

Algebraic lattices in cryptography

Alice Pellet-Mary

Université de Bordeaux

Journées d'inauguration de la fédération MARGAUx
La Rochelle

Motivation: cryptography

Cryptographic primitives

public key
encryption

signature

homomorphic
encryption

...

error correcting codes

lattices

isogenies

factoring

discrete logarithm

...

(Supposedly intractable) algorithmic problems

Motivation: cryptography

Cryptographic primitives

public key
encryption

signature

homomorphic
encryption

...

error correcting codes

lattices

isogenies

~~factoring~~

~~discrete logarithm~~

...

(Supposedly intractable) algorithmic problems
in a quantum world

Motivation: cryptography

Cryptographic primitives

public key
encryption

signature

homomorphic
encryption

...

error correcting codes

lattices

isogenies

~~factoring~~

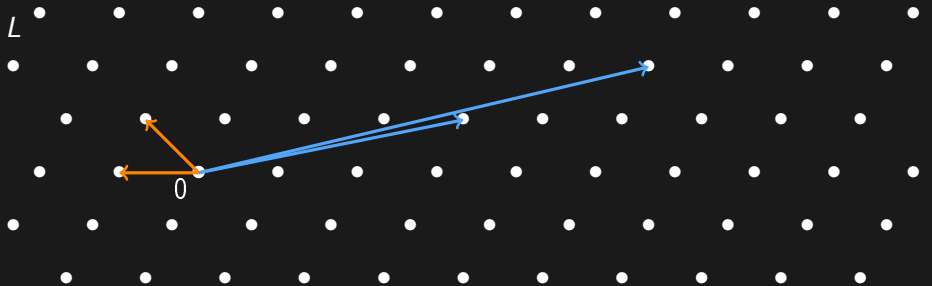
~~discrete logarithm~~

...

(Supposedly intractable) algorithmic problems
in a quantum world

Lattices

Lattices



- ▶ $L = \{Bx \mid x \in \mathbb{Z}^n\}$ is a **lattice**
- ▶ $B \in GL_n(\mathbb{R})$ is a **basis**
- ▶ n is the **dimension** of L

Algorithmic problems

L



SVP : Shortest Vector Problem

CVP : Closest Vector Problem

Algorithmic problems

L



approx-SVP : Shortest Vector Problem

approx-CVP : Closest Vector Problem

Algorithmic problems



approx-SVP : Shortest Vector Problem

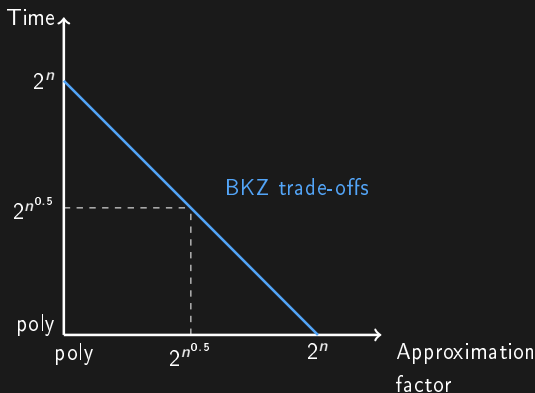
approx-CVP : Closest Vector Problem

Supposedly **hard** to solve when n is large (input: a bad basis of L)

- ▶ even with a **quantum** computer
- ▶ even with a small **approximation factor** ($\text{poly}(n)$)

Hardness of SVP and CVP

Best Time/Approximation trade-off for SVP, CVP (even quantumly):
BKZ algorithm [Sch87,SE94]

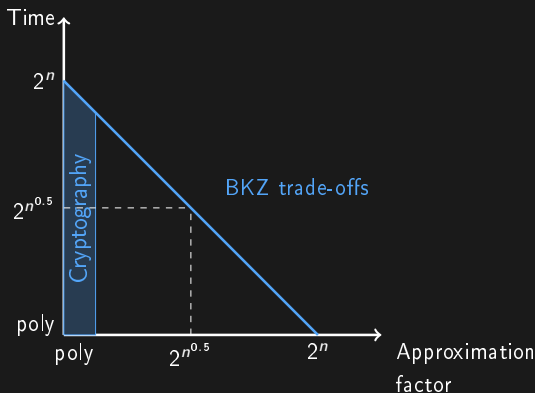


[Sch87] C.-P. Schnorr. A hierarchy of polynomial time lattice basis reduction algorithms. TCS.

[SE94] C.-P. Schnorr and M. Euchner. Lattice basis reduction: improved practical algorithms and solving subset sum problems. Mathematical programming.

Hardness of SVP and CVP

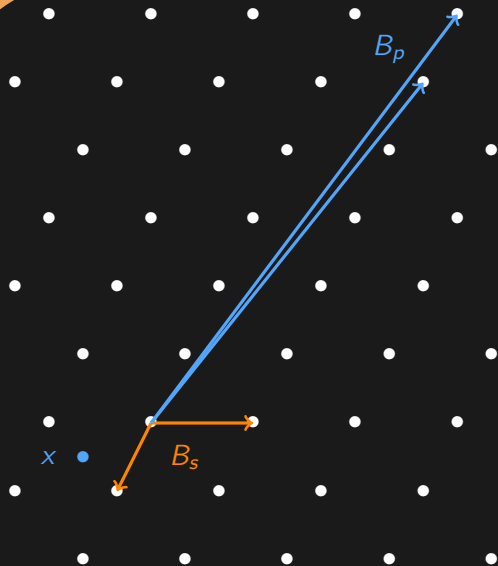
Best Time/Approximation trade-off for SVP, CVP (even quantumly):
BKZ algorithm [Sch87,SE94]



[Sch87] C.-P. Schnorr. A hierarchy of polynomial time lattice basis reduction algorithms. TCS.

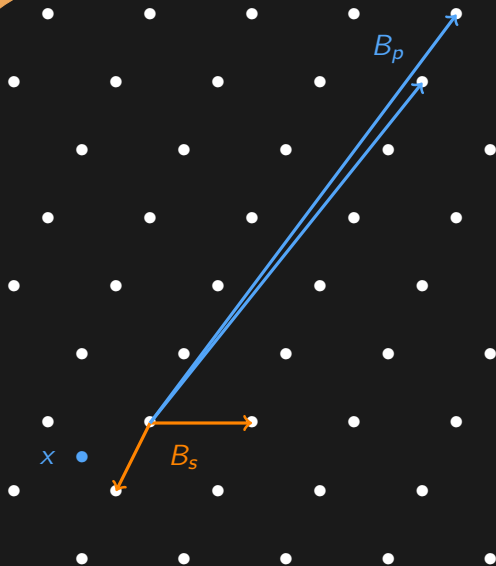
[SE94] C.-P. Schnorr and M. Euchner. Lattice basis reduction: improved practical algorithms and solving subset sum problems. Mathematical programming.

Public key encryption from lattices



$$\text{pk} = (B_p, x)$$
$$\text{sk} = B_s$$

Public key encryption from lattices

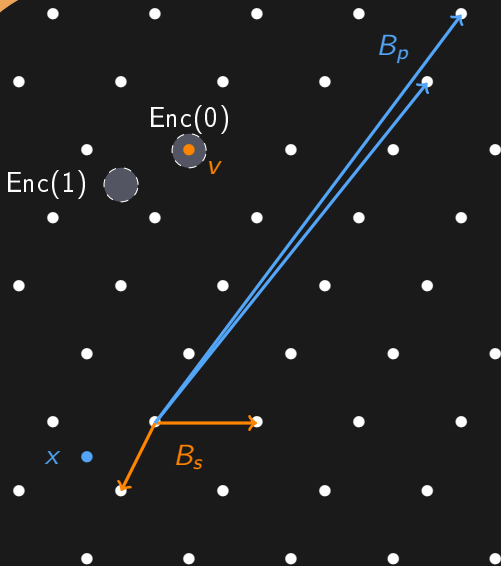


$$\text{pk} = (B_p, x)$$

$$\text{sk} = B_s$$

message: $m \in \{0, 1\}$

Public key encryption from lattices



$$pk = (B_p, x)$$

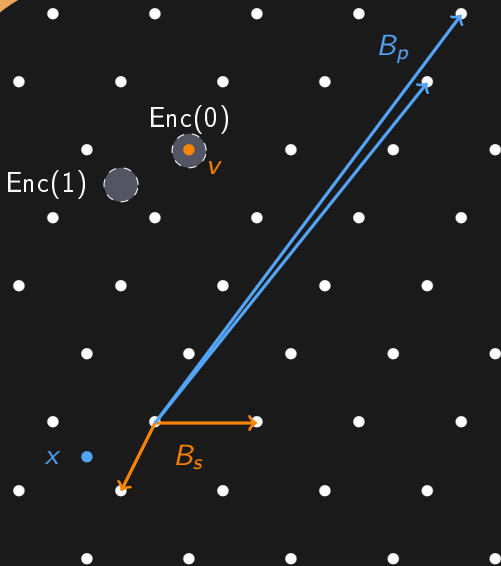
$$sk = B_s$$

message: $m \in \{0, 1\}$

Encryption(m, pk):

- ▶ sample random $v \in L$
- ▶ sample small $e \in \mathbb{R}^n$
- ▶ return $c = v + e + m \cdot x$

Public key encryption from lattices



$$\text{pk} = (B_p, x)$$

$$\text{sk} = B_s$$

message: $m \in \{0, 1\}$

Encryption(m, pk):

- ▶ sample random $v \in L$
- ▶ sample small $e \in \mathbb{R}^n$
- ▶ return $c = v + e + m \cdot x$

Decryption(c, sk):

- ▶ find $w \in L$ closest to c
- ▶ if c is very close to w , return $m = 0$
- ▶ otherwise return $m = 1$

Structured lattices

Why?

Motivation

Schemes using lattices are usually not efficient

(storage: n^2 , matrix-vector mult: n^2)

⇒ improve efficiency using **structured lattices**

Why?

Motivation

Schemes using lattices are usually not efficient

(storage: n^2 , matrix-vector mult: n^2)

⇒ improve efficiency using **structured lattices**

Two examples: (submitted to the NIST post-quantum standardization process)

	Frodo (unstructured lattices)	Kyber (structured lattices)
secret key size (in Bytes)	19 888	1 632
public key size (in Bytes)	9 616	800

Structured lattices: example

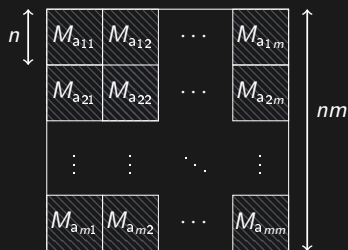
$$M_a = \begin{pmatrix} a_1 & -a_n & \cdots & -a_2 \\ a_2 & a_1 & \cdots & -a_3 \\ \vdots & \ddots & \ddots & \vdots \\ a_n & a_{n-1} & \cdots & a_1 \end{pmatrix}$$

basis of a special case of
ideal lattice

Structured lattices: example

$$M_a = \begin{pmatrix} a_1 & -a_n & \cdots & -a_2 \\ a_2 & a_1 & \cdots & -a_3 \\ \vdots & \ddots & \ddots & \vdots \\ a_n & a_{n-1} & \cdots & a_1 \end{pmatrix}$$

basis of a special case of
ideal lattice

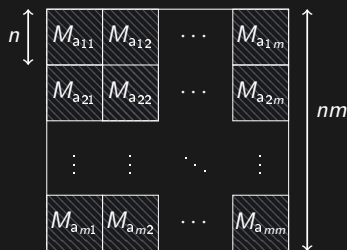


basis of a special case of
module lattice
of rank m

Structured lattices: example

$$M_a = \begin{pmatrix} a_1 & -a_n & \cdots & -a_2 \\ a_2 & a_1 & \cdots & -a_3 \\ \vdots & \ddots & \ddots & \vdots \\ a_n & a_{n-1} & \cdots & a_1 \end{pmatrix}$$

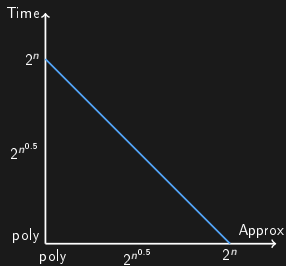
basis of a special case of
ideal lattice



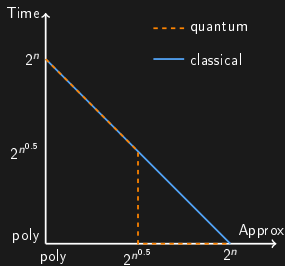
basis of a special case of
module lattice
of rank m

Is SVP still hard when restricted to ideal/module lattices?

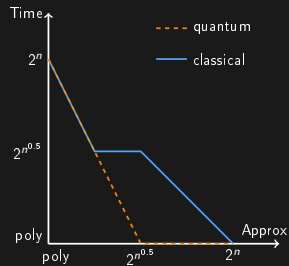
SVP in modules and ideals



Modules
(rank ≥ 2)

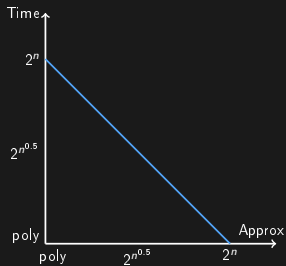


ideals
(in cyclotomic fields)

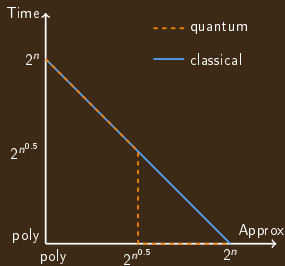


ideals
(with $2^{O(n)}$ pre-processing)

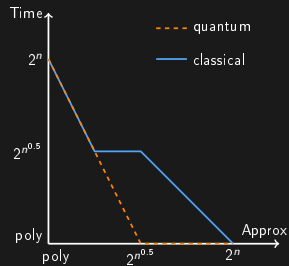
SVP in modules and ideals



Modules
(rank ≥ 2)

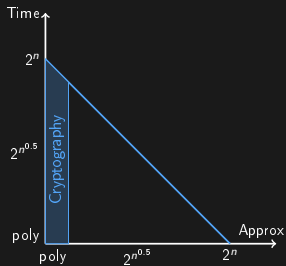


ideals
(in cyclotomic fields)

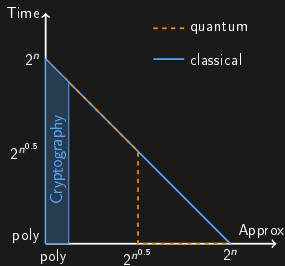


ideals
(with $2^{O(n)}$ pre-processing)

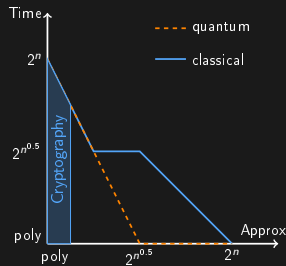
Impact on cryptography



Modules
(rank ≥ 2)

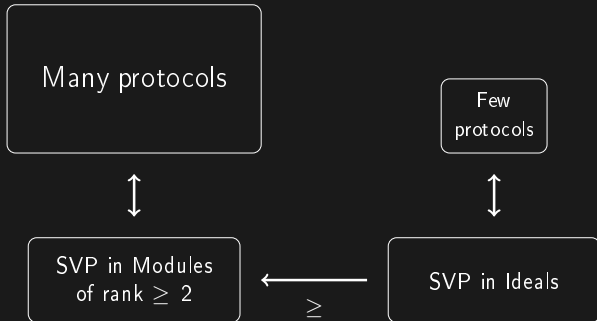


ideals
(in cyclotomic fields)



ideals
(with $2^{O(n)}$ pre-processing)

Impact on cryptography



Algorithms for ideal lattices

History: algorithms for ideal-SVP

[RBV04]: principal ideals in small dimension

[RBV04] G. Rekaya, J.-C. Belfiore, E. Viterbo. A very efficient lattice reduction tool on fast fading channels. ISITA.

History: algorithms for ideal-SVP

[RBV04]: principal ideals in small dimension

[CGS14]: principal ideals in cyclotomic fields
(without analysis)

[CGS14]: P. Campbell, M. Groves, and D. Shepherd. Soliloquy: a cautionary tale.

History: algorithms for ideal-SVP

[RBV04]: principal ideals in small dimension

[CGS14]: principal ideals in cyclotomic fields
(without analysis)

[CDPR16]: analysis of [CGS14]
 $\Rightarrow 2^{O(\sqrt{n})}$ approximation factor in quantum poly time

[CDPR16] R. Cramer, L. Ducas, C. Peikert and O. Regev. Recovering short generators of principal ideals in cyclotomic rings. Eurocrypt.

History: algorithms for ideal-SVP

[RBV04]: principal ideals in small dimension

[CGS14]: principal ideals in cyclotomic fields
(without analysis)

[CDPR16]: analysis of [CGS14]
 $\Rightarrow 2^{O(\sqrt{n})}$ approximation factor in quantum poly time

[CDW17]: any ideal in cyclotomic fields

[CDW17] R. Cramer, L. Ducas, B. Wesolowski. Short stickelberger class relations and application to ideal-SVP.
Eurocrypt.

History: algorithms for ideal-SVP

[RBV04]: principal ideals in small dimension

[CGS14]: principal ideals in cyclotomic fields
(without analysis)

[CDPR16]: analysis of [CGS14]
 $\Rightarrow 2^{O(\sqrt{n})}$ approximation factor in quantum poly time

[CDW17]: any ideal in cyclotomic fields

[PHS19]: more trade-offs but exponential pre-processing
(any ideal, any number field)

[PHS19] A. Pellet-Mary, G. Hanrot, D. Stehlé. Approx-SVP in ideal lattices with pre-processing. Eurocrypt.

History: algorithms for ideal-SVP

[RBV04]: principal ideals in small dimension

[CGS14]: principal ideals in cyclotomic fields
(without analysis)

[CDPR16]: analysis of [CGS14]
 $\Rightarrow 2^{O(\sqrt{n})}$ approximation factor in quantum poly time

[CDW17]: any ideal in cyclotomic fields

[PHS19]: more trade-offs but exponential pre-processing
(any ideal, any number field)

[PHS19] A. Pellet-Mary, G. Hanrot, D. Stehlé. Approx-SVP in ideal lattices with pre-processing. Eurocrypt.

Notation

$K = \mathbb{Q}[X]/(X^n + 1)$, with $n = 2^k$ (or any cyclotomic field)

$O_K = \mathbb{Z}[X]/(X^n + 1)$

Notation

$K = \mathbb{Q}[X]/(X^n + 1)$, with $n = 2^k$ (or any cyclotomic field)

$O_K = \mathbb{Z}[X]/(X^n + 1)$

► **Units:** $O_K^\times = \{a \in O_K \mid \exists b \in O_K, ab = 1\}$

Notation

$K = \mathbb{Q}[X]/(X^n + 1)$, with $n = 2^k$ (or any cyclotomic field)

$O_K = \mathbb{Z}[X]/(X^n + 1)$

- ▶ **Units:** $O_K^\times = \{a \in O_K \mid \exists b \in O_K, ab = 1\}$
- ▶ **Principal ideals:** $\langle g \rangle = \{gr \mid r \in O_K\}$
 - ▶ g is a **generator** of $\langle g \rangle$
 - ▶ $\{\text{generators of } \langle g \rangle\} = \{gu \mid u \in O_K^\times\}$

Why is $\langle g \rangle$ a lattice?

O_K is a lattice

$$O_K = \mathbb{Z}[X]/(X^n + 1) \rightarrow \mathbb{C}^n$$
$$r(X) \mapsto (r(\alpha_1), r(\alpha_2), \dots, r(\alpha_n)),$$

where $\alpha_1, \dots, \alpha_n$ are the roots of $X^n + 1$ in \mathbb{C}



Why is $\langle g \rangle$ a lattice?

O_K is a lattice

$$O_K = \mathbb{Z}[X]/(X^n + 1) \rightarrow \mathbb{C}^n$$
$$r(X) \mapsto (r(\alpha_1), r(\alpha_2), \dots, r(\alpha_n)),$$

where $\alpha_1, \dots, \alpha_n$ are the roots of $X^n + 1$ in \mathbb{C}

$$\begin{cases} \langle g \rangle \subseteq O_K \simeq \mathbb{Z}^n \\ \text{stable by '+' and '-'} \end{cases} \Rightarrow \text{ideal lattice}$$



Objective and first idea [CDPR,CGS14]

Objective: Given a basis of $\langle g \rangle$, find a (somehow) small element $gr \in \langle g \rangle$

Objective and first idea [CDPR,CGS14]

Objective: Given a basis of $\langle g \rangle$, find a (somehow) small element $gr \in \langle g \rangle$

Idea: Maybe g is a somehow small element of $\langle g \rangle$

Objective and first idea [CDPR,CGS14]

Objective: Given a basis of $\langle g \rangle$, find a (somehow) small element $gr \in \langle g \rangle$

Idea: Maybe g is a somehow small element of $\langle g \rangle$

► If $n = 1$: e.g. $\langle 2 \rangle \Rightarrow 2$ and -2 are the smallest elements.



Objective and first idea [CDPR,CGS14]

Objective: Given a basis of $\langle g \rangle$, find a (somehow) small element $gr \in \langle g \rangle$

Idea: Maybe g is a somehow small element of $\langle g \rangle$

► If $n = 1$: e.g. $\langle 2 \rangle \Rightarrow 2$ and -2 are the smallest elements.

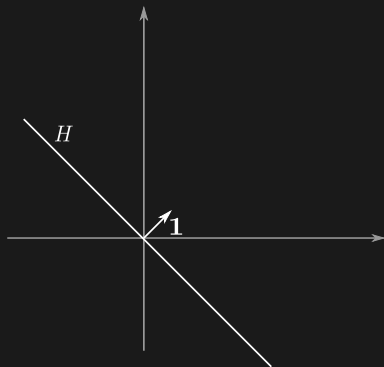


► For larger n : one of the generators is somehow small

The Log space

$\text{Log} : \mathcal{O}_K \rightarrow \mathbb{R}^n$ (take the log of every coordinate)

Let $\mathbf{1} = (1, \dots, 1)$ and $H = \mathbf{1}^\perp$.



The Log space

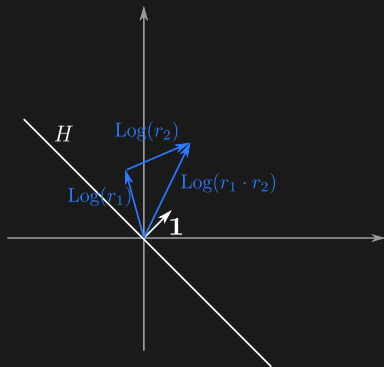
$\text{Log} : \mathcal{O}_K \rightarrow \mathbb{R}^n$ (take the log of every coordinate)

Let $\mathbf{1} = (1, \dots, 1)$ and $H = \mathbf{1}^\perp$.

Properties ($r \in \mathcal{O}_K$)

$\text{Log } r = h + a \cdot \mathbf{1}$, with $h \in H$

- $\text{Log}(r_1 \cdot r_2) = \text{Log}(r_1) + \text{Log}(r_2)$



The Log space

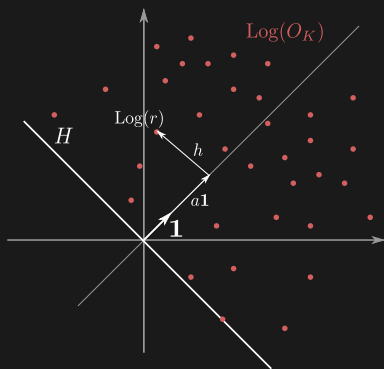
$\text{Log} : \mathcal{O}_K \rightarrow \mathbb{R}^n$ (take the log of every coordinate)

Let $\mathbf{1} = (1, \dots, 1)$ and $H = \mathbf{1}^\perp$.

Properties ($r \in \mathcal{O}_K$)

$\text{Log } r = h + a \cdot \mathbf{1}$, with $h \in H$

- $\text{Log}(r_1 \cdot r_2) = \text{Log}(r_1) + \text{Log}(r_2)$
- $a \geq 0$



The Log space

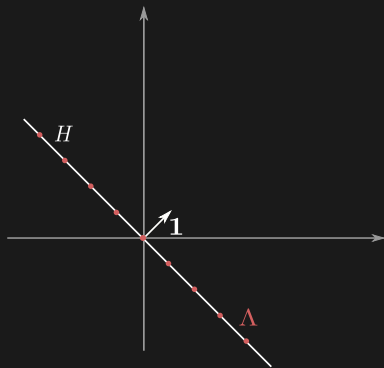
$\text{Log} : O_K \rightarrow \mathbb{R}^n$ (take the log of every coordinate)

Let $\mathbf{1} = (1, \dots, 1)$ and $H = \mathbf{1}^\perp$.

Properties ($r \in O_K$)

$\text{Log } r = h + a \cdot \mathbf{1}$, with $h \in H$

- $\text{Log}(r_1 \cdot r_2) = \text{Log}(r_1) + \text{Log}(r_2)$
- $a \geq 0$
- $a = 0$ iff r is a unit



The Log space

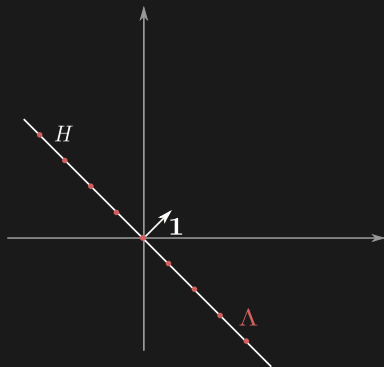
$\text{Log} : O_K \rightarrow \mathbb{R}^n$ (take the log of every coordinate)

Let $\mathbf{1} = (1, \dots, 1)$ and $H = \mathbf{1}^\perp$.

Properties ($r \in O_K$)

$\text{Log } r = h + a \cdot \mathbf{1}$, with $h \in H$

- $\text{Log}(r_1 \cdot r_2) = \text{Log}(r_1) + \text{Log}(r_2)$
- $a \geq 0$
- $a = 0$ iff r is a unit



The Log unit lattice

$\Lambda := \text{Log}(O_K^\times)$ is a lattice in H .

The Log space

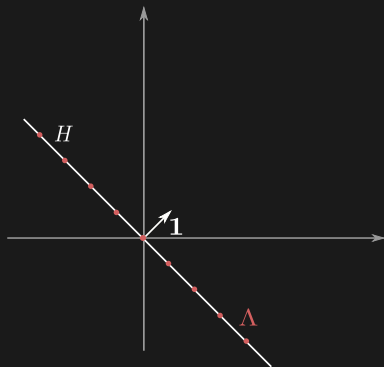
$\text{Log} : O_K \rightarrow \mathbb{R}^n$ (take the log of every coordinate)

Let $\mathbf{1} = (1, \dots, 1)$ and $H = \mathbf{1}^\perp$.

Properties ($r \in O_K$)

$\text{Log } r = h + a \cdot \mathbf{1}$, with $h \in H$

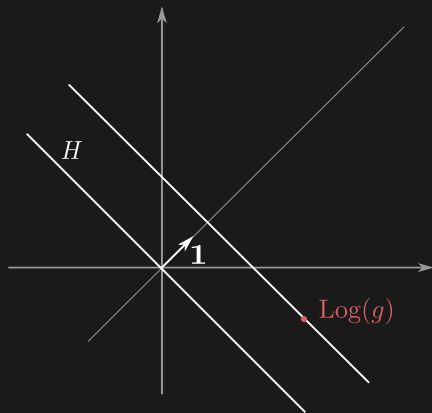
- $\text{Log}(r_1 \cdot r_2) = \text{Log}(r_1) + \text{Log}(r_2)$
- $a \geq 0$
- $a = 0$ iff r is a unit
- $\|r\| \simeq \exp(\|\text{Log } r\|_\infty)$



The Log unit lattice

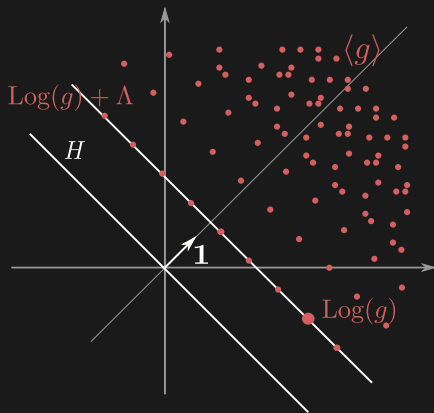
$\Lambda := \text{Log}(O_K^\times)$ is a lattice in H .

What does $\text{Log}\langle g \rangle$ look like?



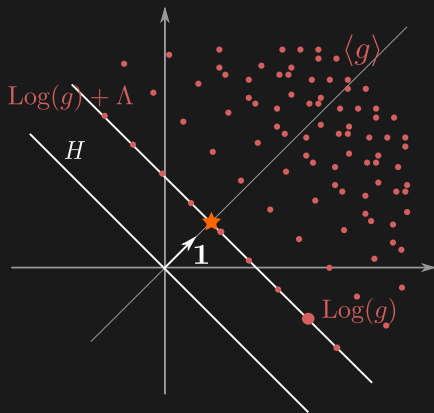
The algorithm [CGS14,CDPR16]

What does $\text{Log}\langle g \rangle$ look like?



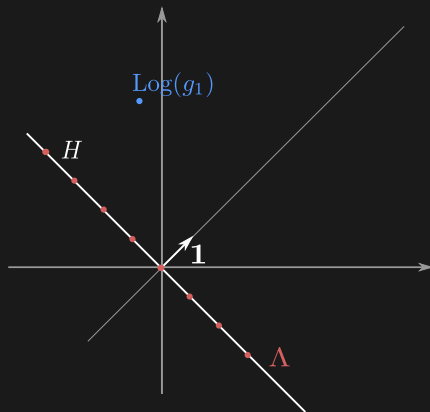
The algorithm [CGS14,CDPR16]

What does $\text{Log}\langle g \rangle$ look like?



The algorithm [CGS14,CDPR16]

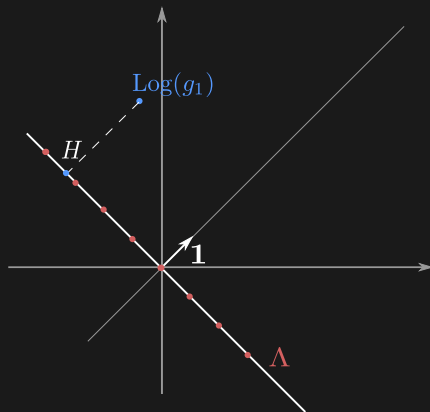
- ▶ Find a generator g_1 of $\langle g \rangle$.
 - ▶ [BS16]: quantum poly time



[BS16]: J.-F. Biasse, F. Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. SODA.

The algorithm [CGS14,CDPR16]

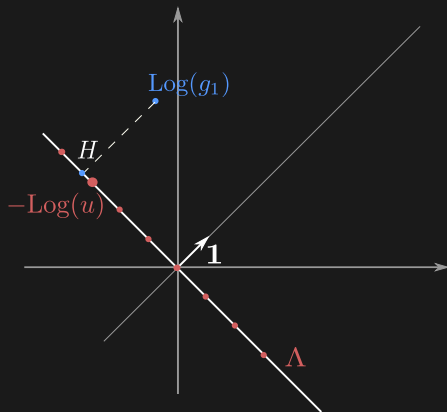
- ▶ Find a generator g_1 of $\langle g \rangle$.
 - ▶ [BS16]: quantum poly time



[BS16]: J.-F. Biasse, F. Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. SODA.

The algorithm [CGS14,CDPR16]

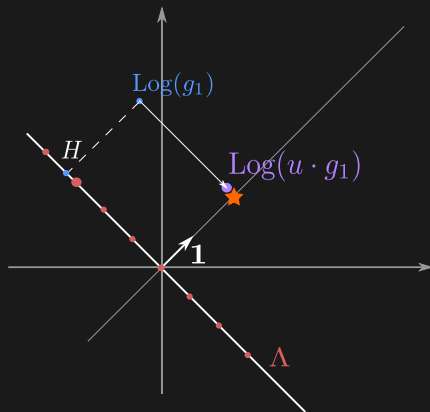
- ▶ Find a generator g_1 of $\langle g \rangle$.
 - ▶ [BS16]: quantum poly time
- ▶ Solve CVP in Λ



[BS16]: J.-F. Biasse, F. Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. SODA.

The algorithm [CGS14,CDPR16]

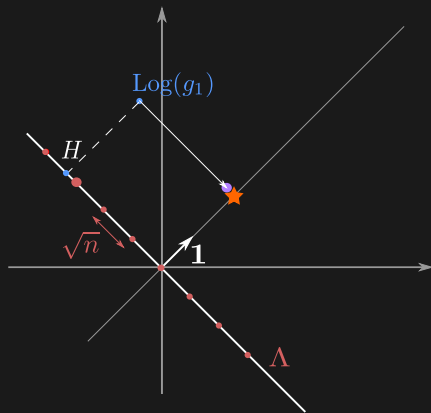
- ▶ Find a generator g_1 of $\langle g \rangle$.
 - ▶ [BS16]: quantum poly time
- ▶ Solve CVP in Λ



[BS16]: J.-F. Biasse, F. Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. SODA.

The algorithm [CGS14,CDPR16]

- ▶ Find a generator g_1 of $\langle g \rangle$.
 - ▶ [BS16]: quantum poly time
- ▶ Solve CVP in Λ
 - ▶ Good basis of Λ
(cyclotomic field)
 - \Rightarrow CVP in poly time
 - $\Rightarrow \|h\| \leq \tilde{O}(\sqrt{n})$

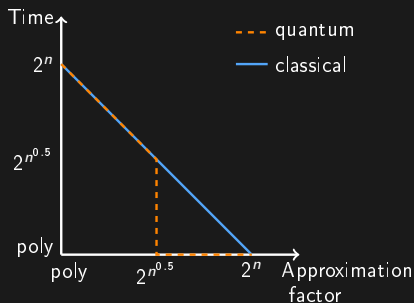


[BS16]: J.-F. Biasse, F. Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. SODA.

The algorithm [CGS14,CDPR16]

- ▶ Find a generator g_1 of $\langle g \rangle$.
 - ▶ [BS16]: quantum poly time
- ▶ Solve CVP in Λ
 - ▶ Good basis of Λ (cyclotomic field)
 \Rightarrow CVP in poly time
 $\Rightarrow \|h\| \leq \tilde{O}(\sqrt{n})$

$$\|ug_1\| \leq 2^{\tilde{O}(\sqrt{n})} \cdot \lambda_1$$



- Heuristic
- Cyclotomic fields

[BS16]: J.-F. Biasse, F. Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. SODA.

Conclusion

Some open questions

- ▶ Are there some number fields stronger than others?
(are cyclotomic fields particularly weak?)

Some open questions

- ▶ Are there some number fields stronger than others?
(are cyclotomic fields particularly weak?)
- ▶ Are modules of rank ≥ 2 really safer than ideals?

Some open questions

- ▶ Are there some number fields stronger than others?
(are cyclotomic fields particularly weak?)
- ▶ Are modules of rank ≥ 2 really safer than ideals?
- ▶ Are there some better structured lattices?

Some open questions

- ▶ Are there some number fields stronger than others?
(are cyclotomic fields particularly weak?)
- ▶ Are modules of rank ≥ 2 really safer than ideals?
- ▶ Are there some better structured lattices?

Thank you