \mathbb{Q}[\zeta_{16}]$:

$$x = \frac{65210}{3}\zeta^7 + \frac{78658}{3}\zeta^6 - 41412\zeta^5 + \frac{16567}{3}\zeta^4 + 36970\zeta^3 - \frac{100235}{3}\zeta^2 - \frac{145843}{12}\zeta + \frac{86961}{2}.$$

- We have: $N_{L/\mathbb{Q}}(x)^{\frac{1}{8}} \approx 6.6758$
- Embeddings:

$$|\sigma_1(x)| = |\sigma_{15}(x)| \approx 2771.189$$
$$|\sigma_3(x)| = |\sigma_{13}(x)| \approx 1.558406 \times 10^{-08}$$
$$|\sigma_5(x)| = |\sigma_{11}(x)| \approx 172334.9$$
$$|\sigma_7(x)| = |\sigma_9(x)| \approx 266.8642.$$

$\rightarrow$ **Idea**: Try to keep the core design principles of what we saw.

- Work on $\mathcal{O}_L$-filtrations of the lattice
- Reduce to a rank 2 oracle on projected quotients
- Size-reduction?

Unit rounding for cyclotomics

There is a quasi-linear randomized algorithm that given $x \in (\mathbb{R} \otimes K)^\times$ finds unit $u \in \mathcal{O}_K^\times$ such that for any field embedding $\sigma : K \to \mathbb{C}$:

$$\sigma\left(xu^{-1}\right) = 2^{\mathrm{O}\left(\sqrt{f \log f}\right)} N_{K/\mathbb{Q}}(x)^{\frac{1}{\varphi(f)}}$$

How to attack the reduction problem?

In $L = \mathbb{Q}[\zeta_{16}]$:

$$x = \frac{65210}{3}\zeta^7 + \frac{78658}{3}\zeta^6 - 41412\zeta^5 + \frac{16567}{3}\zeta^4 + 36970\zeta^3 - \frac{100235}{3}\zeta^2 - \frac{145843}{12}\zeta + \frac{86961}{2}.$$

- We have: $N_{L/\mathbb{Q}}(x)^{\frac{1}{8}} \approx 6.6758$
- When using **Unit**:

$$\left|\sigma_1\left(\frac{x}{u}\right)\right| = \left|\sigma_{15}\left(\frac{x}{u}\right)\right| \approx 7.83729$$
$$\left|\sigma_3\left(\frac{x}{u}\right)\right| = \left|\sigma_{13}\left(\frac{x}{u}\right)\right| \approx 7.33868$$
$$\left|\sigma_5\left(\frac{x}{u}\right)\right| = \left|\sigma_{11}\left(\frac{x}{u}\right)\right| \approx 5.93346$$
$$\left|\sigma_7\left(\frac{x}{u}\right)\right| = \left|\sigma_9\left(\frac{x}{u}\right)\right| \approx 5.82028.$$

→ **Idea**: Try to keep the core design principles of what we saw.

- Work on $\mathcal{O}_L$-filtrations of the lattice
- Reduce to a rank 2 oracle on projected quotients
- Size-reduction?

Unit rounding for cyclotomics

There is a quasi-linear randomized algorithm that given $x \in (\mathbb{R} \otimes K)^\times$ finds unit $u \in \mathcal{O}_K^\times$ such that for any field embedding $\sigma : K \to \mathbb{C}$:

$$\sigma\left(xu^{-1}\right) = 2^{\mathrm{O}\left(\sqrt{f \log f}\right)} N_{K/\mathbb{Q}}(x)^{\frac{1}{\varphi(f)}}$$

How to attack the reduction problem?

Size-Reduce

```
U ← Id_{d,d}
for i = 1 to d do
    D ← D_i(Unit(R_{i,i}));
    (U, R) ← (U, R) · D^{-1} ;
    for j = i − 1 down to 1 do
        Σ_{ℓ=0}^{n−1} r_ℓ X^ℓ ← R_{i,j} / R_{j,j}
        μ ← Σ_{ℓ=0}^{n−1} ⌊r_ℓ⌉ X^ℓ
        (U, R) *= T_{i,j}(−μ)
    end for
end for
return U
```

→ **Idea**: Try to keep the core design principles of what we saw.

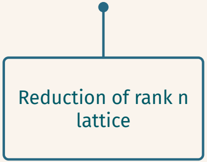
- Work on $\mathcal{O}_L$-filtrations of the lattice
- Reduce to a rank 2 oracle on projected quotients
- Size-reduction?

Unit rounding for cyclotomics

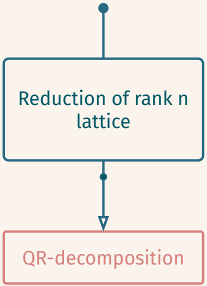
There is a quasi-linear randomized algorithm that given $x \in (\mathbb{R} \otimes K)^\times$ finds unit $u \in \mathcal{O}_K^\times$ such that for any field embedding $\sigma : K \to \mathbb{C}$:

$$\sigma\left(xu^{-1}\right) = 2^{\mathrm{O}\left(\sqrt{f \log f}\right)} N_{K/\mathbb{Q}}(x)^{\frac{1}{\varphi(f)}}$$

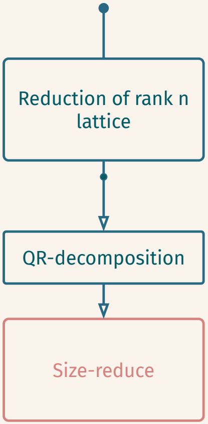
As a flowchart



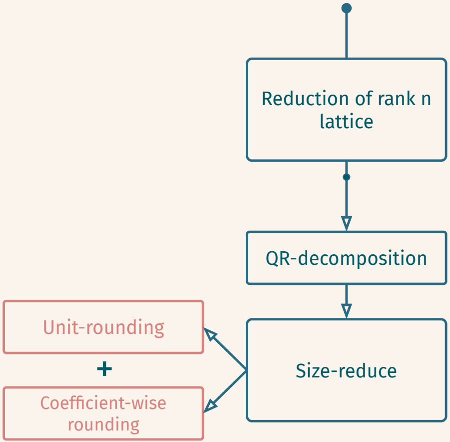
As a flowchart



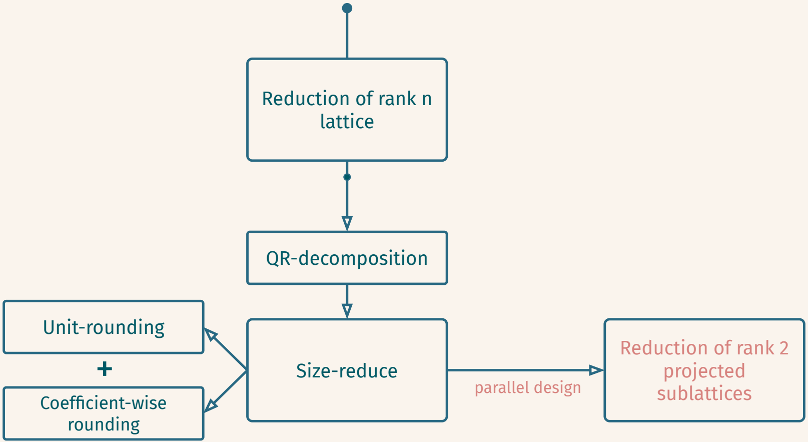
As a flowchart



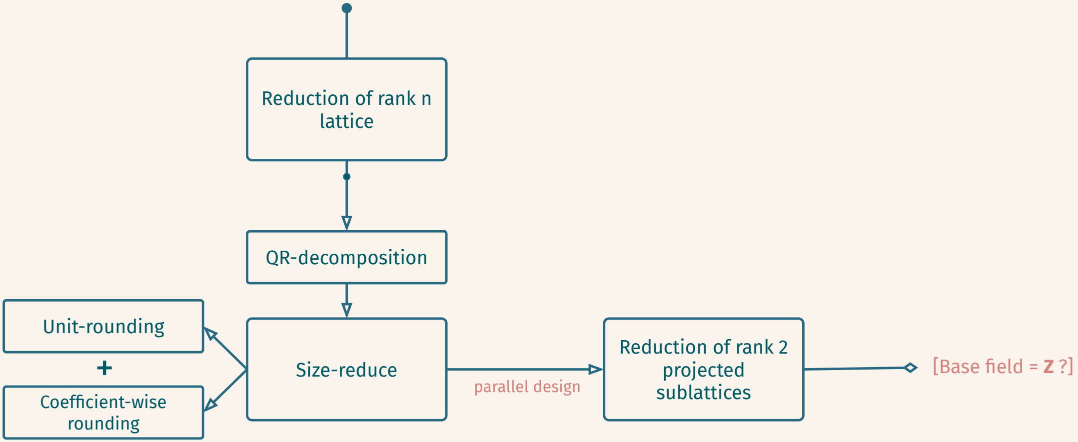
As a flowchart



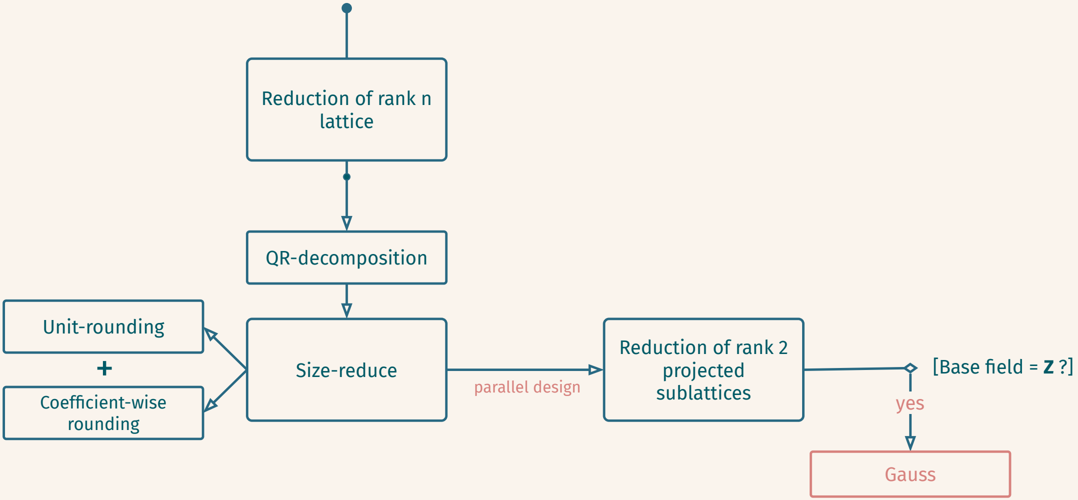
As a flowchart



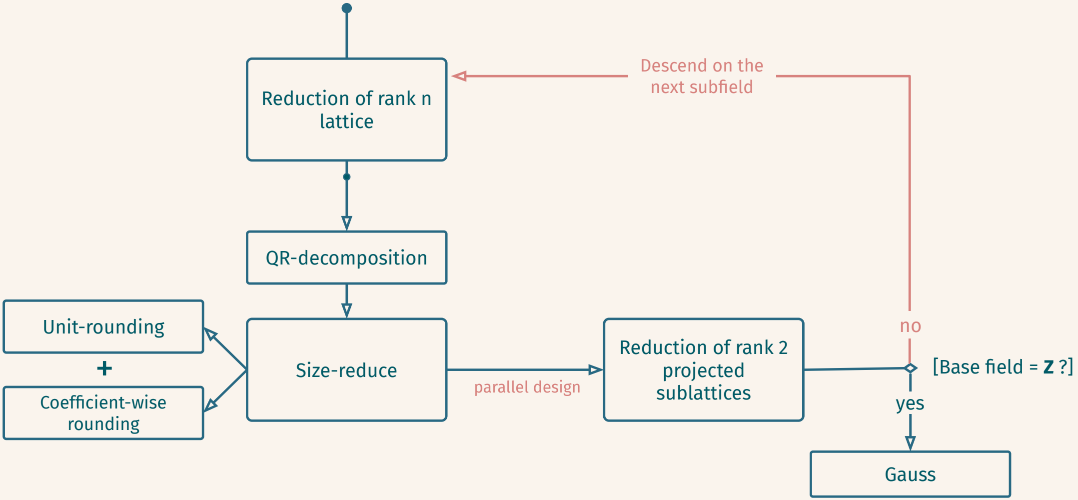
As a flowchart



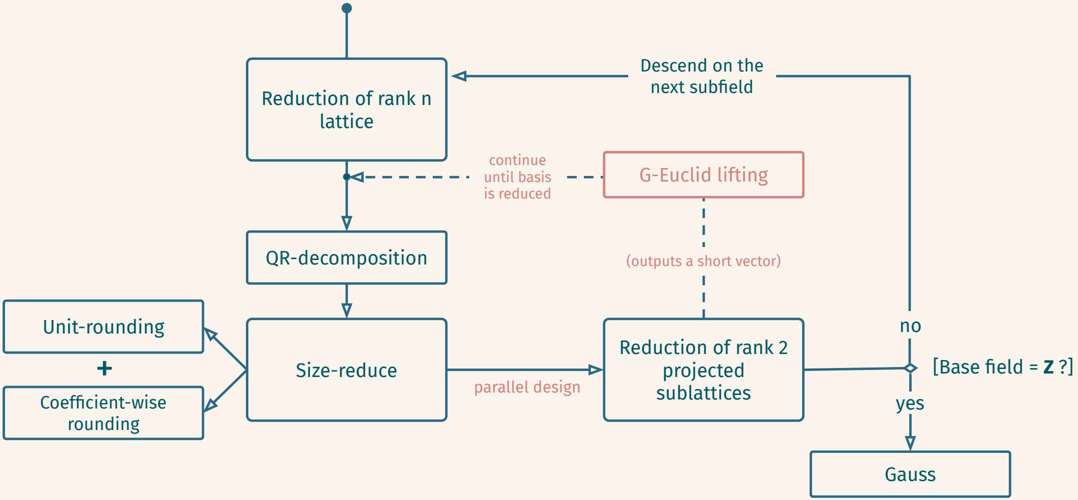
As a flowchart



As a flowchart



As a flowchart



General strategy

$$\begin{tikzcd} \mathcal{O}_{K_h} \\ \mathcal{O}_{K_{h-1}} \arrow[u, hook] \\ \vdots \arrow[u, hook] \\ \mathbb{Z} \arrow[u, hook] \end{tikzcd}$$

General strategy

$$\begin{tikzcd}
\mathcal{O}_{K_h} & m_1\mathcal{O}_{K_h} \oplus \cdots \oplus m_d\mathcal{O}_{K_h} \\
\mathcal{O}_{K_{h-1}} \arrow[u, hook] & \\
\vdots \arrow[u, hook] & \\
\mathbb{Z} \arrow[u, hook] &
\end{tikzcd}$$

General strategy

$$\begin{tikzcd}
\mathcal{O}_{K_h} & m_1\mathcal{O}_{K_h} \oplus \cdots \oplus m_d\mathcal{O}_{K_h} \arrow[r, dashed, "\text{reduce rk } 2"] & \alpha_1\mathcal{O}_{K_h} \oplus \alpha_2\mathcal{O}_{K_h} \\
\mathcal{O}_{K_{h-1}} \arrow[u, hook] \\
\vdots \arrow[u, hook] \\
Z \arrow[u, hook]
\end{tikzcd}$$

General strategy

$$\begin{tikzcd}
\mathcal{O}_{K_h} & m_1\mathcal{O}_{K_h} \oplus \cdots \oplus m_d\mathcal{O}_{K_h} \arrow[r, dashed, "\text{reduce rk 2}"] & \alpha_1\mathcal{O}_{K_h} \oplus \alpha_2\mathcal{O}_{K_h} \arrow[dl, dashed, bend right, "\text{descend}"'] \\
\mathcal{O}_{K_{h-1}} \arrow[u, hook] & m'_1\mathcal{O}_{K_{h-1}} \oplus \cdots \oplus m'_{2m_h}\mathcal{O}_{K_{h-1}} & \\
\vdots \arrow[u, hook] & & \\
\mathbb{Z} \arrow[u, hook] & &
\end{tikzcd}$$

General strategy

$$
\begin{tikzcd}
\mathcal{O}_{K_h} & m_1\mathcal{O}_{K_h} \oplus \cdots \oplus m_d\mathcal{O}_{K_h} \arrow[r, dash, dashed, "\text{reduce rk } 2"] & \alpha_1\mathcal{O}_{K_h} \oplus \alpha_2\mathcal{O}_{K_h} \arrow[dl, dashed, bend right, "\text{descend}"'] \\
\mathcal{O}_{K_{h-1}} \arrow[u, hook] & m'_1\mathcal{O}_{K_{h-1}} \oplus \cdots \oplus m'_{2m_h}\mathcal{O}_{K_{h-1}} \arrow[r, dash, dashed] & \alpha'_1\mathcal{O}_{K_{h-1}} \oplus \alpha'_2\mathcal{O}_{K_{h-1}} \\
\vdots \arrow[u, hook] & & \\
Z \arrow[u, hook] & &
\end{tikzcd}
$$

General strategy

$$
\begin{tikzcd}
\mathcal{O}_{K_h} & m_1\mathcal{O}_{K_h} \oplus \cdots \oplus m_d\mathcal{O}_{K_h} \arrow[r, dashed, "\text{reduce rk } 2"] & \alpha_1\mathcal{O}_{K_h} \oplus \alpha_2\mathcal{O}_{K_h} \arrow[dl, dashed, bend right, two heads, "\text{descend}"'] \\
\mathcal{O}_{K_{h-1}} \arrow[u, hook] & m'_1\mathcal{O}_{K_{h-1}} \oplus \cdots \oplus m'_{2m_h}\mathcal{O}_{K_{h-1}} \arrow[r, dashed, dash] & \alpha'_1\mathcal{O}_{K_{h-1}} \oplus \alpha'_2\mathcal{O}_{K_{h-1}} \arrow[dl, dotted, two heads] \\
\vdots \arrow[u, hook] & \vdots \arrow[r, dotted, dash] & \vdots \arrow[dl, dotted, bend right, "\text{descend}"'] \\
Z \arrow[u, hook] & M_Z = \beta_1 Z \oplus \cdots \oplus \beta_k Z &
\end{tikzcd}
$$

General strategy

$$
\begin{tikzcd}
\mathcal{O}_{K_h} & m_1\mathcal{O}_{K_h} \oplus \cdots \oplus m_d\mathcal{O}_{K_h} \arrow[r, dash, dashed, "\text{reduce rk 2}" description] & \alpha_1\mathcal{O}_{K_h} \oplus \alpha_2\mathcal{O}_{K_h} \arrow[dl, dashed, bend right, two heads, "\text{descend}" description] \\
\mathcal{O}_{K_{h-1}} \arrow[u, hook] & m'_1\mathcal{O}_{K_{h-1}} \oplus \cdots \oplus m'_{2m_h}\mathcal{O}_{K_{h-1}} \arrow[r, dash, dashed] & \alpha'_1\mathcal{O}_{K_{h-1}} \oplus \alpha'_2\mathcal{O}_{K_{h-1}} \arrow[dl, dotted, two heads] \\
\vdots \arrow[u, hook] & \vdots \arrow[r, dash, dotted] & \vdots \arrow[dl, dotted, bend right, two heads, "\text{descend}" description] \\
\mathbb{Z} \arrow[u, hook] & M_{\mathbb{Z}} = \beta_1\mathbb{Z} \oplus \cdots \oplus \beta_k\mathbb{Z} \arrow[r, dash, dashed, "\text{reduce rank 2}" description] & \alpha_1\mathbb{Z} \oplus \alpha_2\mathbb{Z}
\end{tikzcd}
$$

$$
\begin{tikzcd}
\mathcal{O}_{K_h} & m_1\mathcal{O}_{K_h} \oplus \cdots \oplus m_d\mathcal{O}_{K_h} \arrow[r, dashed, "\text{reduce rk 2}"] & \alpha_1\mathcal{O}_{K_h} \oplus \alpha_2\mathcal{O}_{K_h} \arrow[dl, dashed, bend right, "\text{descend}"'] \\
\mathcal{O}_{K_{h-1}} \arrow[u, hook] & m'_1\mathcal{O}_{K_{h-1}} \oplus \cdots \oplus m'_{2m_h}\mathcal{O}_{K_{h-1}} \arrow[r, dashed] & \alpha'_1\mathcal{O}_{K_{h-1}} \oplus \alpha'_2\mathcal{O}_{K_{h-1}} \arrow[dl, dotted] \\
\vdots \arrow[u, hook] & \vdots \arrow[r, dotted] & \vdots \arrow[dl, dotted, bend right, "\text{descend}"'] \\
\mathbb{Z} \arrow[u, hook] & M_{\mathbb{Z}} = \beta_1\mathbb{Z} \oplus \cdots \oplus \beta_k\mathbb{Z} \arrow[r, dashed, "\text{reduce rank 2}"] & \alpha_1\mathbb{Z} \oplus \alpha_2\mathbb{Z} \arrow[d, dashed, "\textsc{Schonhage}"] \\
 & & v \text{ (short)}
\end{tikzcd}
$$

$$
\begin{tikzcd}[column sep=large]
\mathcal{O}_{K_h} & m_1\mathcal{O}_{K_h} \oplus \cdots \oplus m_d\mathcal{O}_{K_h} \arrow[r, dashed, "\text{reduce rk 2}"] & \alpha_1\mathcal{O}_{K_h} \oplus \alpha_2\mathcal{O}_{K_h} \arrow[dl, dashed, bend right, "\text{descend}"'] & \\
\mathcal{O}_{K_{h-1}} \arrow[u, hook] & m'_1\mathcal{O}_{K_{h-1}} \oplus \cdots \oplus m'_{2m_h}\mathcal{O}_{K_{h-1}} \arrow[r, dashed, no head] & \alpha'_1\mathcal{O}_{K_{h-1}} \oplus \alpha'_2\mathcal{O}_{K_{h-1}} \arrow[dl, dotted] & \\
\vdots \arrow[u, hook] & \vdots \arrow[r, dotted, no head, "\text{descend}"] & \vdots \arrow[dl, dotted, bend right] & \\
\mathbb{Z} \arrow[u, hook] & M_{\mathbb{Z}} = \beta_1\mathbb{Z} \oplus \cdots \oplus \beta_k\mathbb{Z} \arrow[r, dashed, "\text{reduce rank 2}"] & \alpha_1\mathbb{Z} \oplus \alpha_2\mathbb{Z} \arrow[r, no head, "\cong"] \arrow[d, dashed, "\text{SCHONHAGE}"] & \upsilon\mathbb{Z} \oplus \omega\mathbb{Z} \ \text{(reduced)} \\
 & & \upsilon \ \text{(short)} \arrow[ur, dashed, bend right, "\text{complete}"'] &
\end{tikzcd}
$$

General strategy

$$
\begin{tikzcd}
\mathcal{O}_{K_h} & m_1\mathcal{O}_{K_h} \oplus \cdots \oplus m_d\mathcal{O}_{K_h} \arrow[r, dashed, "\text{reduce rk 2}"] & \alpha_1\mathcal{O}_{K_h} \oplus \alpha_2\mathcal{O}_{K_h} \arrow[dl, dashed, bend right, "\text{descend}"'] & & \\
\mathcal{O}_{K_{h-1}} \arrow[u, hook] & m'_1\mathcal{O}_{K_{h-1}} \oplus \cdots \oplus m'_{2m_h}\mathcal{O}_{K_{h-1}} \arrow[r, dashed, no head] & \alpha'_1\mathcal{O}_{K_{h-1}} \oplus \alpha'_2\mathcal{O}_{K_{h-1}} \arrow[dl, dotted] & & \\
\vdots \arrow[u, hook] & \vdots \arrow[r, dotted, no head, "\text{descend}"] \arrow[d, dotted] & \vdots \arrow[l, dotted, bend right] & \upsilon' \in M' \text{ (short)} & \\
\mathsf{Z} \arrow[u, hook] & M_{\mathsf{Z}} = \beta_1\mathsf{Z} \oplus \cdots \oplus \beta_k\mathsf{Z} \arrow[r, dashed, no head, "\text{reduce rank 2}"] \arrow[urr, dashed] & \alpha_1\mathsf{Z} \oplus \alpha_2\mathsf{Z} \arrow[rr, no head, "\cong" description] \arrow[d, dashed, "\textsc{Schonhage}"] & & \upsilon\mathsf{Z} \oplus \omega\mathsf{Z} \text{ (reduced)} \\
& & \upsilon \text{ (short)} \arrow[urr, dashed, bend right, "\text{complete}"'] & &
\end{tikzcd}
$$

General strategy

$$
\begin{tikzcd}
\mathcal{O}_{K_h} & m_1\mathcal{O}_{K_h} \oplus \cdots \oplus m_d\mathcal{O}_{K_h} \arrow[r, dashed, "\text{reduce rk } 2"] & \alpha_1\mathcal{O}_{K_h} \oplus \alpha_2\mathcal{O}_{K_h} \arrow[dl, dashed, bend right, "\text{descend}"'] & & \\
\mathcal{O}_{K_{h-1}} \arrow[u, hook] & m_1'\mathcal{O}_{K_{h-1}} \oplus \cdots \oplus m_{2m_h}'\mathcal{O}_{K_{h-1}} \arrow[r, dashed] & \alpha_1'\mathcal{O}_{K_{h-1}} \oplus \alpha_2'\mathcal{O}_{K_{h-1}} \arrow[rr, dash, "\cong"] \arrow[dl, dotted] & & \upsilon'\mathcal{O}_{K_{h-1}} \oplus \omega'\mathcal{O}_{K_{h-1}} \\
\vdots \arrow[u, hook] & \vdots \arrow[r, dotted, "\text{descend}"] & \vdots \arrow[dl, dotted, bend right] & \upsilon' \in M' \text{ (short)} \arrow[ur, dashed, bend right, "\text{Lift}"'] & \\
\mathsf{Z} \arrow[u, hook] & M_{\mathsf{Z}} = \beta_1\mathsf{Z} \oplus \cdots \oplus \beta_k\mathsf{Z} \arrow[r, dashed, "\text{reduce rank } 2"] \arrow[urr, dashed] & \alpha_1\mathsf{Z} \oplus \alpha_2\mathsf{Z} \arrow[rr, dash, "\cong"] \arrow[d, dashed, "\text{SCHONHAGE}"] & & \upsilon\mathsf{Z} \oplus \omega\mathsf{Z} \text{ (reduced)} \\
& & \upsilon \text{ (short)} \arrow[urr, dashed, bend right, "\text{complete}"'] & &
\end{tikzcd}
$$

General strategy

$$
\begin{tikzcd}
\mathcal{O}_{K_h} & m_1\mathcal{O}_{K_h} \oplus \cdots \oplus m_d\mathcal{O}_{K_h} \arrow[r, dashed, "\text{reduce rk 2}"] & \alpha_1\mathcal{O}_{K_h} \oplus \alpha_2\mathcal{O}_{K_h} \arrow[ddl, dashed, bend right, "\text{descend}"'] & & \\
 & & & \upsilon \in M \text{ (short)} & \\
\mathcal{O}_{K_{h-1}} \arrow[uu, hook] & m'_1\mathcal{O}_{K_{h-1}} \oplus \cdots \oplus m'_{2m_h}\mathcal{O}_{K_{h-1}} \arrow[urr] \arrow[r, dash, dashed] & \alpha'_1\mathcal{O}_{K_{h-1}} \oplus \alpha'_2\mathcal{O}_{K_{h-1}} \arrow[rr, dash, "\cong" description] \arrow[dl, dotted] & & \upsilon'\mathcal{O}_{K_{h-1}} \oplus \omega'\mathcal{O}_{K_{h-1}} \\
\vdots \arrow[u, hook] & \vdots \arrow[d, dotted] & \vdots \arrow[l, dotted, "\text{descend}"] & \upsilon' \in M' \text{ (short)} \arrow[ur, dashed, bend right, "\text{Lift}"'] & \\
\mathbb{Z} \arrow[u, hook] & M_{\mathbb{Z}} = \beta_1\mathbb{Z} \oplus \cdots \oplus \beta_k\mathbb{Z} \arrow[urr, dashed] \arrow[r, dash, dashed, "\text{reduce rank 2}"] & \alpha_1\mathbb{Z} \oplus \alpha_2\mathbb{Z} \arrow[rr, dash, "\cong" description] \arrow[d, dashed, "\text{SCHONHAGE}"] & & \upsilon\mathbb{Z} \oplus \omega\mathbb{Z} \text{ (reduced)} \\
 & & \upsilon \text{ (short)} \arrow[urr, dashed, bend right, "\text{complete}"'] & &
\end{tikzcd}
$$

General strategy

$$
\begin{tikzcd}
\mathcal{O}_{K_h} & m_1\mathcal{O}_{K_h} \oplus \cdots \oplus m_d\mathcal{O}_{K_h} \arrow[r, dashed, "\text{reduce rk 2}"] & \alpha_1\mathcal{O}_{K_h} \oplus \alpha_2\mathcal{O}_{K_h} \arrow[rr, no head, "\cong"] \arrow[ddl, dashed, bend right, "\text{descend}"'] & & \upsilon\mathcal{O}_{K_h} \oplus \omega\mathcal{O}_{K_h} \\
& & & \upsilon \in M \ (\text{short}) \arrow[ur, dashed, bend right, "\text{Lift}"'] & \\
\mathcal{O}_{K_{h-1}} \arrow[uu, hook] & m'_1\mathcal{O}_{K_{h-1}} \oplus \cdots \oplus m'_{2m_h}\mathcal{O}_{K_{h-1}} \arrow[r, dashed, no head] \arrow[urr] & \alpha'_1\mathcal{O}_{K_{h-1}} \oplus \alpha'_2\mathcal{O}_{K_{h-1}} \arrow[rr, no head, "\cong"] \arrow[dl, dotted] & & \upsilon'\mathcal{O}_{K_{h-1}} \oplus \omega'\mathcal{O}_{K_{h-1}} \\
\vdots \arrow[u, hook] & \vdots & \vdots \arrow[l, dotted, "\text{descend}"] \arrow[dl, dotted] & \upsilon' \in M' \ (\text{short}) \arrow[ur, dashed, bend right, "\text{Lift}"'] & \\
\mathbb{Z} \arrow[u, hook] & M_{\mathbb{Z}} = \beta_1\mathbb{Z} \oplus \cdots \oplus \beta_k\mathbb{Z} \arrow[r, dashed, "\text{reduce rank 2}"] \arrow[urr, dashed] & \alpha_1\mathbb{Z} \oplus \alpha_2\mathbb{Z} \arrow[rr, no head, "\cong"] \arrow[d, dashed, "\text{SCHONHAGE}"] & & \upsilon\mathbb{Z} \oplus \omega\mathbb{Z} \ (\text{reduced}) \\
& & \upsilon \ (\text{short}) \arrow[urr, dashed, bend right, "\text{complete}"'] & &
\end{tikzcd}
$$

Lifting up!

- Recursive call over K_{h-1} allows to deduce short $x \in K_h$ (small combinations of the basis vectors)

Lifting up!

- Recursive call over K_{h-1} allows to deduce short $x \in K_h$ (small combinations of the basis vectors)
- To replace by x in the current basis over K_h, complete into a basis
  $\rightarrow$ complete a (primitive) vector of $\mathcal{O}_{K_h}^2$ into a unimodular matrix

Find $\square$, $\triangle$ s.t. $\left| \begin{pmatrix} a & \square \\ b & \triangle \end{pmatrix} \right| = 1$, i.e

$$a\triangle - b\square = 1$$

Solve a *Bezout* equation

Lifting up!

- Recursive call over K_{h-1} allows to deduce short $x \in K_h$ (small combinations of the basis vectors)
- To replace by x in the current basis over K_h, complete into a basis
  $\rightarrow$ complete a (primitive) vector of $\mathcal{O}_{K_h}^2$ into a unimodular matrix

Find $\square$, $\triangle$ s.t. $\left|\begin{pmatrix} a & \square \\ b & \triangle \end{pmatrix}\right| = 1$, i.e

$$a\triangle - b\square = 1$$

Solve a *Bezout* equation

Recursive Euclide solver(a,b)

Lifting up!

- Recursive call over K_{h-1} allows to deduce short $x \in K_h$ (small combinations of the basis vectors)
- To replace by x in the current basis over K_h, complete into a basis
  $\to$ complete a (primitive) vector of $\mathcal{O}_{K_h}^2$ into a unimodular matrix

Find $\square$, $\triangle$ s.t. $\left|\begin{pmatrix} a & \square \\ b & \triangle \end{pmatrix}\right| = 1$, i.e

$$a\triangle - b\square = 1$$

Solve a *Bezout* equation

Recursive Euclide solver(a,b)

1. **If $K_h = \mathbb{Q}$:** this is extended-GCD !

Lifting up!

- Recursive call over K_{h-1} allows to deduce short $x \in K_h$ (small combinations of the basis vectors)
- To replace by x in the current basis over K_h, complete into a basis
  $\rightarrow$ complete a (primitive) vector of $\mathcal{O}_{K_h}^2$ into a unimodular matrix

Find $\square$, $\triangle$ s.t. $\left|\begin{pmatrix} a & \square \\ b & \triangle \end{pmatrix}\right| = 1$, i.e

$$a\triangle - b\square = 1$$

Solve a *Bezout* equation

Recursive Euclide solver(a,b)

1. **If $K_h = \mathbb{Q}$:** this is extended-GCD !
2. **If the tower $K_h^{\uparrow}$ is not trivial:** Descend problem to the subfield K_{h-1} with $N_{K_h/K_{h-1}}$ and recurse:

$$\mu N_{K_h/K_{h-1}}(a) - \nu N_{K_h/K_{h-1}}(b) = 1.$$

$$a \cdot \underbrace{\mu\, a^{-1} N_{K_h/K_{h-1}}(a)}_{:=\triangle \in \mathcal{O}_{K_h}} - b \cdot \underbrace{\nu\, b^{-1} N_{K_h/K_{h-1}}(b)}_{:=\square \in \mathcal{O}_{K_h}} = 1$$

Lifting up!

- Recursive call over K_{h-1} allows to deduce short $x \in K_h$ (small combinations of the basis vectors)
- To replace by x in the current basis over K_h, complete into a basis
  $\rightarrow$ complete a (primitive) vector of $\mathcal{O}_{K_h}^2$ into a unimodular matrix

Find $\square$, $\triangle$ s.t. $\left|\begin{pmatrix} a & \square \\ b & \triangle \end{pmatrix}\right| = 1$, i.e

$$a\triangle - b\square = 1$$

Solve a *Bezout* equation

Recursive Euclide solver(a,b)

1. **If $K_h = \mathbb{Q}$:** this is extended-GCD !
2. **If the tower $K_h^{\uparrow}$ is not trivial:** Descend problem to the subfield K_{h-1} with $N_{K_h/K_{h-1}}$ and recurse:

$$\mu N_{K_h/K_{h-1}}(a) - \nu N_{K_h/K_{h-1}}(b) = 1.$$

$$a \cdot \underbrace{\mu\, a^{-1} N_{K_h/K_{h-1}}(a)}_{:=\triangle \in \mathcal{O}_{K_h}} - b \cdot \underbrace{\nu\, b^{-1} N_{K_h/K_{h-1}}(b)}_{:=\square \in \mathcal{O}_{K_h}} = 1$$

3. **Reduction of the size of solutions:** To avoid blow-up in the size of the coefficients lifted, need to control size of the solution at each step...

Lifting up!

- Recursive call over K_{h-1} allows to deduce short $x \in K_h$ (small combinations of the basis vectors)
- To replace by x in the current basis over K_h, complete into a basis
  $\rightarrow$ complete a (primitive) vector of $\mathcal{O}_{K_h}^2$ into a unimodular matrix

Find $\square$, $\triangle$ s.t. $\left| \begin{pmatrix} a & \square \\ b & \triangle \end{pmatrix} \right| = 1$, i.e

$$a\triangle - b\square = 1$$

Solve a *Bezout* equation

Recursive Euclide solver(a,b)

1. **If $K_h = \mathbb{Q}$:** this is extended-GCD !
2. **If the tower $K_h^{\uparrow}$ is not trivial:** Descend problem to the subfield K_{h-1} with $N_{K_h/K_{h-1}}$ and recurse:

$$\mu N_{K_h/K_{h-1}}(a) - \nu N_{K_h/K_{h-1}}(b) = 1.$$

$$a \cdot \underbrace{\mu\, a^{-1} N_{K_h/K_{h-1}}(a)}_{:=\triangle \in \mathcal{O}_{K_h}} - b \cdot \underbrace{\nu\, b^{-1} N_{K_h/K_{h-1}}(b)}_{:=\square \in \mathcal{O}_{K_h}} = 1$$

3. **Reduction of the size of solutions:** To avoid blow-up in the size of the coefficients lifted, need to control size of the solution at each step...

Use **Size-reduce** !

Generalized Euclidean algorithm

G-Euclide, Lift

Function ***G-Euclide***:

- **if** $K_h = \mathbb{Q}$ **then return** **ExGcd**(a, b);
- $\mu, \nu \leftarrow$ **G-Euclide**$\left(K_{h-1}^{\uparrow}, N_{K_h/K_{h-1}}(a), N_{K_h/K_{h-1}}(b)\right)$;
- $\mu', \nu' \leftarrow \mu\, a^{-1} N_{K_h/K_{h-1}}(a), \nu\, b^{-1} N_{K_h/K_{h-1}}(b)$;
- $W \leftarrow \begin{pmatrix} a & \nu' \\ b & \mu' \end{pmatrix}$;
- $V \leftarrow$ **Size-Reduce**(**Orthogonalize**(W)); **return** $W \cdot V[2]$

Function ***Lift***:

- $a, b \leftarrow$ **Ascend**$(K_h, U[1])$; $\mu, \nu \leftarrow$ **G-Euclide**$\left(K_{h-1}^{\uparrow}, a, b\right)$;
- $U \leftarrow \begin{pmatrix} a & \nu \\ b & \mu \end{pmatrix}$;
- **return** U

On the complexity of the reduction

Complexity [E-Kirchner-Fouque 2019]

Let f be a log-smooth integer. The complexity of the algorithm **Reduce** on rank two modules over $K = \mathbb{Q}[x]/\Phi_f(x)$, represented as a matrix M whose number of bits in the input coefficients is uniformly bounded by $B > n$, is *heuristically* a $\tilde{\mathrm{O}}\left(n^2 B\right)$ with $n = \varphi(f)$. The first column of the reduced matrix has its coefficients uniformly bounded by $2^{\tilde{\mathrm{O}}(n)} \operatorname{covol}(M)^{\frac{1}{2n}}$.

On the complexity of the reduction

Complexity [E-Kirchner-Fouque 2019]

Let f be a log-smooth integer. The complexity of the algorithm **Reduce** on rank two modules over $K = \mathbb{Q}[x]/\Phi_f(x)$, represented as a matrix M whose number of bits in the input coefficients is uniformly bounded by $B > n$, is *heuristically* a $\tilde{O}(n^2 B)$ with $n = \varphi(f)$. The first column of the reduced matrix has its coefficients uniformly bounded by $2^{\tilde{O}(n)} \operatorname{covol}(M)^{\frac{1}{2n}}$.

Sketch of proof.

- Estimate a relation between approximation factor and number of rounds: $\rho = O\left(d^2 \log p\right)$.

On the complexity of the reduction

Complexity [E-Kirchner-Fouque 2019]

Let f be a log-smooth integer. The complexity of the algorithm **Reduce** on rank two modules over $K = \mathbb{Q}[x]/\Phi_f(x)$, represented as a matrix M whose number of bits in the input coefficients is uniformly bounded by $B > n$, is *heuristically* a $\tilde{\mathrm{O}}\left(n^2 B\right)$ with $n = \varphi(f)$. The first column of the reduced matrix has its coefficients uniformly bounded by $2^{\tilde{\mathrm{O}}(n)} \operatorname{covol}(M)^{\frac{1}{2n}}$.

Sketch of proof.

- Estimate a relation between approximation factor and number of rounds: $\rho = \mathrm{O}\left(d^2 \log p\right)$.
- Limiting factor for the precision: represent the shortest Archimedean embedding of the norm of the Gram-Schmidt orthogonalization of the initial basis.

On the complexity of the reduction

Complexity [E-Kirchner-Fouque 2019]

Let f be a log-smooth integer. The complexity of the algorithm **Reduce** on rank two modules over $K = \mathbb{Q}[x]/\Phi_f(x)$, represented as a matrix M whose number of bits in the input coefficients is uniformly bounded by $B > n$, is *heuristically* a $\tilde{\mathrm{O}}\left(n^2 B\right)$ with $n = \varphi(f)$. The first column of the reduced matrix has its coefficients uniformly bounded by $2^{\tilde{\mathrm{O}}(n)} \mathrm{covol}(M)^{\frac{1}{2n}}$.

Sketch of proof.

- Estimate a relation between approximation factor and number of rounds: $\rho = \mathrm{O}\left(d^2 \log p\right)$.
- Limiting factor for the precision: represent the shortest Archimedean embedding of the norm of the Gram-Schmidt orthogonalization of the initial basis.
- Devise a bound by looking at the sum of all the bitsizes used in the recursive calls (use the potential to show that dividing the degrees by $\frac{d}{2}$ leads to a multiplication by a factor at most in $\mathrm{O}\left(d^2\right)$)

On the complexity of the reduction

Complexity [E-Kirchner-Fouque 2019]

Let f be a log-smooth integer. The complexity of the algorithm **Reduce** on rank two modules over $K = \mathbb{Q}[x]/\Phi_f(x)$, represented as a matrix M whose number of bits in the input coefficients is uniformly bounded by $B > n$, is *heuristically* a $\tilde{\mathrm{O}}\left(n^2 B\right)$ with $n = \varphi(f)$. The first column of the reduced matrix has its coefficients uniformly bounded by $2^{\tilde{\mathrm{O}}(n)}\,\mathrm{covol}(M)^{\frac{1}{2n}}$.

Sketch of proof.

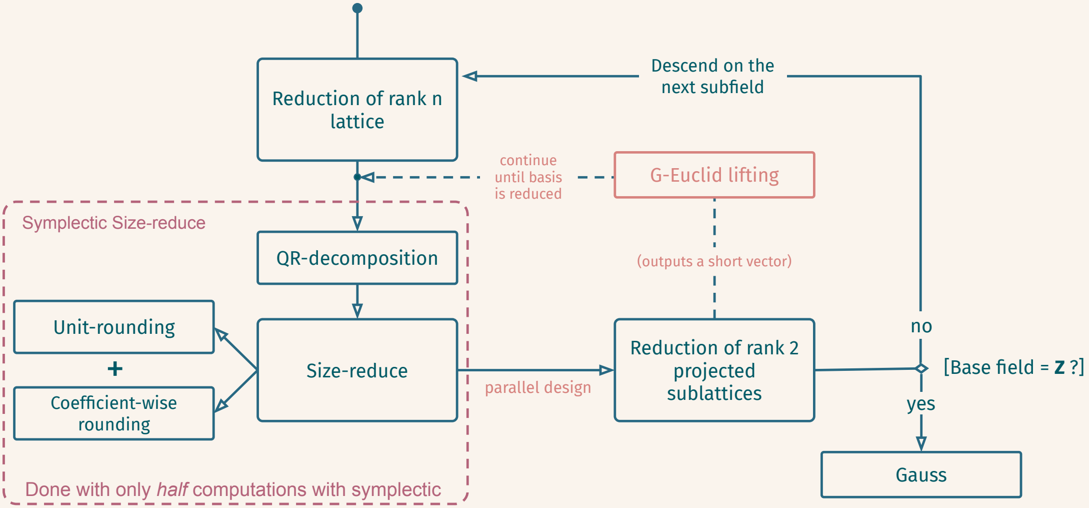
- Estimate a relation between approximation factor and number of rounds: $\rho = \mathrm{O}\left(d^2 \log p\right)$.
- Limiting factor for the precision: represent the shortest Archimedean embedding of the norm of the Gram-Schmidt orthogonalization of the initial basis.
- Devise a bound by looking at the sum of all the bitsizes used in the recursive calls (use the potential to show that dividing the degrees by $\frac{d}{2}$ leads to a multiplication by a factor at most in $\mathrm{O}\left(d^2\right)$)
- Sum at each level to conclude on the complexity.

What if i want an actual SVP?

A reduction a la Lovasz

There exists a reduction to γ-HSVP over $\mathcal{O}_L$ from γ^2-SVP over $\mathcal{O}_L$ using at most $2\,\mathrm{rk}$ calls to the Hermite-SVP oracle.

Wait there is more !



Faster with symplectic symmetries

A nano-primer on symplectic geometry

A nano-primer on symplectic geometry

Euclidean space

Symplectic space

A nano-primer on symplectic geometry

Euclidean space

- Symmetric bilinear Form $\langle \cdot, \cdot \rangle$

Symplectic space

- Antisymmetric bilinear Form ω

A nano-primer on symplectic geometry

Euclidean space

- Symmetric bilinear Form $\langle \cdot, \cdot \rangle$
- Transformation group: $O_n(\mathbb{R})$

Symplectic space

- Antisymmetric bilinear Form ω
- Transformation group: $\mathrm{Sp}_\omega(\mathbb{R})$

A nano-primer on symplectic geometry

Euclidean space

- Symmetric bilinear Form $\langle\cdot,\cdot\rangle$
- Transformation group: $O_n(\mathbb{R})$
- *Nice* bases: Orthonormal bases

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

Symplectic space

- Antisymmetric bilinear Form ω
- Transformation group: $\mathrm{Sp}_\omega(\mathbb{R})$
- *Nice* bases: Darboux bases

$$\begin{bmatrix} 0 & I_d \\ -I_d & 0 \end{bmatrix}$$

A nano-primer on symplectic geometry

Euclidean space

- Symmetric bilinear Form $\langle \cdot, \cdot \rangle$
- Transformation group: $O_n(\mathbb{R})$
- *Nice* bases: Orthonormal bases

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

Symplectic space

- Antisymmetric bilinear Form ω
- Transformation group: $\mathrm{Sp}_\omega(\mathbb{R})$
- *Nice* bases: Darboux bases

$$\begin{bmatrix} 0 & I_d \\ -I_d & 0 \end{bmatrix}$$

A nano-primer on symplectic geometry

Euclidean space

- Symmetric bilinear Form $\langle \cdot, \cdot \rangle$
- Transformation group: $O_n(\mathbb{R})$
- *Nice* bases: Orthonormal bases

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

Symplectic space

- Antisymmetric bilinear Form ω
- Transformation group: $\mathrm{Sp}_\omega(\mathbb{R})$
- *Nice* bases: Darboux bases

$$\begin{bmatrix} 0 & I_d \\ -I_d & 0 \end{bmatrix}$$

A nano-primer on symplectic geometry

Euclidean space

- Symmetric bilinear Form $\langle \cdot, \cdot \rangle$
- Transformation group: $O_n(\mathbb{R})$
- *Nice* bases: Orthonormal bases

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

Symplectic space

- Antisymmetric bilinear Form ω
- Transformation group: $\mathrm{Sp}_\omega(\mathbb{R})$
- *Nice* bases: Darboux bases

$$\begin{bmatrix} 0 & I_d \\ -I_d & 0 \end{bmatrix}$$

A nano-primer on symplectic geometry

Euclidean space

- Symmetric bilinear Form $\langle \cdot, \cdot \rangle$
- Transformation group: $O_n(\mathbb{R})$
- *Nice* bases: Orthonormal bases

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

Symplectic space

- Antisymmetric bilinear Form ω
- Transformation group: $\mathrm{Sp}_\omega(\mathbb{R})$
- *Nice* bases: Darboux bases

$$\begin{bmatrix} 0 & I_d \\ -I_d & 0 \end{bmatrix}$$

A nano-primer on symplectic geometry

Euclidean space

- Symmetric bilinear Form $\langle \cdot, \cdot \rangle$
- Transformation group: $O_n(\mathbb{R})$
- *Nice* bases: Orthonormal bases

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

Symplectic space

- Antisymmetric bilinear Form ω
- Transformation group: $\mathrm{Sp}_\omega(\mathbb{R})$
- *Nice* bases: Darboux bases

$$\begin{bmatrix} 0 & I_d \\ -I_d & 0 \end{bmatrix}$$

A nano-primer on symplectic geometry

Euclidean space

- Symmetric bilinear Form $\langle \cdot, \cdot \rangle$
- Transformation group: $O_n(\mathbb{R})$
- *Nice* bases: Orthonormal bases

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

Symplectic space

- Antisymmetric bilinear Form ω
- Transformation group: $\mathrm{Sp}_\omega(\mathbb{R})$
- *Nice* bases: Darboux bases

$$\begin{bmatrix} 0 & I_d \\ -I_d & 0 \end{bmatrix}$$

A nano-primer on symplectic geometry

Euclidean space

- Symmetric bilinear Form $\langle \cdot, \cdot \rangle$
- Transformation group: $O_n(\mathbb{R})$
- *Nice* bases: Orthonormal bases

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

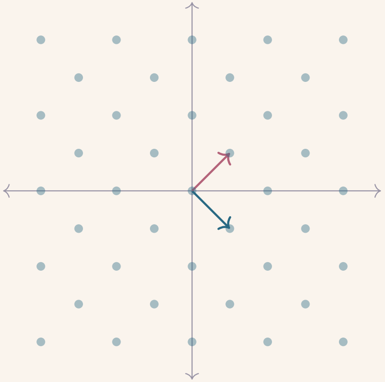
Symplectic space

- Antisymmetric bilinear Form ω
- Transformation group: $\mathrm{Sp}_\omega(\mathbb{R})$
- *Nice* bases: Darboux bases

$$\begin{bmatrix} 0 & I_d \\ -I_d & 0 \end{bmatrix}$$

More on Darboux base

sorry, symplectic spaces are of even dimension, so the first non-trivial case is of dim 4... no cute drawing today!



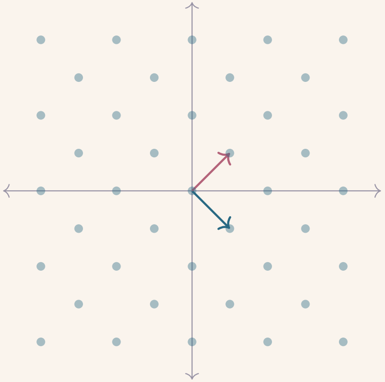
Standard symplectic form

$\omega(u, u) = \det((u, u))$

- Darboux "elements" (u, v) goes by pair of Gram matrix $j = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Note $j^2 = -\operatorname{Id}$.
- (u, v) acts as the complex $u + iv$
- The Darboux matrix statisfies $J^2 = -\operatorname{Id}_{2n}$
  $\rightarrow$ a symplectic space has a complex structure

More on Darboux base

sorry, symplectic spaces are of even dimension, so the first non-trivial case is of dim 4... no cute drawing today!



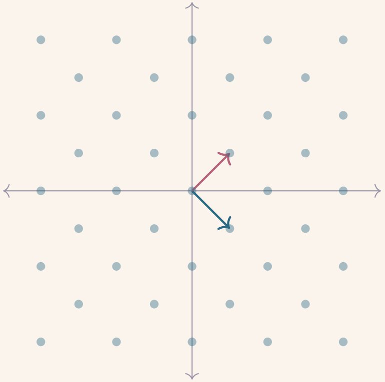
Standard symplectic form
$\omega(u, u) = \det((u, u))$

- Darboux "elements" (u, v) goes by pair of Gram matrix $j = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Note $j^2 = -\mathrm{Id}$.
- (u, v) acts as the complex $u + iv$
- The Darboux matrix statisfies $J^2 = -\mathrm{Id}_{2n}$
  $\rightarrow$ a symplectic space has a complex structure

To construct your Darboux basis at home:

More on Darboux base

sorry, symplectic spaces are of even dimension, so the first non-trivial case is of dim 4... no cute drawing today!



Standard symplectic form
$\omega(u, u) = \det((u, u))$

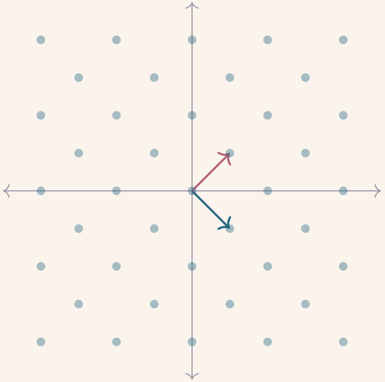
- Darboux "elements" (u, v) goes by pair of Gram matrix $j = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Note $j^2 = -\mathrm{Id}$.
- (u, v) acts as the complex $u + iv$
- The Darboux matrix statisfies $J^2 = -\mathrm{Id}_{2n}$
  $\rightarrow$ a symplectic space has a complex structure

To construct your Darboux basis at home:

1. Take a basis $(x_1, \ldots, x_n)$, wlog $\omega(x_1, x_2) \neq 0$

More on Darboux base

sorry, symplectic spaces are of even dimension, so the first non-trivial case is of dim 4... no cute drawing today!



Standard symplectic form
$\omega(u, u) = \det((u, u))$

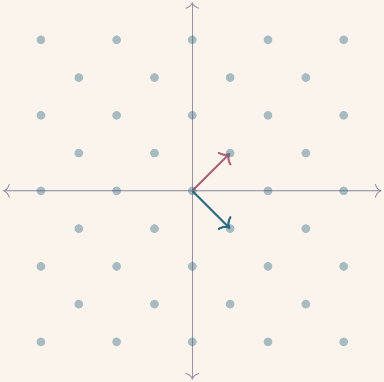
- Darboux "elements" (u, v) goes by pair of Gram matrix $j = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Note $j^2 = -\operatorname{Id}$.
- (u, v) acts as the complex $u + iv$
- The Darboux matrix statisfies $J^2 = -\operatorname{Id}_{2n}$
  $\rightarrow$ a symplectic space has a complex structure

To construct your Darboux basis at home:

1. Take a basis $(x_1, \ldots, x_n)$, wlog $\omega(x_1, x_2) \neq 0$
2. Scale to get $\omega(x_1, x_2) = +1$

More on Darboux base

sorry, symplectic spaces are of even dimension, so the first non-trivial case is of dim 4... no cute drawing today!



Standard symplectic form

$\omega(u, u) = \det((u, u))$

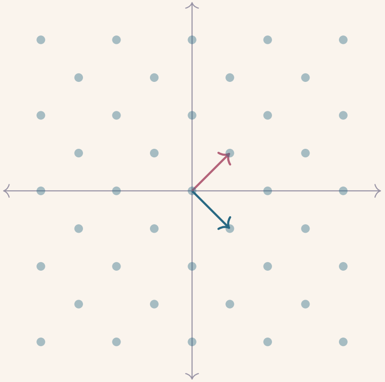
- Darboux "elements" (u, v) goes by pair of Gram matrix $j = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Note $j^2 = -\mathrm{Id}$.
- (u, v) acts as the complex $u + iv$
- The Darboux matrix statisfies $J^2 = -\mathrm{Id}_{2n}$
  $\rightarrow$ a symplectic space has a complex structure

To construct your Darboux basis at home:

1. Take a basis $(x_1, \ldots, x_n)$, wlog $\omega(x_1, x_2) \neq 0$
2. Scale to get $\omega(x_1, x_2) = +1$
3. $x_i \leftarrow x_i - \omega(x_i, x_1)x_2 - \omega(x_i, x_2)x_1$

More on Darboux base

sorry, symplectic spaces are of even dimension, so the first non-trivial case is of dim 4... no cute drawing today!



Standard symplectic form
$\omega(u, u) = \det((u, u))$

- Darboux "elements" (u, v) goes by pair of Gram matrix $j = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Note $j^2 = -\mathrm{Id}$.
- (u, v) acts as the complex $u + iv$
- The Darboux matrix statisfies $J^2 = -\mathrm{Id}_{2n}$
  $\rightarrow$ a symplectic space has a complex structure

To construct your Darboux basis at home:

1. Take a basis $(x_1, \ldots, x_n)$, wlog $\omega(x_1, x_2) \neq 0$
2. Scale to get $\omega(x_1, x_2) = +1$
3. $x_i \leftarrow x_i - \omega(x_i, x_1)x_2 - \omega(x_i, x_2)x_1$
4. Take a x_i such that $\omega_(x_3, x_4) \neq 0$, scale, etc.

Elementary transformations compatible with J'-symplectism

Symplectic structure is compatible
with the QR-decomposition
(for corresponding inner product).

Elementary transformations compatible with J'-symplectism

Symplectic structure is compatible
with the QR-decomposition
(for corresponding inner product).

Shape of block triangular symplectic matrices

$$\begin{pmatrix} A & AU \\ 0 & A^{-s} \end{pmatrix}$$

where $U = U^s$ ($\cdot^s$ is the symmetry w.r.t. the antidiagonal)

Elementary transformations compatible with J'-symplectism

Symplectic structure is compatible with the QR-decomposition
(for corresponding inner product).

Shape of block triangular symplectic matrices

$$\begin{pmatrix} A & AU \\ 0 & A^{-s} \end{pmatrix}$$

where $U = U^s$ ($\cdot^s$ is the symmetry w.r.t. the antidiagonal)

Elementary J-symplectic matrices

- For any $A \in \mathrm{GL}_d(L)$,

$$\begin{pmatrix} A & 0 \\ 0 & A^{-s} \end{pmatrix}$$

- For any $A \in \mathrm{GL}_2(L)$ with $\det A = 1$

$$\begin{pmatrix} \mathrm{Id}_\ell & 0 & 0 \\ 0 & A & 0 \\ 0 & 0 & \mathrm{Id}_r \end{pmatrix}$$

Elementary transformations compatible with J'-symplectism

Symplectic structure is compatible
with the QR-decomposition
(for corresponding inner product).

Shape of block triangular symplectic matrices

$$\begin{pmatrix} A & AU \\ 0 & A^{-s} \end{pmatrix}$$

where $U = U^s$ ($\cdot^s$ is the symmetry w.r.t. the antidiagonal)

Elementary J-symplectic matrices

- For any $A \in \mathrm{GL}_d(L)$,

$$\begin{pmatrix} A & 0 \\ 0 & A^{-s} \end{pmatrix}$$

- For any $A \in \mathrm{GL}_2(L)$ with $\det A = 1$

$$\begin{pmatrix} \mathrm{Id}_\ell & 0 & 0 \\ 0 & A & 0 \\ 0 & 0 & \mathrm{Id}_r \end{pmatrix}$$

Local reductions occurring during the reduction, swaps and transvections can preserve the J-symplectism.

Symplectic size-reduction

Symplectic-Size-Reduce

1 Set A, U such that $\begin{pmatrix} A & AU \\ 0 & A^{-s} \end{pmatrix} = R$;

2 $V \leftarrow$ **Size-Reduce**(A);

3 **return** $\begin{pmatrix} V & -V\lfloor U \rceil \\ 0 & V^{-s} \end{pmatrix}$

- R is upper-triangular, only depends on the first half of Q,
- We compute only the part above the antidiagonal of AU. Enough to compute the part above the antidiagonal of $A^{-1}(AU)$, which is persymmetric.

Symplectic bases $\Rightarrow$ Gram-Schmidt (Gram-Darboux) vectors are paired.

Size-reduction is cut in half ! (size-red half, apply blindly)

Speeding up lattice reduction with symplectic symmetries

Symplectic bases $\Rightarrow$ Gram-Schmidt (Gram-Darboux) vectors are paired.

Size-reduction is cut in half ! (size-red half, apply blindly)

LLL can be made 2 times faster !

(thank you for attention, bye!)

Going further with symplectic symmetries in a recursive tower

Going further with symplectic symmetries in a recursive tower

$J_h \in \bigwedge^2(K_h^2)$ is the determinant form:

$$J_h\left(\begin{pmatrix} x_0 \\ x_1 \end{pmatrix}, \begin{pmatrix} y_0 \\ y_1 \end{pmatrix}\right) = x_0 y_1 - x_1 y_0$$

Going further with symplectic symmetries in a recursive tower

$J_h \in \bigwedge^2(K_h^2)$ is the determinant form:

$$J_h\left(\begin{pmatrix} x_0 \\ x_1 \end{pmatrix}, \begin{pmatrix} y_0 \\ y_1 \end{pmatrix}\right) = x_0 y_1 - x_1 y_0$$

M is J_h-symplectic iff $\det M = 1$.

Going further with symplectic symmetries in a recursive tower

$J_h \in \bigwedge^2(K_h^2)$ is the determinant form:

$$J_h\left(\begin{pmatrix} x_0 \\ x_1 \end{pmatrix}, \begin{pmatrix} y_0 \\ y_1 \end{pmatrix}\right) = x_0 y_1 - x_1 y_0$$

$\rightarrow$ Descend the form J_h in J'_h to K_{h-1} by composition with a non-trivial linear form $\tau : K_h \rightarrow K_{h-1}$

Going further with symplectic symmetries in a recursive tower

$J_h \in \bigwedge^2(K_h^2)$ is the determinant form:

$$J_h\left(\begin{pmatrix} x_0 \\ x_1 \end{pmatrix}, \begin{pmatrix} y_0 \\ y_1 \end{pmatrix}\right) = x_0 y_1 - x_1 y_0$$

$\rightarrow$ Descend the form J_h in J_h' to K_{h-1} by composition with a non-trivial linear form $\tau : K_h \rightarrow K_{h-1}$

Idea: Adapt the work of Sawyer *[Computing the Iwasawa decomposition of the classical Lie groups of non compact type using the QR decomposition]*

Going further with symplectic symmetries in a recursive tower

$J_h \in \bigwedge^2(K_h^2)$ is the determinant form:

$$J_h\left(\begin{pmatrix} x_0 \\ x_1 \end{pmatrix}, \begin{pmatrix} y_0 \\ y_1 \end{pmatrix}\right) = x_0 y_1 - x_1 y_0$$

$\rightarrow$ Descend the form J_h in J'_h to K_{h-1} by composition with a non-trivial linear form $\tau : K_h \rightarrow K_{h-1}$

Idea: Adapt the work of Sawyer *[Computing the Iwasawa decomposition of the classical Lie groups of non compact type using the QR decomposition]*

Suppose: $K_h \cong {}^{K_{h-1}[T]}\!/\!_{T^{d_h} + a}$

Going further with symplectic symmetries in a recursive tower

$J_h \in \bigwedge^2(K_h^2)$ is the determinant form:

$$J_h\left(\begin{pmatrix} x_0 \\ x_1 \end{pmatrix}, \begin{pmatrix} y_0 \\ y_1 \end{pmatrix}\right) = x_0 y_1 - x_1 y_0$$

$\rightarrow$ Descend the form J_h in J'_h to K_{h-1} by composition with a non-trivial linear form $\tau : K_h \rightarrow K_{h-1}$

Idea: Adapt the work of Sawyer *[Computing the Iwasawa decomposition of the classical Lie groups of non compact type using the QR decomposition]*

$$\text{Suppose: } K_h \cong {}^{K_{h-1}[T]}\!\big/_{T^{d_h} + a}$$

Define:

$$\tau : \left| \begin{array}{ccc} K_h & \longrightarrow & K_{h-1} \\ y & \longmapsto & \mathrm{tr}_{K_h/K_{h-1}}\left(\frac{Ty}{d_h a}\right) \end{array} \right. ,$$

J'_h is now:

$$J'_h = \begin{pmatrix} 0 & R_{d_h} \\ -R_{d_h} & 0 \end{pmatrix}$$

in the power basis.

Going further with symplectic symmetries in a recursive tower

$J_h \in \bigwedge^2(K_h^2)$ is the determinant form:

$$J_h\left(\begin{pmatrix} x_0 \\ x_1 \end{pmatrix}, \begin{pmatrix} y_0 \\ y_1 \end{pmatrix}\right) = x_0 y_1 - x_1 y_0$$

$\rightarrow$ Descend the form J_h in J'_h to K_{h-1} by composition with a non-trivial linear form $\tau : K_h \rightarrow K_{h-1}$

Idea: Adapt the work of Sawyer *[Computing the Iwasawa decomposition of the classical Lie groups of non compact type using the QR decomposition]*

$$\text{Suppose: } K_h \cong {K_{h-1}[T]}/{T^{d_h} + a}$$

Define:

$$\tau : \left| \begin{array}{ccc} K_h & \longrightarrow & K_{h-1} \\ y & \longmapsto & \mathrm{tr}_{K_h/K_{h-1}}\left(\frac{Ty}{d_h a}\right) \end{array} \right. ,$$

J'_h is now:

$$J'_h = \begin{pmatrix} 0 & R_{d_h} \\ -R_{d_h} & 0 \end{pmatrix}$$

in the power basis.

Going further with symplectic symmetries in a recursive tower

$J_h \in \bigwedge^2(K_h^2)$ is the determinant form:

$$J_h\left(\begin{pmatrix} x_0 \\ x_1 \end{pmatrix}, \begin{pmatrix} y_0 \\ y_1 \end{pmatrix}\right) = x_0 y_1 - x_1 y_0$$

$\rightarrow$ Descend the form J_h in J'_h to K_{h-1} by composition with a non-trivial linear form $\tau : K_h \rightarrow K_{h-1}$

$\rightarrow$ Extend the definition of symplectism to $K_{h-1}^{2d_h}$

Symplectic group after descent

A $2d_h \times 2d_h$ matrix M' is symplectic if it preserves the J'_h form, that is if $J'_h \circ M' = J'_h$.

Idea: Adapt the work of Sawyer *[Computing the Iwasawa decomposition of the classical Lie groups of non compact type using the QR decomposition]*

$$\text{Suppose: } K_h \cong K_{h-1}[T] / T^{d_h} + a$$

Define:

$$\tau : \left| \begin{array}{ccc} K_h & \longrightarrow & K_{h-1} \\ y & \longmapsto & \mathrm{tr}_{K_h/K_{h-1}}\left(\frac{Ty}{d_h a}\right) \end{array} \right. ,$$

J'_h is now:

$$J'_h = \begin{pmatrix} 0 & R_{d_h} \\ -R_{d_h} & 0 \end{pmatrix}$$

in the power basis.

Going further with symplectic symmetries in a recursive tower

$J_h \in \bigwedge^2(K_h^2)$ is the determinant form:

$$J_h\left(\begin{pmatrix} x_0 \\ x_1 \end{pmatrix}, \begin{pmatrix} y_0 \\ y_1 \end{pmatrix}\right) = x_0 y_1 - x_1 y_0$$

$\rightarrow$ Descend the form J_h in J'_h to K_{h-1} by composition with a non-trivial linear form $\tau : K_h \rightarrow K_{h-1}$

$\rightarrow$ Extend the definition of symplectism to $K_{h-1}^{2d_h}$

Symplectic group after descent

A $2d_h \times 2d_h$ matrix M' is symplectic if it preserves the J'_h form, that is if $J'_h \circ M' = J'_h$.

Compatibility

Let M be a 2×2 matrix over K_h which is J_h-symplectic, then its descent $M' \in K_{h-1}^{2d_h \times 2d_h}$ is J'_h-symplectic.

Going further with symplectic symmetries in a recursive tower

$J_h \in \bigwedge^2(K_h^2)$ is the determinant form:

$$J_h\left(\begin{pmatrix} x_0 \\ x_1 \end{pmatrix}, \begin{pmatrix} y_0 \\ y_1 \end{pmatrix}\right) = x_0 y_1 - x_1 y_0$$

$\rightarrow$ Descend the form J_h in J'_h to K_{h-1} by composition with a non-trivial linear form $\tau : K_h \rightarrow K_{h-1}$

$\rightarrow$ Extend the definition of symplectism to $K_{h-1}^{2d_h}$

Symplectic group after descent

A $2d_h \times 2d_h$ matrix M' is symplectic if it preserves the J'_h form, that is if $J'_h \circ M' = J'_h$.

Compatibility

Let M be a 2×2 matrix over K_h which is J_h-symplectic, then its descent $M' \in K_{h-1}^{2d_h \times 2d_h}$ is J'_h-symplectic.

Compatibility with decompositions

Fix a basis of the symplectic space where the matrix corresponding to J'_h is $\begin{pmatrix} 0 & R_{d_h} \\ -R_{d_h} & 0 \end{pmatrix}$.

Then, for any M a J'_h-symplectic matrix and QR its QR decomposition, both Q and R are J'_h-symplectic.

Improved complexity [E-Kirchner-Fouque 2019]

Select an integer f a power of $q = \mathrm{O}(\log f)$ and let $n = \varphi(f)$. The complexity for reducing matrices M of dimension two over $L = \mathbb{Q}[x]/\Phi_f(x)$ with B the number of bits in the input coefficients is *heuristically*

$$\tilde{\mathrm{O}}\left(n^{2+\varepsilon(q)}B\right) + n^{\mathrm{O}(\log\log n)}, \qquad \varepsilon(q) = \frac{\log(1/2 + 1/2q)}{\log q} < 0$$

and the first column of the reduced matrix has coefficients bounded by

$$2^{\tilde{\mathrm{O}}(n)}\left|N_{K_h/\mathbb{Q}}(\det M)\right|^{\frac{1}{2n}}.$$

From that preliminary work...

Exploitation of the symplectic symmetries:

1. **Decrease** the complexity, but...
2. **Increase** the approximation factor

From that preliminary work...

- Getting further using higher-order symplectic structures

Exploitation of the symplectic symmetries:

1. **Decrease** the complexity, but...
2. **Increase** the approximation factor

Seek for transformations preserving arbitrary non-degenerate alternate forms (for example the *volume form*)

From that preliminary work...

- Getting further using higher-order symplectic structures

Exploitation of the symplectic symmetries:

1. **Decrease** the complexity, but...
2. **Increase** the approximation factor

Seek for transformations preserving arbitrary non-degenerate alternate forms (for example the *volume form*)

Problems:

- Non uniqueness of higher-order symplectic structures (no Darboux' structure theorem)
- Find a descent compatible with this additional structure

From that preliminary work...

- Getting further using higher-order symplectic structures

Exploitation of the symplectic symmetries:

1. **Decrease** the complexity, but...
2. **Increase** the approximation factor

Seek for transformations preserving arbitrary non-degenerate alternate forms (for example the *volume form*)

Problems:

- Non uniqueness of higher-order symplectic structures (no Darboux' structure theorem)
- Find a descent compatible with this additional structure

From that preliminary work...

- Getting further using higher-order symplectic structures
- Get rid of the heuristics: reduce *projective* modules

From that preliminary work...

- Getting further using higher-order symplectic structures

- Get rid of the heuristics: reduce *projective* modules

Over $\mathcal{O}_L$ a projective module is of the shape: $\alpha_1\mathfrak{a}_1 \oplus \cdots \oplus \alpha_n\mathfrak{a}_n$

- Need to adapt the lifting to ideals [Cohen]

From that preliminary work...

- Getting further using higher-order symplectic structures
- Get rid of the heuristics: reduce *projective* modules

Over $\mathcal{O}_L$ a projective module is of the shape: $\alpha_1\mathfrak{a}_1 \oplus \cdots \oplus \alpha_n\mathfrak{a}_n$

- Need to adapt the lifting to ideals [Cohen]
- Requires computations with ideals: bottleneck is now the ideal multiplication algorithm

From that preliminary work...

- Getting further using higher-order symplectic structures

- Get rid of the heuristics: reduce *projective* modules

Over $\mathcal{O}_L$ a projective module is of the shape: $\alpha_1 \mathfrak{a}_1 \oplus \cdots \oplus \alpha_n \mathfrak{a}_n$

- Need to adapt the lifting to ideals [Cohen]
- Requires computations with ideals: bottleneck is now the ideal multiplication algorithm
- 2-elements representation: multiplying $\mathfrak{a} = \alpha_1 \mathcal{O}_L + \alpha_2 \mathcal{O}_L, \mathfrak{b} = \beta_1 \mathcal{O}_L + \beta_2 \mathcal{O}_L$ consists in the reduction of the ideal generated by $(\alpha_i \beta_j)_{1 \leqslant i,j \leqslant 2}$ (module spanned by 4 elements)

From that preliminary work...

- Getting further using higher-order symplectic structures
- Get rid of the heuristics: reduce *projective* modules

Over $\mathcal{O}_L$ a projective module is of the shape: $\alpha_1\mathfrak{a}_1 \oplus \cdots \oplus \alpha_n\mathfrak{a}_n$

- Need to adapt the lifting to ideals [Cohen]
- Requires computations with ideals: bottleneck is now the ideal multiplication algorithm

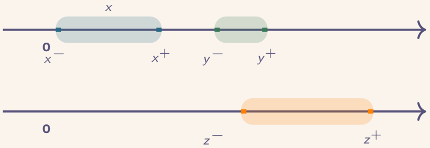
Cross recursive algorithms: reduction and ideal multiplication

From that preliminary work...

- Getting further using higher-order symplectic structures

- Get rid of the heuristics: reduce *projective* modules

- Certification using *Interval arithmetic*

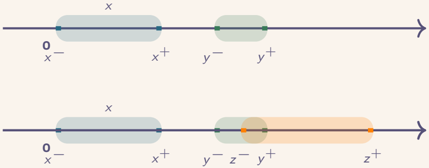


From that preliminary work...

- Getting further using higher-order symplectic structures

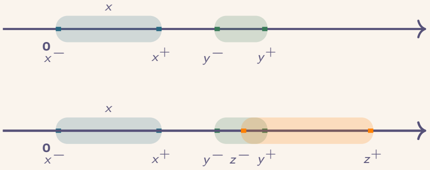
- Get rid of the heuristics: reduce *projective* modules

- Certification using *Interval arithmetic*



From that preliminary work...

- Getting further using higher-order symplectic structures
- Get rid of the heuristics: reduce *projective* modules
- Certification using *Interval arithmetic*



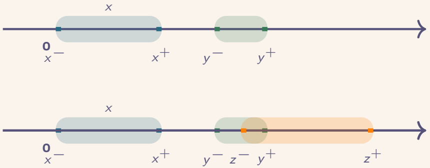
Interval Arithmetic used in such a way allows detecting lack of precision at runtime of a numerical algorithm.

From that preliminary work...

- Getting further using higher-order symplectic structures

- Get rid of the heuristics: reduce *projective* modules

- Certification using *Interval arithmetic*



Interval Arithmetic used in such a way allows detecting lack of precision at runtime of a numerical algorithm.

$\longrightarrow$ Certified reduction + use quasi-optimal precision with adaptive strategy

Proved, *certified* and *efficient* framework
for reducing *general* algebraic lattices

Thank you !