Twisted-PHS: Using the Product Formula to Solve Approx-SVP in Ideal Lattices

Olivier Bernard[1,2] Adeline Roux-Langlois[1]

[1]Univ Rennes, CNRS, IRISA
{olivier.bernard, adeline.roux-langlois}@irisa.fr

[2]Thales, Gennevilliers, Laboratoire CHiffre

Asiacrypt 2020

9th December

Today's à la carte

1. Historical timeline
2. A twisted description of the log-S-unit lattice
   - Units: reducing Principal Ideal Generators
   - S-units: reducing Class group Discrete Logarithms
   - Using the Product Formula
3. Experimental results
   - Log-S-unit lattice geometry
   - Ideal-SVP approximation factors
4. What's next ?

Today's à la carte

1. Historical timeline
2. A twisted description of the log-S-unit lattice
   - Units: reducing Principal Ideal Generators
   - S-units: reducing Class group Discrete Logarithms
   - Using the Product Formula
3. Experimental results
   - Log-S-unit lattice geometry
   - Ideal-SVP approximation factors
4. What's next ?

Shortest Vector Problem

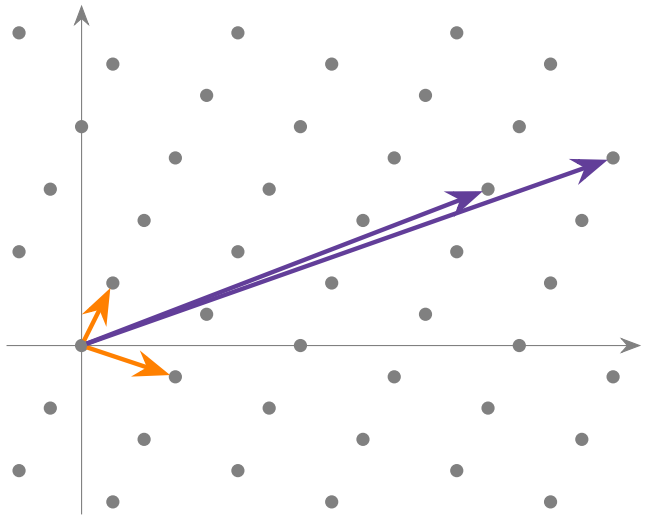
Definition (Lattice)

A lattice L is a discrete subgroup of $\mathbb{R}^n$ (say a "$\mathbb{Z}$-vector space").

Example: $\begin{pmatrix} 1 & 2 \\ 3 & -1 \end{pmatrix}$ and $\begin{pmatrix} 13 & 5 \\ 17 & 6 \end{pmatrix}$ are two possible bases.

Shortest Vector Problem (SVP)

Given a basis of L, find the shortest $v \in L$:
$$\|v\|_2 = \lambda_1(L).$$



Structured variants: Ideal, Module

- Hard problem (quantumly and classically)

On lattice-based cryptography

Post-Quantum Cryptography: NIST Competition

- Numerous lattice-based submissions;
- Rely (mostly) on LWE, Ring-LWE et Module-LWE;

Security proofs

Worst case to average case reductions, in particular:

$$\text{id-SVP} \leq \text{Ring-LWE},$$
$$\text{mod-SVP} \leq \text{Module-LWE}.$$

- How hard is id-SVP?

Structured cryptanalysis

Algorithmic Number Theory

Class group, units, S-units computations: *(number field of degree n)*

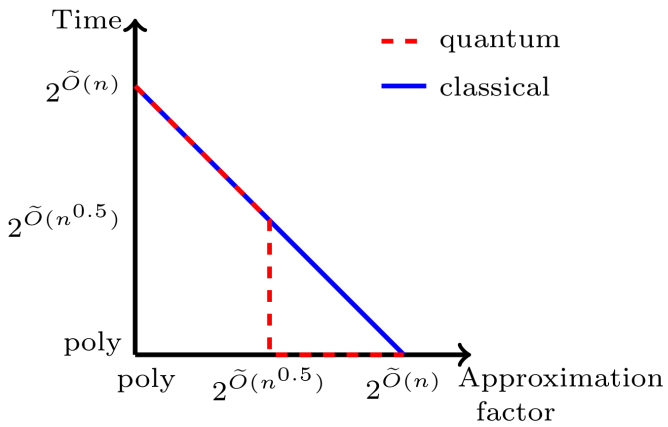
1. Classically: $2^{\sqrt{n}}$ in cyclotomic fields, $2^{n^{2/3}}$ in general.
2. Quantumly: polynomial [EHKS14,BS16]

Structured cryptanalysis

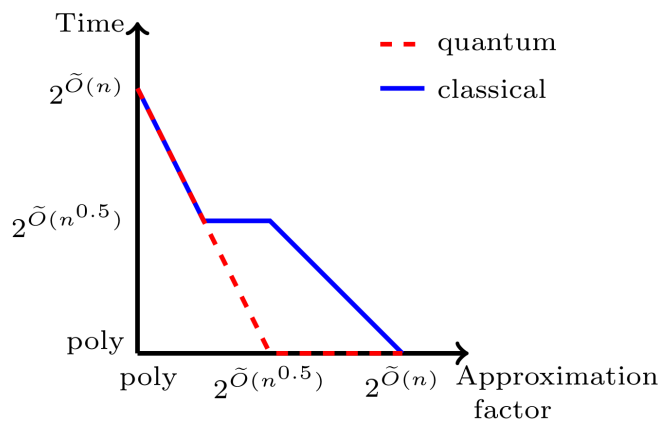
Impacts on Approx-id-SVP ?

1. [CGS14] Find a short generator is easy? (Cyclotomic fields)
2. [CDPR16] Proves [CGS14], generically does not solve id-SVP.
3. [CDW17] Extend to all ideals thanks to the Stickelberger lattice.
4. [DPW19] Experiments on [CDW17]: beats BKZ-300 for $n \geq 24000$.
5. [PHS19] Extends to all fields, but precomputation in 2^n.

[CDW17][1]



[PHS19] (with 2^n precomputation)[1]



[1] Graphs taken from [PHS19, Fig.1.1-2]. Thanks to Alice Pellet-Mary for sharing !

This work: a new twisted log-S-unit lattice description

Our work: Twisted-PHS

1. Description of the log-S-unit lattice using the Product Formula: add weights $\ln \mathcal{N}(\mathfrak{p})$ to valuations at $\mathfrak{p}$.
2. Prove this is at least as good as [PHS19] (under same heuristics).
3. Experimentally: orthogonal lattice, tiny approximation factors.

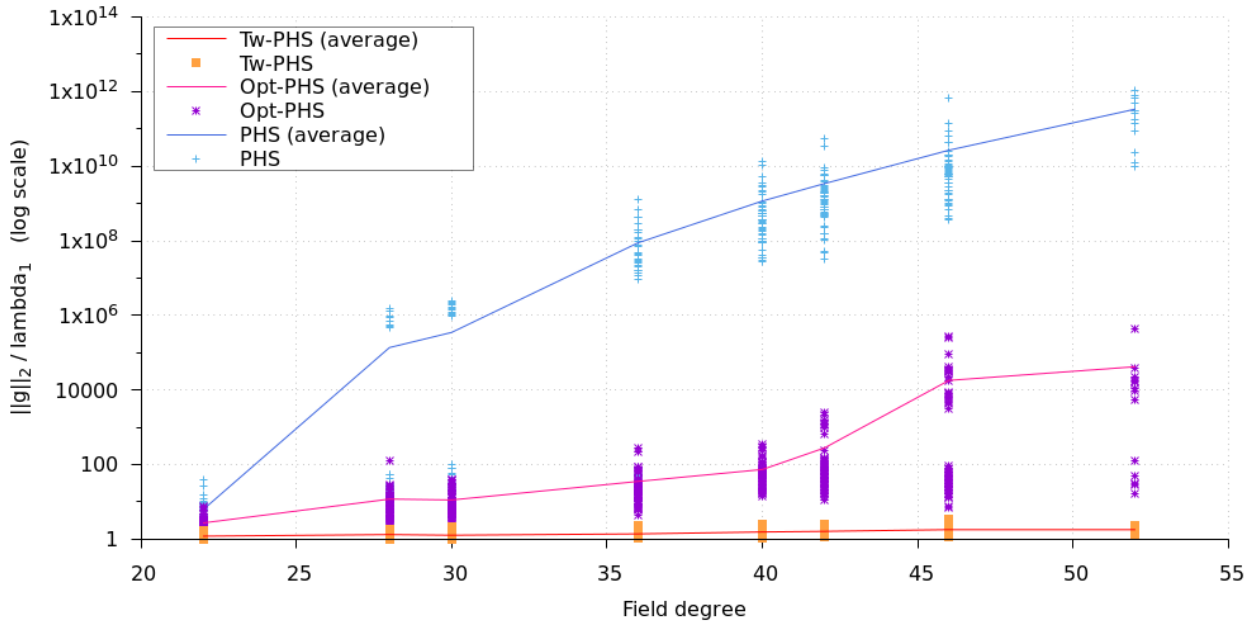


Figure: prime conductor cyclotomic fields, avg. over 50 ideals of 100-bits prime norm.

Experimental consequences: a Christmas list

Potential impacts on Approx-id-SVP:

- No theoretical impact (yet)
- Orthogonal: No more exponential precomputation (quantumly) ?
- Tiny aproximation factors: beats Schnorr's hierarchy ?

▶ Towards a quantum polynomial time algorithm to break id-SVP ?

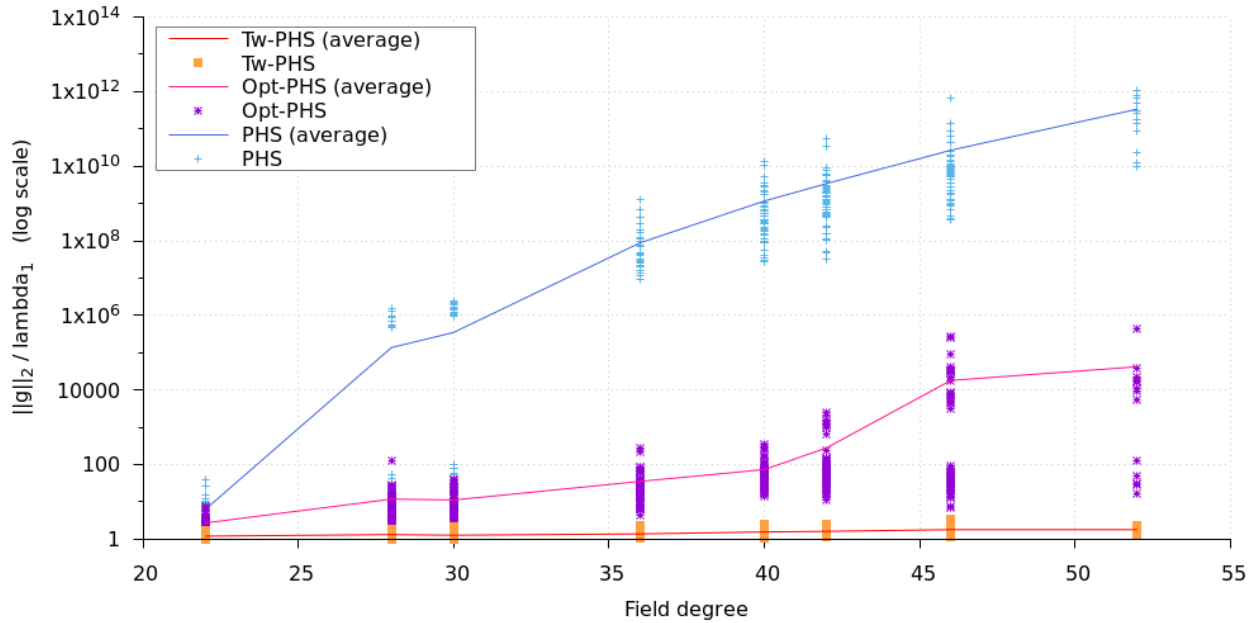


Figure: prime conductor cyclotomic fields, avg. over 50 ideals of 100-bits prime norm.

Today's à la carte

1. Historical timeline

2. A twisted description of the log-S-unit lattice
   - Units: reducing Principal Ideal Generators
   - S-units: reducing Class group Discrete Logarithms
   - Using the Product Formula

3. Experimental results
   - Log-S-unit lattice geometry
   - Ideal-SVP approximation factors

4. What's next ?

The log-unit lattice

Let K a number field of degree n, $\{\sigma : K \hookrightarrow \mathbb{C}\}$ its embeddings into $\mathbb{C}$.

Algebraic unit

An algebraic integer $u \in K$ is a unit iff:

$$1 = |\mathcal{N}(u)| \quad \Big(= \prod_\sigma |\sigma(u)|\Big).$$

Logarithmic embedding

$$\mathrm{Log}_\infty : \alpha \in K \longmapsto \Big(\ln|\sigma(\alpha)|\Big)_\sigma \in \mathbb{R}^n.$$

Hence:

- u is a unit $\iff$ $\mathrm{Log}_\infty(u) \in \mathbf{1}^\perp$.
- Their images form the log-unit lattice: $\Lambda_K \subsetneq \mathbf{1}^\perp$.

The log-unit lattice

Let K a number field of degree n, $\{\sigma : K \hookrightarrow \mathbb{C}\}$ its embeddings into $\mathbb{C}$.

Algebraic unit

An algebraic integer $u \in K$ is a unit iff:

$$1 = |\mathcal{N}(u)| \quad \Big(= \prod_\sigma |\sigma(u)|\Big).$$

Logarithmic embedding

$$\mathsf{Log}_\infty : \alpha \in K \longmapsto \Big(\ln|\sigma(\alpha)|\Big)_\sigma \qquad \in \mathbb{R}^n.$$

Hence:

- u is a unit $\iff$ $\mathsf{Log}_\infty(u) \in \mathbf{1}^\perp$.
- Their images form the log-unit lattice: $\Lambda_K \subsetneq \mathbf{1}^\perp$.

The log-unit lattice

Let K a number field of degree n, $\{\sigma : K \hookrightarrow \mathbb{C}\}$ its embeddings into $\mathbb{C}$.

Algebraic unit

An algebraic integer $u \in K$ is a unit iff:

$$1 = |\mathcal{N}(u)| \quad \Big(= \prod_\sigma |\sigma(u)|\Big).$$

Logarithmic embedding

$$\mathrm{Log}_\infty : \alpha \in K \longmapsto \Big(\ln|\sigma(\alpha)|\Big)_\sigma \qquad \in \mathbb{R}^n.$$

Hence:

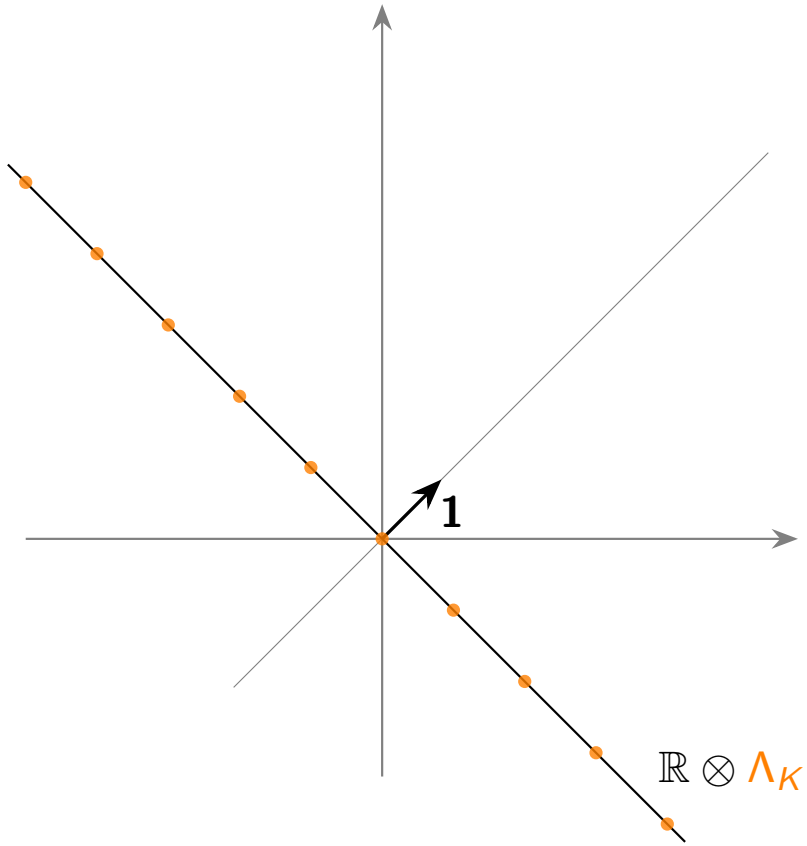
- u is a unit $\iff$ $\mathrm{Log}_\infty(u) \in \mathbf{1}^\perp$.
- Their images form the log-unit lattice: $\Lambda_K \subsetneq \mathbf{1}^\perp$.

Folklore: generator reduction

Let $\mathfrak{b}$ a principal ideal challenge, given as $\langle g_0 \rangle = \mathfrak{b}$.

Shortest generator: $g = u^{-1} \cdot g_0$, $\mathrm{Log}_\infty g \in \mathrm{Log}_\infty g_0 + \Lambda_K$.

1. Project $\mathrm{Log}_\infty g_0$ into $\mathbb{R} \otimes \Lambda_K$.
2. Find the closest $\mathrm{Log}_\infty u \in \Lambda_K$.
3. Output g_0/u.

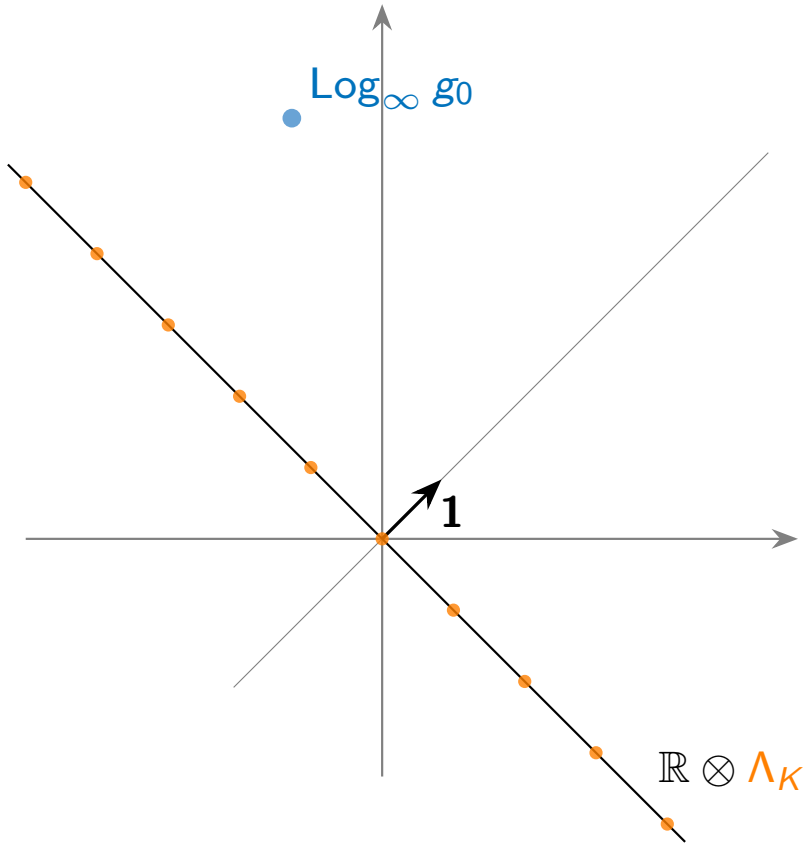


Folklore: generator reduction

Let $\mathfrak{b}$ a principal ideal challenge, given as $\langle g_0 \rangle = \mathfrak{b}$.

Shortest generator: $g = u^{-1} \cdot g_0$, $\mathrm{Log}_\infty g \in \mathrm{Log}_\infty g_0 + \Lambda_K$.

1. Project $\mathrm{Log}_\infty g_0$ into $\mathbb{R} \otimes \Lambda_K$.
2. Find the closest $\mathrm{Log}_\infty u \in \Lambda_K$.
3. Output g_0/u.

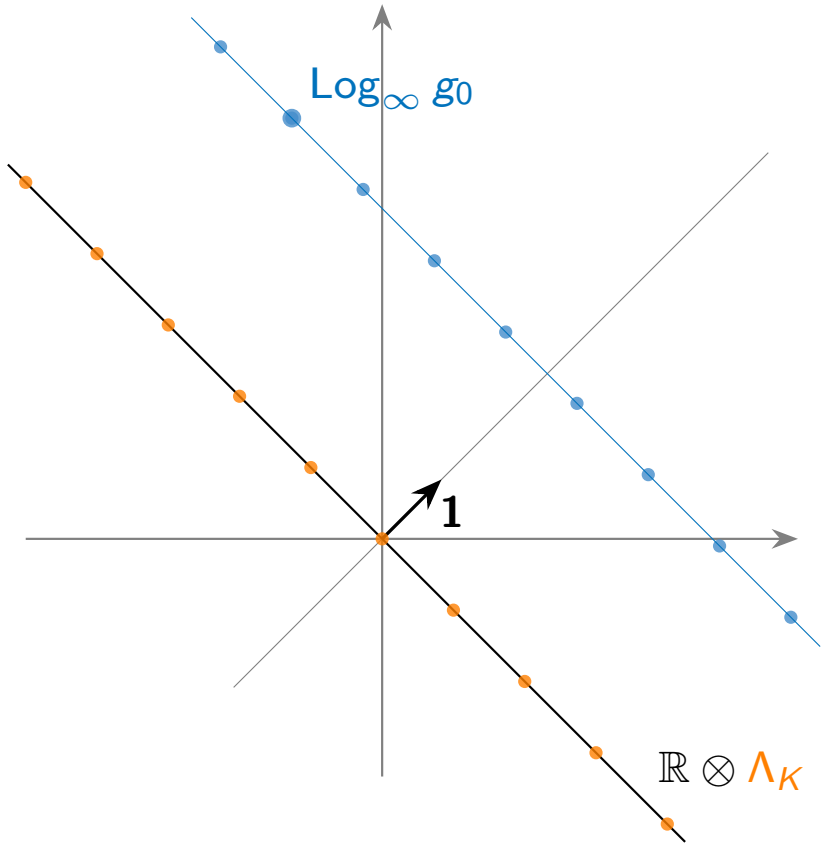


Folklore: generator reduction

Let $\mathfrak{b}$ a principal ideal challenge, given as $\langle g_0 \rangle = \mathfrak{b}$.

Shortest generator: $g = u^{-1} \cdot g_0$, $\mathrm{Log}_\infty g \in \mathrm{Log}_\infty g_0 + \Lambda_K$.

1. Project $\mathrm{Log}_\infty g_0$ into $\mathbb{R} \otimes \Lambda_K$.
2. Find the closest $\mathrm{Log}_\infty u \in \Lambda_K$.
3. Output g_0/u.

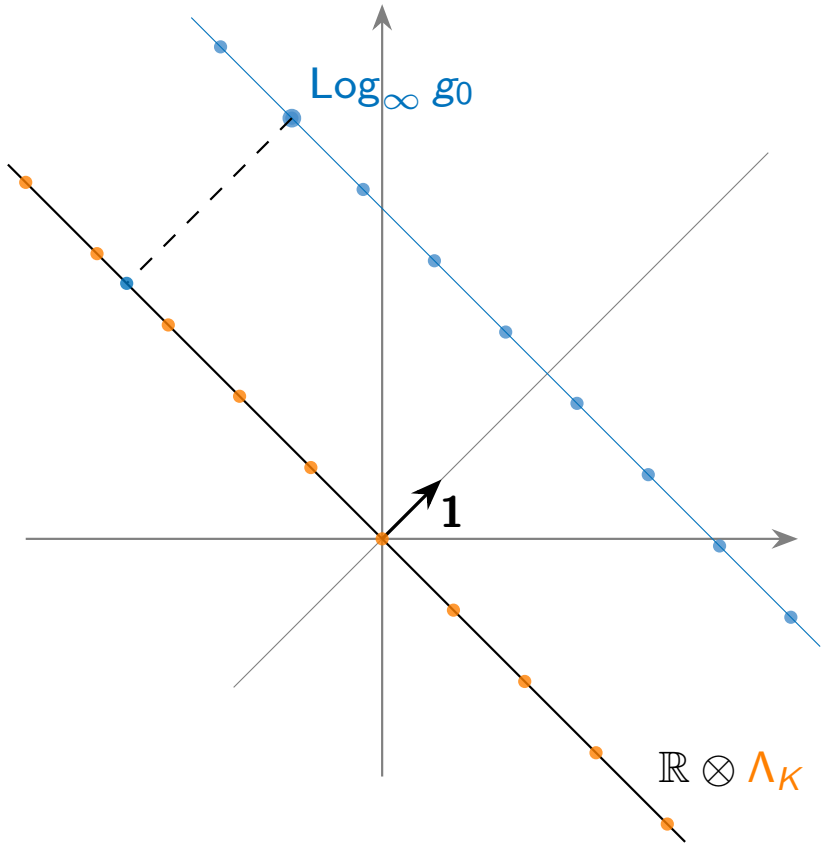


Folklore: generator reduction

Let $\mathfrak{b}$ a principal ideal challenge, given as $\langle g_0 \rangle = \mathfrak{b}$.

Shortest generator: $g = u^{-1} \cdot g_0$, $\mathrm{Log}_\infty g \in \mathrm{Log}_\infty g_0 + \Lambda_K$.

1. Project $\mathrm{Log}_\infty g_0$ into $\mathbb{R} \otimes \Lambda_K$.
2. Find the closest $\mathrm{Log}_\infty u \in \Lambda_K$.
3. Output g_0/u.

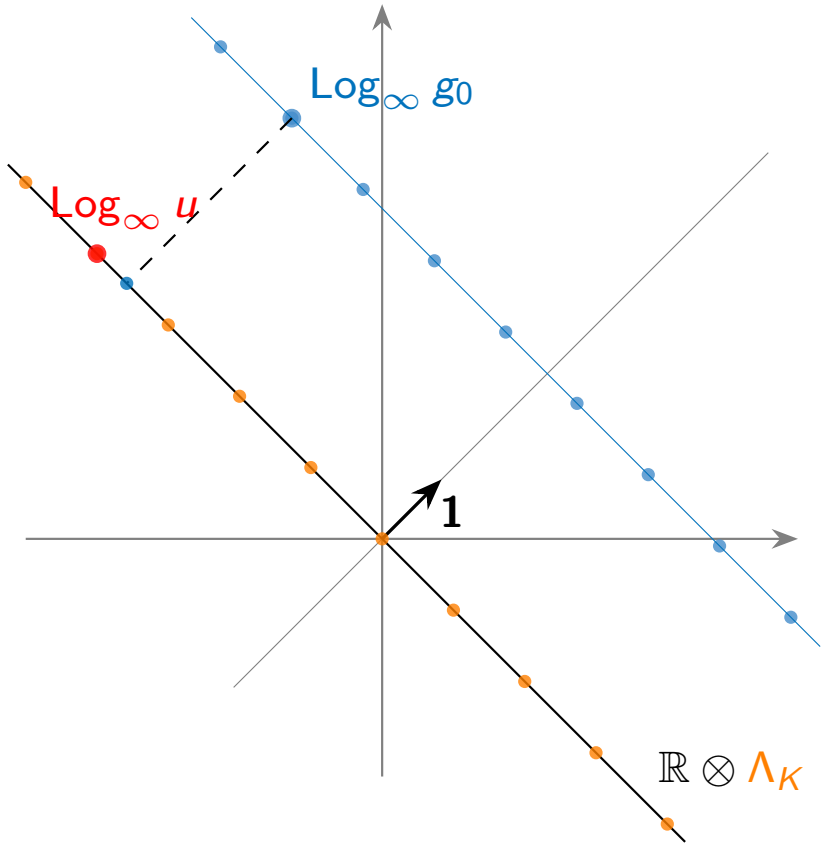


Folklore: generator reduction

Let $\mathfrak{b}$ a principal ideal challenge, given as $\langle g_0 \rangle = \mathfrak{b}$.

Shortest generator: $g = u^{-1} \cdot g_0$, $\mathrm{Log}_\infty g \in \mathrm{Log}_\infty g_0 + \Lambda_K$.

1. Project $\mathrm{Log}_\infty g_0$ into $\mathbb{R} \otimes \Lambda_K$.
2. Find the closest $\mathrm{Log}_\infty u \in \Lambda_K$.
3. Output g_0/u.

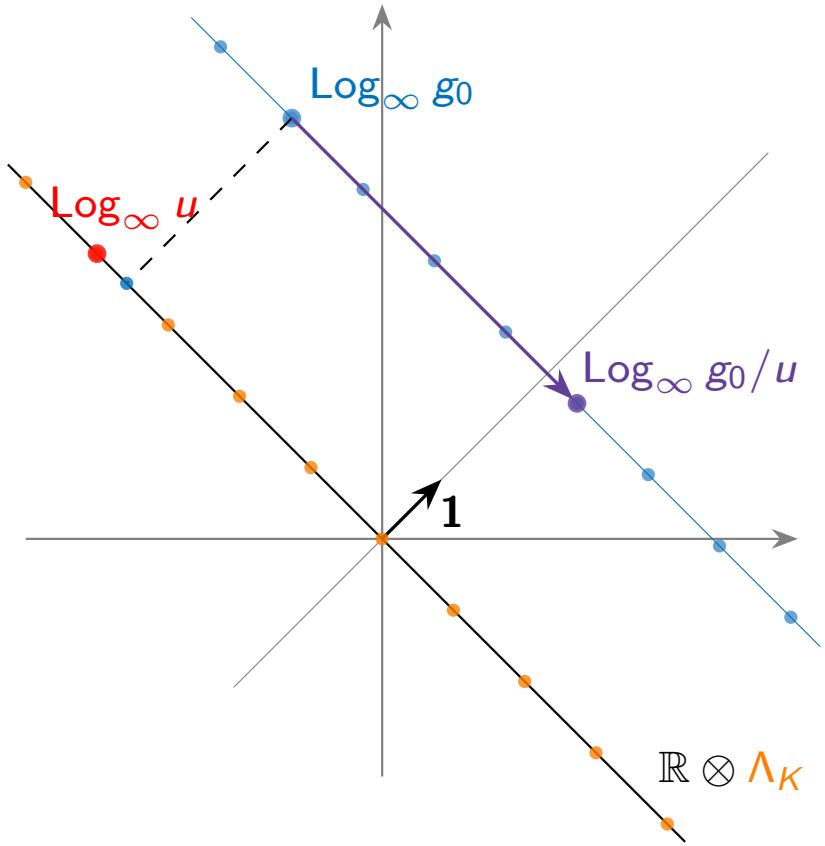


Folklore: generator reduction

Let $\mathfrak{b}$ a principal ideal challenge, given as $\langle g_0 \rangle = \mathfrak{b}$.

Shortest generator: $g = u^{-1} \cdot g_0$, $\mathrm{Log}_\infty g \in \mathrm{Log}_\infty g_0 + \Lambda_K$.

1. Project $\mathrm{Log}_\infty g_0$ into $\mathbb{R} \otimes \Lambda_K$.
2. Find the closest $\mathrm{Log}_\infty u \in \Lambda_K$.
3. Output g_0/u.

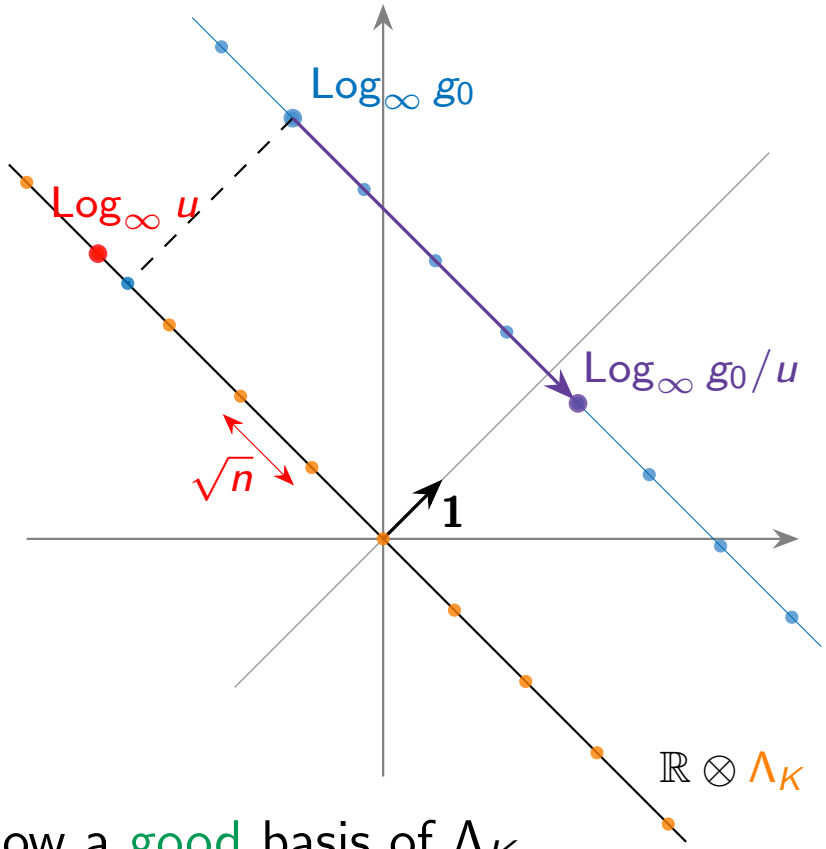


Folklore: generator reduction

Let $\mathfrak{b}$ a principal ideal challenge, given as $\langle g_0 \rangle = \mathfrak{b}$.

Shortest generator: $g = u^{-1} \cdot g_0$,
$\mathrm{Log}_\infty g \in \mathrm{Log}_\infty g_0 + \Lambda_K$.

1. Project $\mathrm{Log}_\infty g_0$ into $\mathbb{R} \otimes \Lambda_K$.
2. Find the closest $\mathrm{Log}_\infty u \in \Lambda_K$.
3. Output g_0/u.



- [CDPR16] Cyclotomic case: we know a good basis of Λ_K.
  Quantum polynomial time, approximation factor generically $2^{\sqrt{n}}$.

Extension: ClDL and S-units

Let FB $= \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$ a factor base of prime ideals.

Class Group Discrete Logarithm (ClDL) Problem

Write $\mathfrak{b}$ as: $\langle \alpha \rangle = \mathfrak{b} \cdot \prod_{\mathfrak{p}_i \in \mathrm{FB}} \mathfrak{p}_i^{v_i}$ for some $v_i \in \mathbb{Z}$.

S-units with respect to FB

s is a S-unit wrpt. FB iff $\langle s \rangle = \prod_{\mathfrak{p} \in \mathrm{FB}} \mathfrak{p}^{v_{\mathfrak{p}}(s)}$.

General idea [PHS19]: Reduce α by using S-units.

$$\varphi_{\mathsf{phs}}(\alpha) \approx \left(\{\ln|\sigma(\alpha)|\}_{\sigma}, \{-v_{\mathfrak{p}}(\alpha)\}_{\mathfrak{p} \in \mathrm{FB}} \right).$$

- Problem: Non homogeneous description.

A new twisted log-S-unit lattice description

Let FB $= \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$ a factor base of prime ideals.

The Product Formula

For all $\alpha \in K$: (in $\mathbb{Q}$: $1 = |12| \cdot 2^{-2} \cdot 3^{-1}$)

$$1 = \prod_\sigma |\sigma(\alpha)| \cdot \prod_\mathfrak{p} \mathcal{N}(\mathfrak{p})^{-v_\mathfrak{p}(\alpha)}.$$

S-logarithmic embedding

$$\mathrm{Log}_{\infty,\mathrm{FB}}(\alpha) = \left(\{\ln|\sigma(\alpha)|\}_\sigma, \{-v_\mathfrak{p}(\alpha) \cdot \ln \mathcal{N}(\mathfrak{p})\}_{\mathfrak{p}\in\mathrm{FB}} \right).$$

With this new representation ("twisted"):

- s is a S-unit $\iff$ $\mathrm{Log}_{\infty,\mathrm{FB}}(s) \in \mathbf{1}^\perp$.
- Their images form the log-S-unit lattice: $\Lambda_{K,\mathrm{FB}} \subsetneq \mathbf{1}^\perp$ in $\mathbb{R}^{n+k}$.

A new twisted log-S-unit lattice description

Let FB $= \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$ a factor base of prime ideals.

S-units with respect to FB

s is a S-unit wrpt. FB iff: (Product formula still holds on FB)

$$1 = \prod_\sigma |\sigma(s)| \cdot \prod_{\mathfrak{p} \in \mathrm{FB}} \mathcal{N}(\mathfrak{p})^{-v_\mathfrak{p}(s)}.$$

S-logarithmic embedding

$$\mathrm{Log}_{\infty,\mathrm{FB}}(\alpha) = \left(\{\ln|\sigma(\alpha)|\}_\sigma, \{-v_\mathfrak{p}(\alpha) \cdot \ln \mathcal{N}(\mathfrak{p})\}_{\mathfrak{p} \in \mathrm{FB}} \right).$$

With this new representation ("twisted"):

- s is a S-unit $\iff$ $\mathrm{Log}_{\infty,\mathrm{FB}}(s) \in \mathbf{1}^\perp$.
- Their images form the log-S-unit lattice: $\Lambda_{K,\mathrm{FB}} \subsetneq \mathbf{1}^\perp$ in $\mathbb{R}^{n+k}$.

A new twisted log-S-unit lattice description

Let FB $= \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$ a factor base of prime ideals.

S-units with respect to FB

s is a S-unit wrpt. FB iff: (Product formula still holds on FB)

$$1 = \prod_\sigma |\sigma(s)| \cdot \prod_{\mathfrak{p} \in \mathrm{FB}} \mathcal{N}(\mathfrak{p})^{-v_\mathfrak{p}(s)}.$$

S-logarithmic embedding

$$\mathrm{Log}_{\infty,\mathrm{FB}}(\alpha) = \left(\{\ln|\sigma(\alpha)|\}_\sigma, \{-v_\mathfrak{p}(\alpha) \cdot \ln \mathcal{N}(\mathfrak{p})\}_{\mathfrak{p} \in \mathrm{FB}} \right).$$

With this new representation ("twisted"):

- s is a S-unit $\iff$ $\mathrm{Log}_{\infty,\mathrm{FB}}(s) \in \mathbf{1}^\perp$.
- Their images form the log-S-unit lattice: $\Lambda_{K,\mathrm{FB}} \subsetneq \mathbf{1}^\perp$ in $\mathbb{R}^{n+k}$.

A new twisted log-S-unit lattice description

Let FB $= \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$ a factor base of prime ideals.

S-units with respect to FB

s is a S-unit wrpt. FB iff: (Product formula still holds on FB)

$$1 = \prod_\sigma |\sigma(s)| \cdot \prod_{\mathfrak{p} \in \mathrm{FB}} \mathcal{N}(\mathfrak{p})^{-v_\mathfrak{p}(s)}.$$

S-logarithmic embedding

$$\mathrm{Log}_{\infty,\mathrm{FB}}(\alpha) = \left(\{\ln|\sigma(\alpha)|\}_\sigma, \{-v_\mathfrak{p}(\alpha) \cdot \ln \mathcal{N}(\mathfrak{p})\}_{\mathfrak{p} \in \mathrm{FB}} \right).$$

With this new representation ("twisted"):

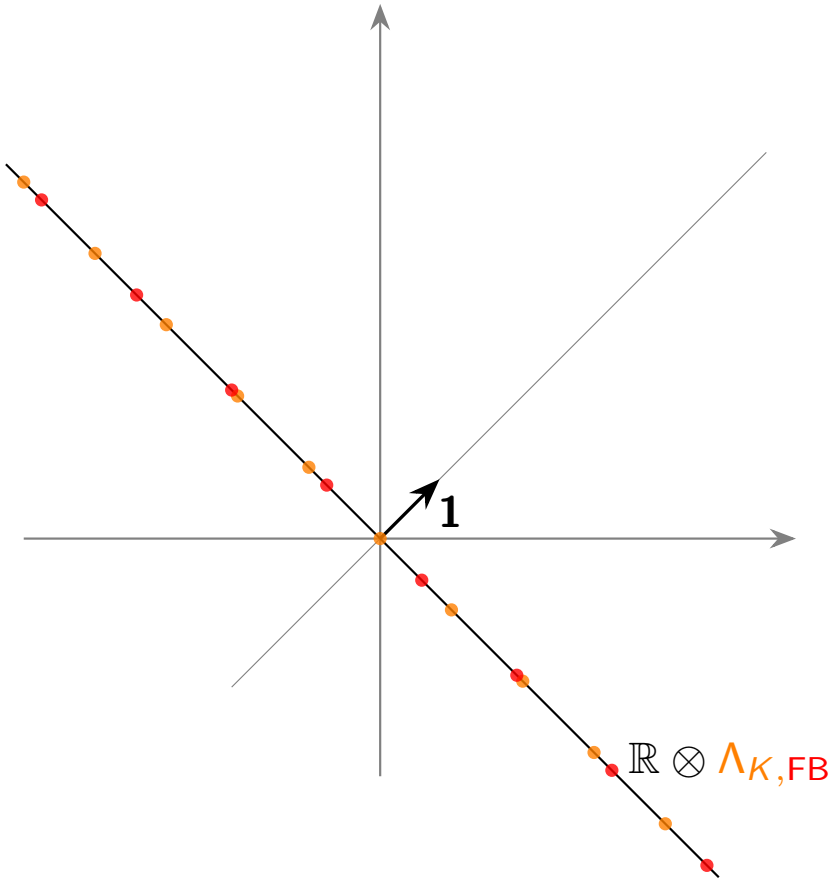
- s is a S-unit $\iff$ $\mathrm{Log}_{\infty,\mathrm{FB}}(s) \in \mathbf{1}^\perp$.
- Their images form the log-S-unit lattice: $\Lambda_{K,\mathrm{FB}} \subsetneq \mathbf{1}^\perp$ in $\mathbb{R}^{n+k}$.

Our CIDL reduction algorithm

Let $\mathfrak{b}$ any ideal challenge, as $\langle \alpha_0 \rangle = \mathfrak{b} \cdot \prod_{\mathfrak{p} \in \mathsf{FB}} \mathfrak{p}^{v_\mathfrak{p}}$. *(CIDL solution)*

Shortest CIDL: $\alpha = s^{-1} \cdot \alpha_0$,
$\mathrm{Log}_{\infty,\mathsf{FB}}\, \alpha \in \mathrm{Log}_{\infty,\mathsf{FB}}\, \alpha_0 + \Lambda_{K,\mathsf{FB}}$.

1. Project $\mathrm{Log}_{\infty,\mathsf{FB}}\, \alpha_0$ into $\mathbf{1}^\perp$.
2. Find closest $\mathrm{Log}_{\infty,\mathsf{FB}}\, s \in \Lambda_{K,\mathsf{FB}}$.
3. Output α_0/s.

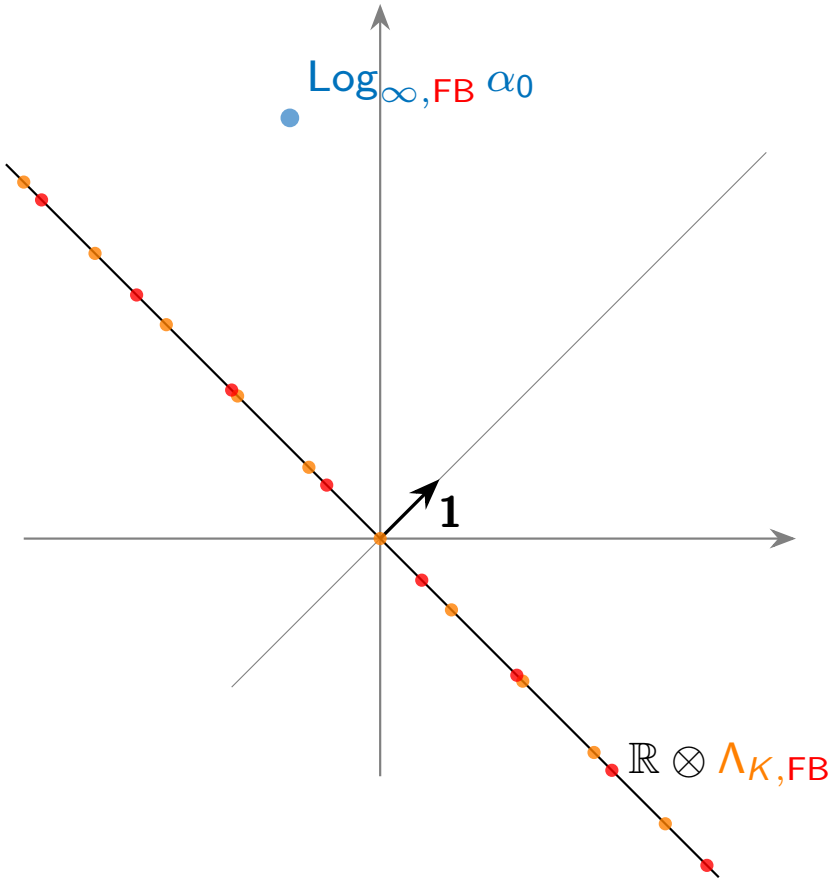


Our CIDL reduction algorithm

Let $\mathfrak{b}$ any ideal challenge, as $\langle \alpha_0 \rangle = \mathfrak{b} \cdot \prod_{\mathfrak{p} \in \mathrm{FB}} \mathfrak{p}^{v_\mathfrak{p}}$. *(CIDL solution)*

Shortest CIDL: $\alpha = s^{-1} \cdot \alpha_0$,
$\mathrm{Log}_{\infty,\mathrm{FB}}\, \alpha \in \mathrm{Log}_{\infty,\mathrm{FB}}\, \alpha_0 + \Lambda_{K,\mathrm{FB}}$.

1. Project $\mathrm{Log}_{\infty,\mathrm{FB}}\, \alpha_0$ into $\mathbf{1}^\perp$.
2. Find closest $\mathrm{Log}_{\infty,\mathrm{FB}}\, s \in \Lambda_{K,\mathrm{FB}}$.
3. Output α_0/s.

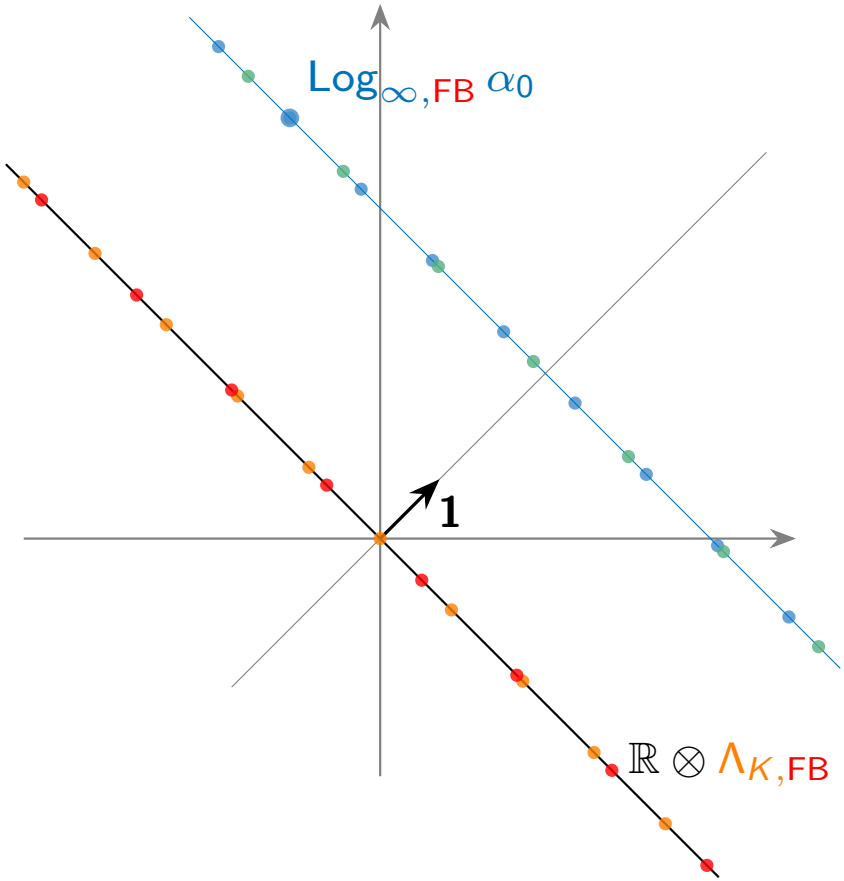


Our CIDL reduction algorithm

Let $\mathfrak{b}$ any ideal challenge, as $\langle \alpha_0 \rangle = \mathfrak{b} \cdot \prod_{\mathfrak{p} \in \mathsf{FB}} \mathfrak{p}^{v_\mathfrak{p}}$. *(CIDL solution)*

Shortest CIDL: $\alpha = s^{-1} \cdot \alpha_0$,
$\mathsf{Log}_{\infty,\mathsf{FB}}\, \alpha \in \mathsf{Log}_{\infty,\mathsf{FB}}\, \alpha_0 + \Lambda_{K,\mathsf{FB}}$.

1. Project $\mathsf{Log}_{\infty,\mathsf{FB}}\, \alpha_0$ into $\mathbf{1}^\perp$.
2. Find closest $\mathsf{Log}_{\infty,\mathsf{FB}}\, s \in \Lambda_{K,\mathsf{FB}}$.
3. Output α_0/s.

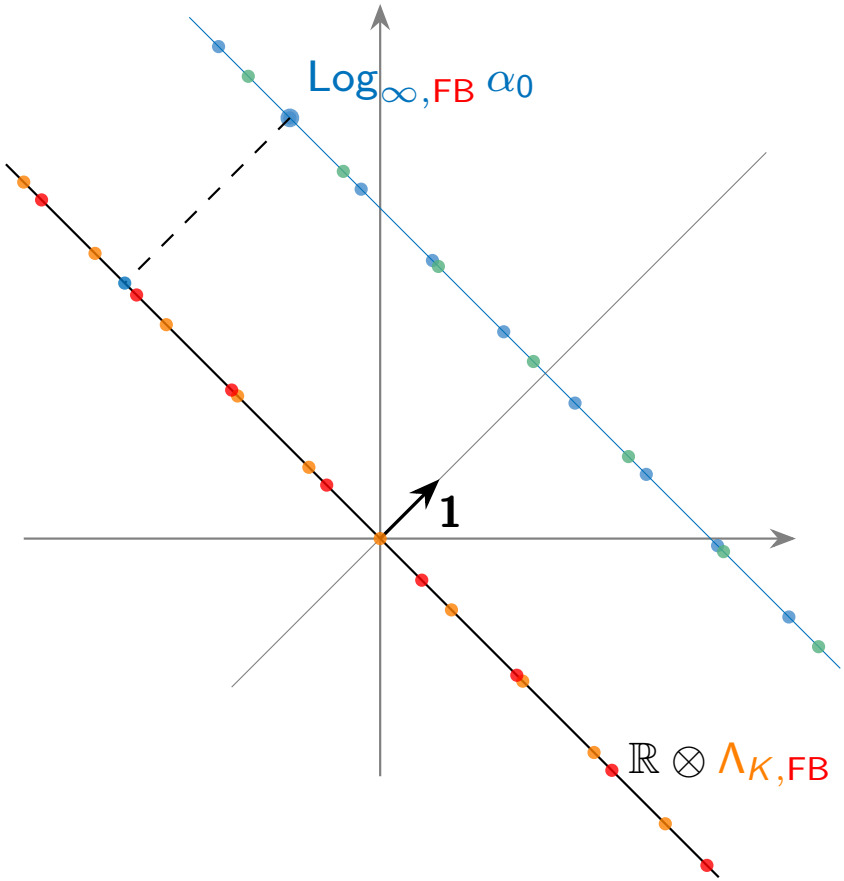


Our CIDL reduction algorithm

Let $\mathfrak{b}$ any ideal challenge, as $\langle \alpha_0 \rangle = \mathfrak{b} \cdot \prod_{\mathfrak{p} \in \mathsf{FB}} \mathfrak{p}^{v_\mathfrak{p}}$. *(CIDL solution)*

Shortest CIDL: $\alpha = s^{-1} \cdot \alpha_0$,
$\mathsf{Log}_{\infty,\mathsf{FB}}\, \alpha \in \mathsf{Log}_{\infty,\mathsf{FB}}\, \alpha_0 + \Lambda_{K,\mathsf{FB}}$.

1. Project $\mathsf{Log}_{\infty,\mathsf{FB}}\, \alpha_0$ into $\mathbf{1}^\perp$.
2. Find closest $\mathsf{Log}_{\infty,\mathsf{FB}}\, s \in \Lambda_{K,\mathsf{FB}}$.
3. Output α_0/s.

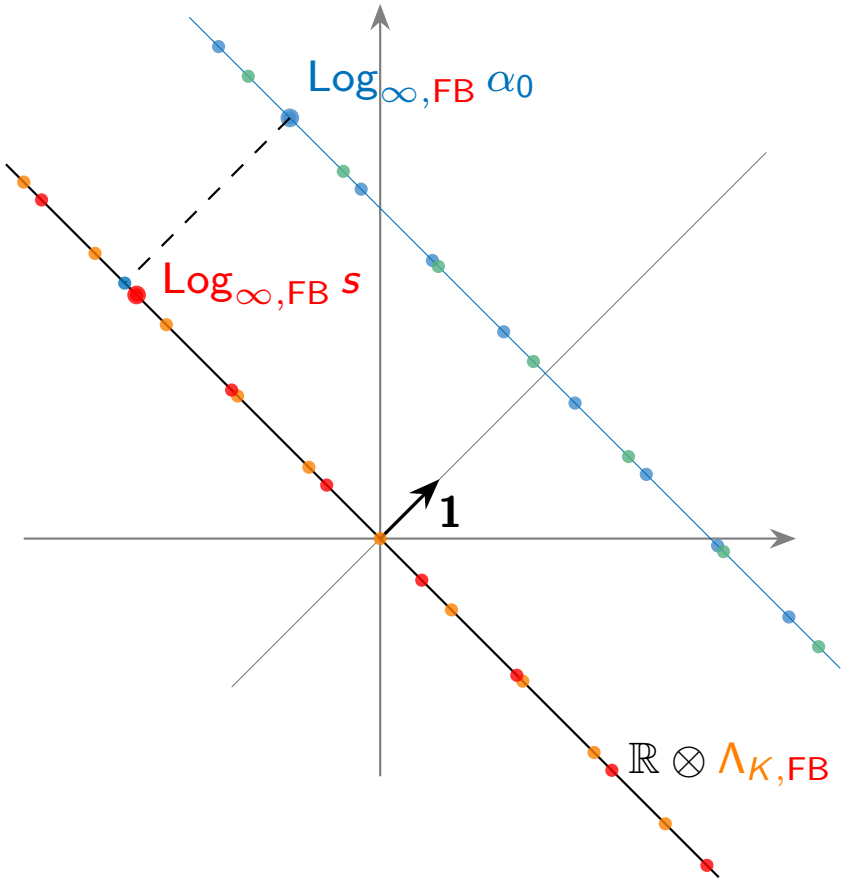


Our CIDL reduction algorithm

Let $\mathfrak{b}$ any ideal challenge, as $\langle \alpha_0 \rangle = \mathfrak{b} \cdot \prod_{\mathfrak{p} \in \mathsf{FB}} \mathfrak{p}^{v_\mathfrak{p}}$. *(CIDL solution)*

Shortest CIDL: $\alpha = s^{-1} \cdot \alpha_0$,
$\mathrm{Log}_{\infty,\mathsf{FB}}\, \alpha \in \mathrm{Log}_{\infty,\mathsf{FB}}\, \alpha_0 + \Lambda_{K,\mathsf{FB}}$.

1. Project $\mathrm{Log}_{\infty,\mathsf{FB}}\, \alpha_0$ into $\mathbf{1}^\perp$.
2. Find closest $\mathrm{Log}_{\infty,\mathsf{FB}}\, s \in \Lambda_{K,\mathsf{FB}}$.
3. Output α_0/s.

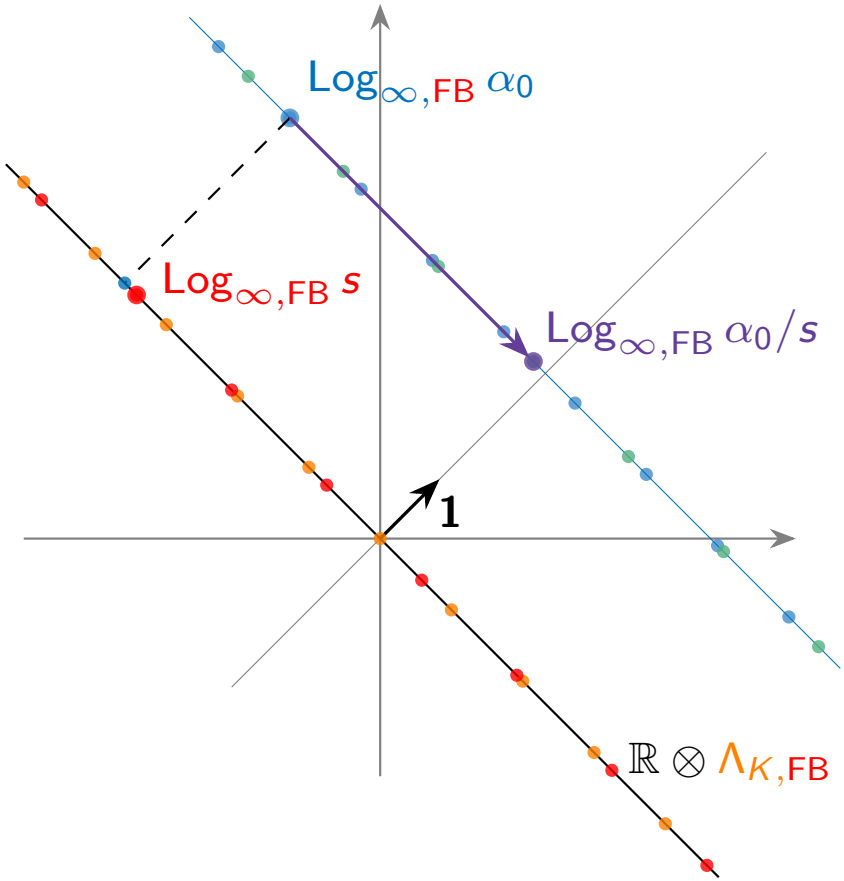


Our CIDL reduction algorithm

Let $\mathfrak{b}$ any ideal challenge, as $\langle \alpha_0 \rangle = \mathfrak{b} \cdot \prod_{\mathfrak{p} \in \mathsf{FB}} \mathfrak{p}^{v_\mathfrak{p}}$. *(CIDL solution)*

Shortest CIDL: $\alpha = s^{-1} \cdot \alpha_0$,
$\mathrm{Log}_{\infty,\mathsf{FB}}\, \alpha \in \mathrm{Log}_{\infty,\mathsf{FB}}\, \alpha_0 + \Lambda_{K,\mathsf{FB}}$.

1. Project $\mathrm{Log}_{\infty,\mathsf{FB}}\, \alpha_0$ into $\mathbf{1}^\perp$.
2. Find closest $\mathrm{Log}_{\infty,\mathsf{FB}}\, s \in \Lambda_{K,\mathsf{FB}}$.
3. Output α_0/s.

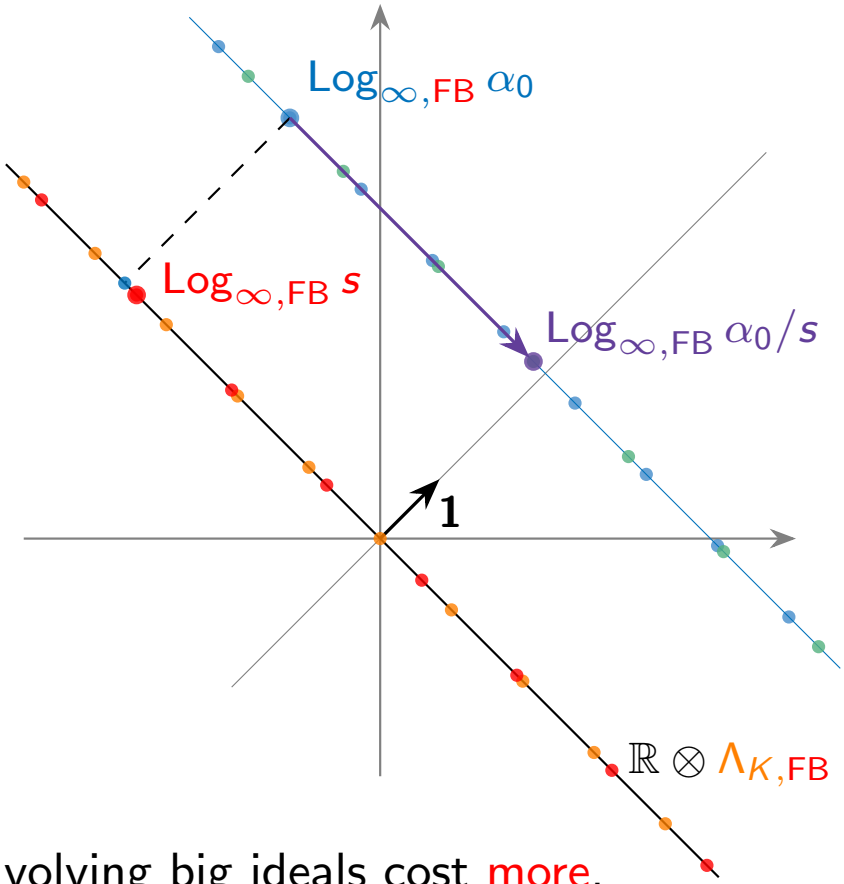


Our CIDL reduction algorithm

Let $\mathfrak{b}$ any ideal challenge, as $\langle \alpha_0 \rangle = \mathfrak{b} \cdot \prod_{\mathfrak{p} \in \mathrm{FB}} \mathfrak{p}^{v_\mathfrak{p}}$. *(CIDL solution)*

Shortest CIDL: $\alpha = s^{-1} \cdot \alpha_0$,
$\mathrm{Log}_{\infty,\mathrm{FB}}\, \alpha \in \mathrm{Log}_{\infty,\mathrm{FB}}\, \alpha_0 + \Lambda_{K,\mathrm{FB}}$.

1. Project $\mathrm{Log}_{\infty,\mathrm{FB}}\, \alpha_0$ into $\mathbf{1}^\perp$.
2. Find closest $\mathrm{Log}_{\infty,\mathrm{FB}}\, s \in \Lambda_{K,\mathrm{FB}}$.
3. Output α_0/s.



- Better chosen S-unit combination: involving big ideals cost more.
  Must guarantee $v_\mathfrak{p}(\alpha) \geq 0$: drift projection in $\mathbf{1}^\perp$, dichotomic strategy.

Today's à la carte

1. Historical timeline
2. A twisted description of the log-S-unit lattice
   - Units: reducing Principal Ideal Generators
   - S-units: reducing Class group Discrete Logarithms
   - Using the Product Formula
3. Experimental results
   - Log-S-unit lattice geometry
   - Ideal-SVP approximation factors
4. What's next ?

Quality estimators

Tricky to evaluate the "quality" of a basis:

- Use several criteria to quantify "short" and "orthogonal"

1. Root-Hermite factor: *(SVP-like problems)*
2. Orthogonality defect (normalized): *(CVP-like problems)*
3. Vector basis angles (min, average): *($\sim$ Random results ?)*
4. Plot Gram-Schmidt log norms.

Quality estimators

Tricky to evaluate the "quality" of a basis:

- Use several criteria to quantify "short" and "orthogonal"

1. Root-Hermite factor: *(SVP-like problems)*

$$\delta_0^d(B_L) = \frac{\|\mathbf{b}_1\|}{\mathrm{Vol}^{1/d} L}.$$

2. Orthogonality defect (normalized): *(CVP-like problems)*
3. Vector basis angles (min, average): *(∼ Random results ?)*
4. Plot Gram-Schmidt log norms.

Quality estimators

Tricky to evaluate the "quality" of a basis:

- Use several criteria to quantify "short" and "orthogonal"

1. Root-Hermite factor: *(SVP-like problems)*
2. Orthogonality defect (normalized): *(CVP-like problems)*

$$\delta^d(B_L) = \frac{\prod_i \|\mathbf{b}_i\|}{\mathrm{Vol}\, L}.$$

3. Vector basis angles (min, average): *($\sim$ Random results ?)*
4. Plot Gram-Schmidt log norms.

Quality estimators

Tricky to evaluate the "quality" of a basis:

- Use several criteria to quantify "short" and "orthogonal"

1. Root-Hermite factor: *(SVP-like problems)*
2. Orthogonality defect (normalized): *(CVP-like problems)*
3. Vector basis angles (min, average): *($\sim$ Random results ?)*

$$\min\{\theta_{ij}, \pi - \theta_{ij}\}, \quad \text{for } \theta_{ij} = \frac{\arccos\langle \mathbf{b}_i, \mathbf{b}_j \rangle}{\|\mathbf{b}_i\| \|\mathbf{b}_j\|}.$$

4. Plot Gram-Schmidt log norms.

Quality estimators

Tricky to evaluate the "quality" of a basis:

- Use several criteria to quantify "short" and "orthogonal"

1. Root-Hermite factor: *(SVP-like problems)*
2. Orthogonality defect (normalized): *(CVP-like problems)*
3. Vector basis angles (min, average): *($\sim$ Random results ?)*
4. Plot Gram-Schmidt log norms.

Quality estimators

Tricky to evaluate the "quality" of a basis:

- Use several criteria to quantify "short" and "orthogonal"

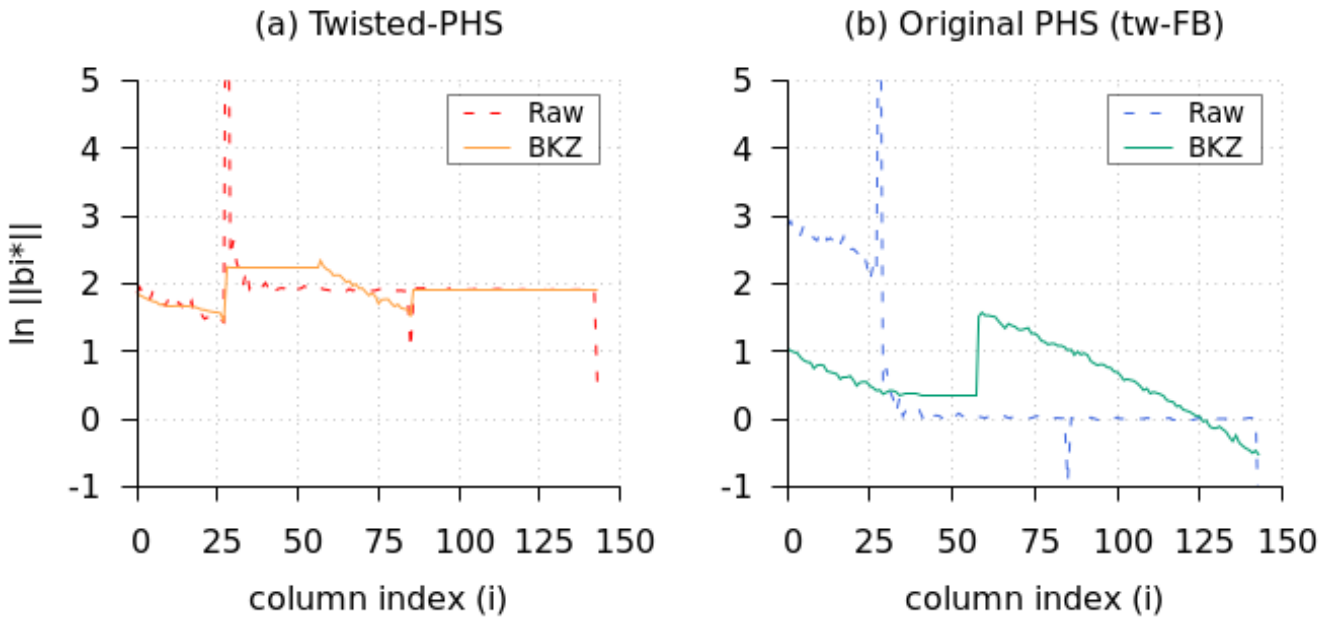
1. Root-Hermite factor: *(SVP-like problems)*
2. Orthogonality defect (normalized): *(CVP-like problems)*
3. Vector basis angles (min, average): *(∼ Random results ?)*
4. Plot Gram-Schmidt log norms.

Observations Twisted-PHS/PHS

- Better (absolute) values in the twisted case.
- Much smaller gap before/after some BKZ reduction.

Twisted log-S-unit basis quality

Seems very orthogonal ! Experimental observation, e.g. for $\mathbb{Q}(\zeta_{59})$:



1. Flatter Gram-Schmidt log norms curve
2. Fewer differences before/after BKZ
3. BKZ Timings: Tw-PHS O(10s) / PHS O(10 min) PHS *(same* FB*)*

▶ Can we just use some naive CVP oracle in the twisted case ?

Sledgehammer argument

Approximation factors: grows extremely slowly with the degree.

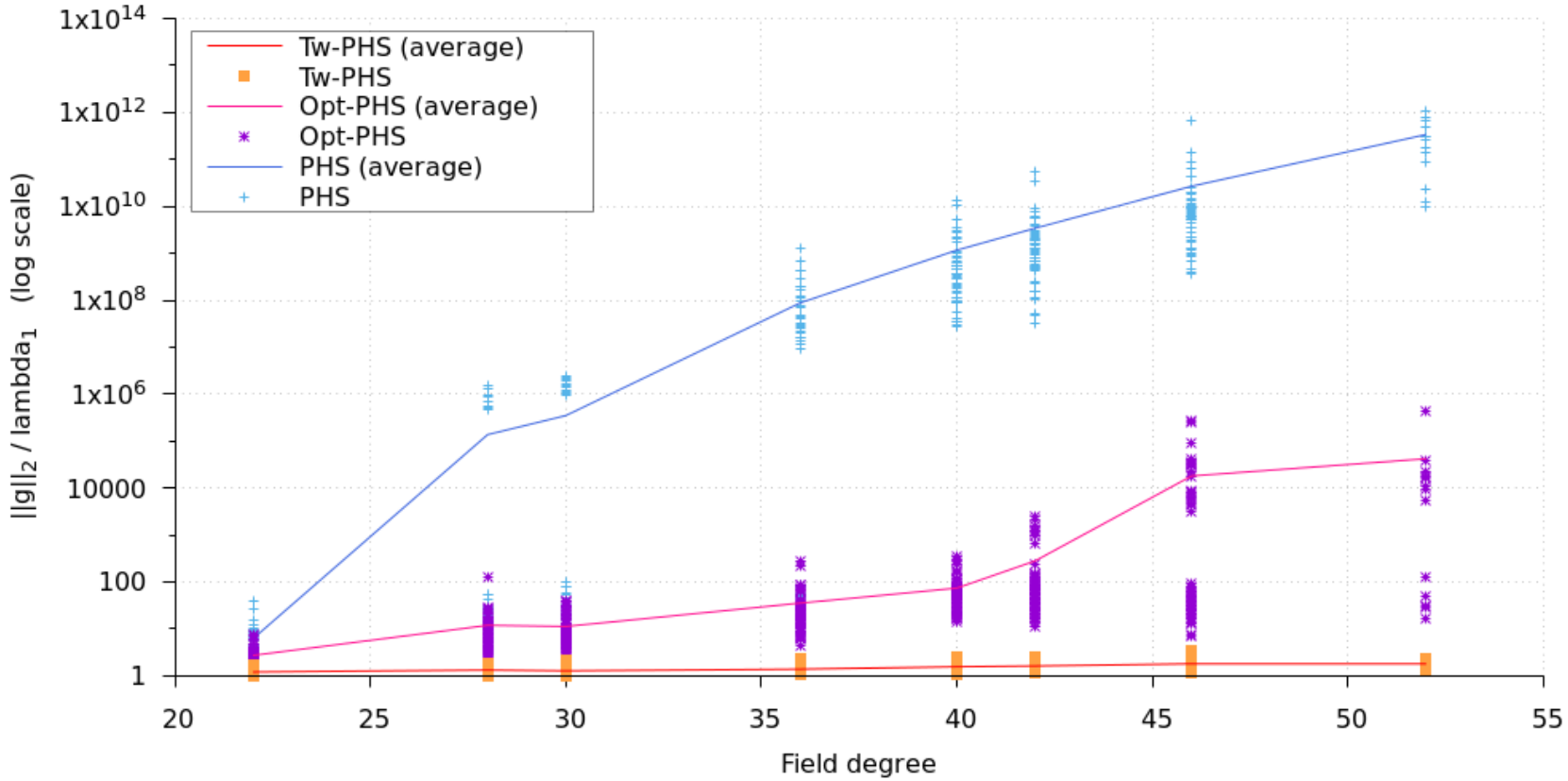


Figure: prime conductor cyclotomic fields, avg. over 50 *ideals of* 100*-bits prime norm.*

Today's à la carte

1. Historical timeline
2. A twisted description of the log-S-unit lattice
   - Units: reducing Principal Ideal Generators
   - S-units: reducing Class group Discrete Logarithms
   - Using the Product Formula
3. Experimental results
   - Log-S-unit lattice geometry
   - Ideal-SVP approximation factors
4. What's next ?

On-going work

1. Theoretic proofs:
   - Orthogonality of the (twisted) log-S-unit lattice for cyclotomic fields,
   - Tighter bounds on Tw-PHS approximation factor ?
2. Extended experiments where S-unit computations are "easier":
   - Multiquadratic/multicubic fields,
   - Cyclotomic fields using (sthg related to) the Stickelberger lattice.
3. Module-SVP: apply similar homogeneization ideas to [LPSW19][2].

[2] [LPSW19] An LLL Algorithm for Module Lattices

On-going work

1. Theoretic proofs:
   - Orthogonality of the (twisted) log-S-unit lattice for cyclotomic fields,
   - Tighter bounds on Tw-PHS approximation factor ?
2. Extended experiments where S-unit computations are "easier":
   - Multiquadratic/multicubic fields,
   - Cyclotomic fields using (sthg related to) the Stickelberger lattice.
3. Module-SVP: apply similar homogeneization ideas to [LPSW19][2].

Questions ?

[2] [LPSW19] An LLL Algorithm for Module Lattices