Log-S-unit lattices using Explicit Stickelberger Generators to solve Approx Ideal-SVP

Olivier Bernard[1,2] Andrea Lesavourey[1] Tuong-Huy Nguyen[1,3]
Adeline Roux-Langlois[1]

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

[2]Thales, Gennevilliers, Laboratoire CHiffre

[3]DGA Maîtrise de l'Information, Bruz

LFANT's Seminar, Bordeaux

7th December 2021

Today's à la carte

Today's à la carte

Yet another slide on SVP

Definition (Lattice)

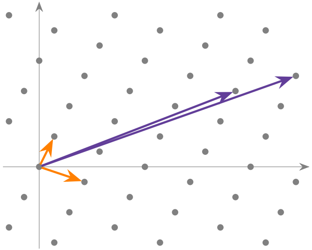
A lattice L is a discrete subgroup of $\mathbb{R}^n$ (say a "$\mathbb{Z}$-vector space").

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

▶ Is the algebraic structure harmful for cryptography ? *(rely on Module-SVP)*

Yet another slide on SVP

Definition (Lattice)

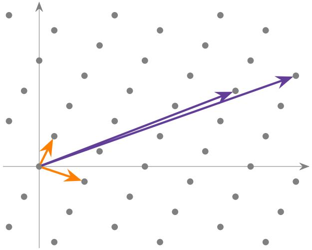
A lattice L is a discrete subgroup of $\mathbb{R}^n$ (say a "$\mathbb{Z}$-vector space").

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

▶ Is the algebraic structure harmful for cryptography ? *(rely on Module-SVP)*

Yet another slide on SVP

Definition (Lattice)

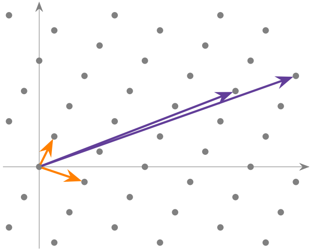
A lattice L is a discrete subgroup of $\mathbb{R}^n$ (say a "$\mathbb{Z}$-vector space").

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 $v \in L$:

$$\|v\|_2 = \lambda_1(L).$$

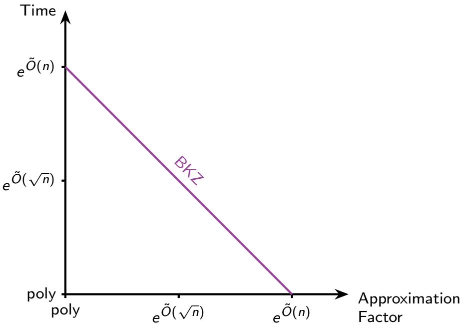


Structured variants: Ideal, Module

▶ Is the algebraic structure harmful for cryptography ? *(rely on Module-SVP)*

Algebraic cryptanalysis of Ideal-Svp

Quantum computer: computes units, class groups, $\mathcal{S}$-units in poly time !
Picture for Ideal-Svp: in cyclotomic fields $K_m = \mathbb{Q}(\zeta_m)$, $m \not\equiv 2 \mod 4$.

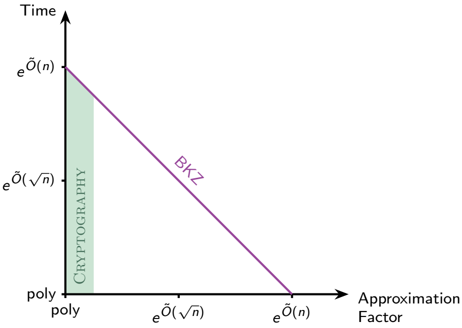


1. Schnorr's hierarchy (unstructured case)
2. CDW algorithm [CDW21]: uses short Stickelberger relations.
3. PHS and Twisted-PHS [PHS19,BR20]: use $\mathcal{S}$-units.

- How "devastating (!?)" would be so-called $\mathcal{S}$-unit attacks in practice ?
(Given a quantum computer, say)

Algebraic cryptanalysis of Ideal-SVP

Quantum computer: computes units, class groups, $\mathcal{S}$-units in poly time !
Picture for Ideal-Svp: in cyclotomic fields $K_m = \mathbb{Q}(\zeta_m), m \not\equiv 2 \mod 4$.

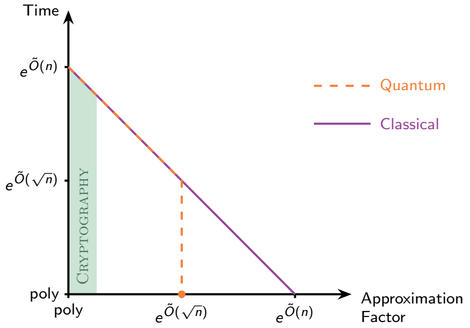


1. Schnorr's hierarchy (unstructured case)
2. CDW algorithm [CDW21]: uses short Stickelberger relations.
3. PHS and Twisted-PHS [PHS19,BR20]: use $\mathcal{S}$-units.

- How "devastating (!?)" would be so-called $\mathcal{S}$-unit attacks in practice ? (Given a quantum computer, say)

Algebraic cryptanalysis of Ideal-SVP

Quantum computer: computes units, class groups, $\mathcal{S}$-units in poly time !
Picture for Ideal-Svp: in cyclotomic fields $K_m = \mathbb{Q}(\zeta_m), m \not\equiv 2 \mod 4$.

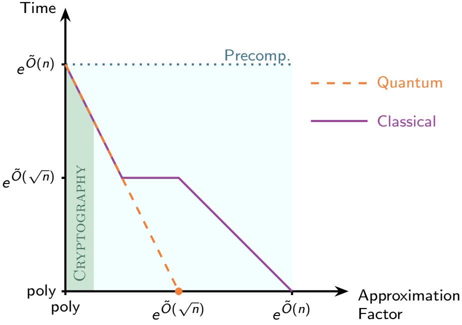


1. Schnorr's hierarchy (unstructured case)
2. CDW algorithm [CDW21]: uses short Stickelberger relations.
3. PHS and Twisted-PHS [PHS19,BR20]: use $\mathcal{S}$-units.

- How "devastating (!?)" would be so-called $\mathcal{S}$-unit attacks in practice ? (Given a quantum computer, say)

Algebraic cryptanalysis of Ideal-SVP

Quantum computer: computes units, class groups, $\mathcal{S}$-units in poly time !
Picture for Ideal-Svp: in cyclotomic fields $K_m = \mathbb{Q}(\zeta_m)$, $m \not\equiv 2 \mod 4$.

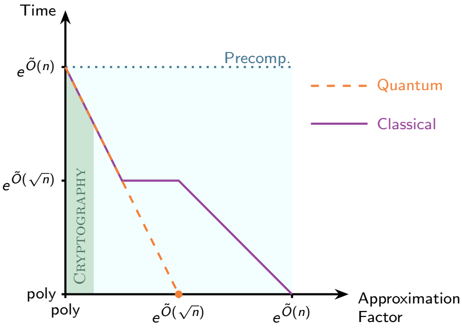


1. Schnorr's hierarchy (unstructured case)
2. CDW algorithm [CDW21]: uses short Stickelberger relations.
3. PHS and Twisted-PHS [PHS19,BR20]: use $\mathcal{S}$-units.

- How "devastating (!?)" would be so-called $\mathcal{S}$-unit attacks in practice ? (Given a quantum computer, say)

Algebraic cryptanalysis of Ideal-SVP

Quantum computer: computes units, class groups, $\mathcal{S}$-units in poly time !
Picture for Ideal-Svp: in cyclotomic fields $K_m = \mathbb{Q}(\zeta_m)$, $m \not\equiv 2 \mod 4$.



1. Schnorr's hierarchy (unstructured case)
2. CDW algorithm [CDW21]: uses short Stickelberger relations.
3. PHS and Twisted-PHS [PHS19,BR20]: use $\mathcal{S}$-units.

- How "devastating (!?)" would be so-called $\mathcal{S}$-unit attacks in practice ? (Given a quantum computer, say)

Today's à la carte

PIP and SGP vs. CLDL and S-CLDL: towards id-SVP

Let K be a number field, $\mathfrak{b}$ any fractional ideal.
$\mathcal{S} = \mathcal{S}_\infty \cup \{\mathfrak{p}_1, \dots, \mathfrak{p}_k\}$ a factor base of prime ideals.

Principal Ideal Problem (PIP)

Given $\mathfrak{b}$, find (if it exists) g st. $\langle g \rangle = \mathfrak{b}$.

Shortest Generator Problem (SGP)

Given $\mathfrak{b} = \langle g \rangle$, find the shortest g_0 st. $\mathfrak{b} = \langle g_0 \rangle$.

- Use units.

PIP and SGP vs. ClDL and S-ClDL: towards id-SVP

Let K be a number field, $\mathfrak{b}$ any fractional ideal.
$\mathcal{S} = \mathcal{S}_\infty \cup \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$ a factor base of prime ideals.

Class Group Discrete Logarithm (ClDL) Problem

Given $\mathfrak{b}$, find (if it exists) α, $v_i \in \mathbb{Z}$ such that: $\langle \alpha \rangle = \mathfrak{b} \cdot \prod_{\mathfrak{p}_i \in \mathcal{S}} \mathfrak{p}_i^{v_i}$.

Shortest Class Group Discrete Logarithm Problem (S-ClDL)

From a ClDL solution, find the shortest α_0 such that:

$$\langle \alpha_0 \rangle = \mathfrak{b} \cdot \prod_{\mathfrak{p} \in \mathcal{S}} \mathfrak{p}_i^{v_i}, \quad v_i \in \mathbb{Z}_+.$$

- Use $\mathcal{S}$-units.

The log-unit lattice

Let K be a number field of degree n,
$\mathcal{S}_\infty = \{\sigma : K \hookrightarrow \mathbb{C}\}$ its embeddings into $\mathbb{C}$.

Algebraic unit

An algebraic integer $u \in \mathcal{O}_K$ is a unit iff:

$$1 = |\mathcal{N}(u)| \quad \left(= \prod_{\sigma\in\mathcal{S}_\infty} |\sigma(u)|\right).$$

Logarithmic embedding

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

Hence:

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

The log-unit lattice

Let K be a number field of degree n,
$\mathcal{S}_\infty = \{\sigma : K \hookrightarrow \mathbb{C}\}$ its embeddings into $\mathbb{C}$.

Algebraic unit

An algebraic integer $u \in \mathcal{O}_K$ is a unit iff:

$$1 = |\mathcal{N}(u)| \quad \left(= \prod_{\sigma\in\mathcal{S}_\infty} |\sigma(u)|\right).$$

Logarithmic embedding

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

Hence:

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

The log-unit lattice

Let K be a number field of degree n,
$\mathcal{S}_\infty = \{\sigma : K \hookrightarrow \mathbb{C}\}$ its embeddings into $\mathbb{C}$.

Algebraic unit

An algebraic integer $u \in \mathcal{O}_K$ is a unit iff:

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

Logarithmic embedding

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

Hence:

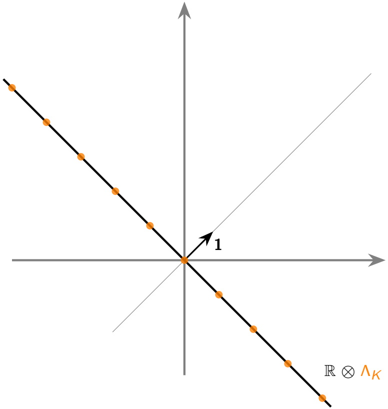
- u is a unit $\iff$ $\mathrm{Log}_{\mathcal{S}_\infty}(u) \in \mathbf{1}^\perp$.
- Their images form the log-unit lattice: $\Lambda_K \subsetneq \mathbf{1}^\perp$.

Folklore: generator reduction

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

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

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

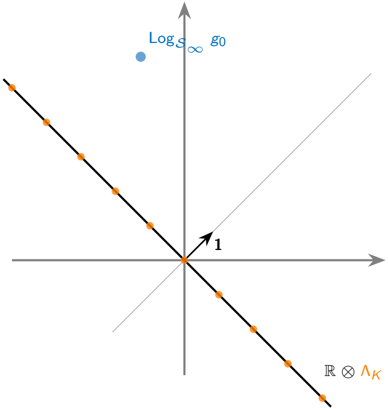


Folklore: generator reduction

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

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

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

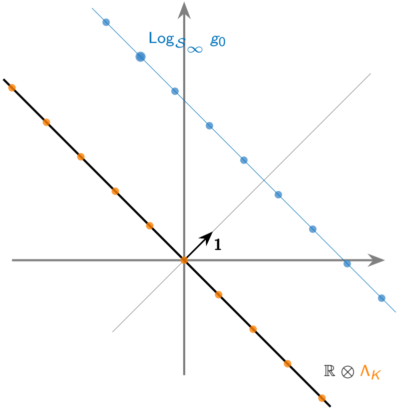


Folklore: generator reduction

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

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

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

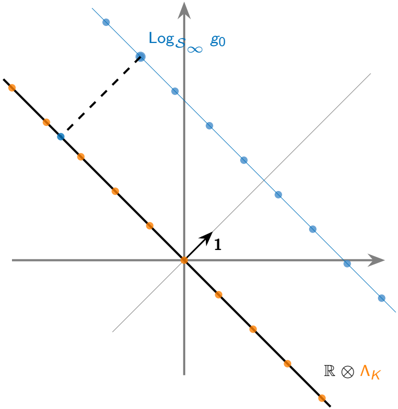


Folklore: generator reduction

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

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

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

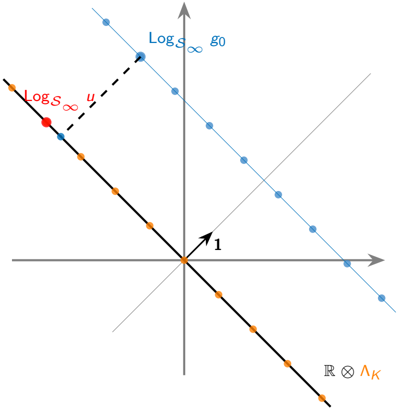


Folklore: generator reduction

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

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

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

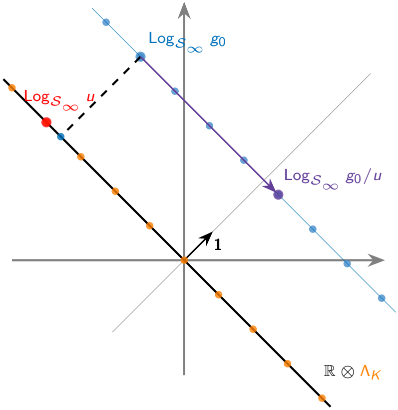


Folklore: generator reduction

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

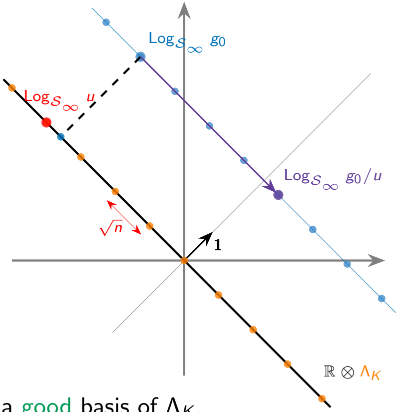
Shortest generator: $g = u^{-1} \cdot g_0$,
$\mathrm{Log}_{\mathcal{S}_\infty}\, g \in \mathrm{Log}_{\mathcal{S}_\infty}\, g_0 + \Lambda_K$.

1. Project $\mathrm{Log}_{\mathcal{S}_\infty}\, g_0$ into $\mathbb{R} \otimes \Lambda_K$.
2. Find the closest $\mathrm{Log}_{\mathcal{S}_\infty}\, u \in \Lambda_K$.
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: $g = u^{-1} \cdot g_0$,
$\mathrm{Log}_{\mathcal{S}_\infty}\ g \in \mathrm{Log}_{\mathcal{S}_\infty}\ g_0 + \Lambda_K$.

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

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

The log-$\mathcal{S}$-unit lattice

Let $\mathcal{S} = \mathcal{S}_\infty \cup \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$ a factor base containing k prime ideals.

$\mathcal{S}$-unit

An algebraic $\mathcal{S}$-integer $u \in \mathcal{O}_{K,\mathcal{S}}$ is a $\mathcal{S}$-unit iff:

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

Logarithmic $\mathcal{S}$-embedding ("twisted" representation)

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

Hence:

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

The log-$\mathcal{S}$-unit lattice

Let $\mathcal{S} = \mathcal{S}_\infty \cup \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$ a factor base containing k prime ideals.

$\mathcal{S}$-unit

An algebraic $\mathcal{S}$-integer $u \in \mathcal{O}_{K,\mathcal{S}}$ is a $\mathcal{S}$-unit iff:

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

Logarithmic $\mathcal{S}$-embedding ("twisted" representation)

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

Hence:

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

The log-$\mathcal{S}$-unit lattice

Let $\mathcal{S} = \mathcal{S}_\infty \cup \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$ a factor base containing k prime ideals.

$\mathcal{S}$-unit

An algebraic $\mathcal{S}$-integer $u \in \mathcal{O}_{K,\mathcal{S}}$ is a $\mathcal{S}$-unit iff:

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

Logarithmic $\mathcal{S}$-embedding ("twisted" representation)

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

Hence:

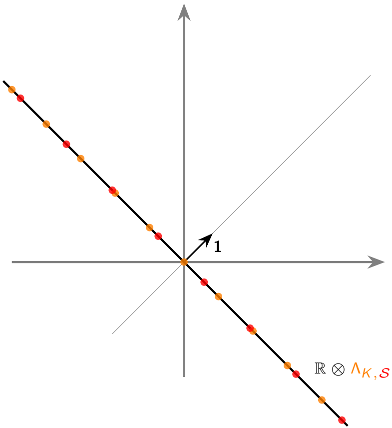
- s is a $\mathcal{S}$-unit $\iff$ $\mathrm{Log}_\mathcal{S}(s) \in \mathbf{1}^\perp$.
- Their images form the log-$\mathcal{S}$-unit lattice: $\Lambda_{K,\mathcal{S}} \subsetneq \mathbf{1}^\perp$ in $\mathbb{R}^{n+k}$.

ClDL reduction algorithm (Twisted-PHS)

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

Shortest ClDL: $\alpha = s^{-1}\cdot\alpha_0$,
$\mathrm{Log}_\mathcal{S}\,\alpha \in \mathrm{Log}_\mathcal{S}\,\alpha_0 + \Lambda_{K,\mathcal{S}}$.

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

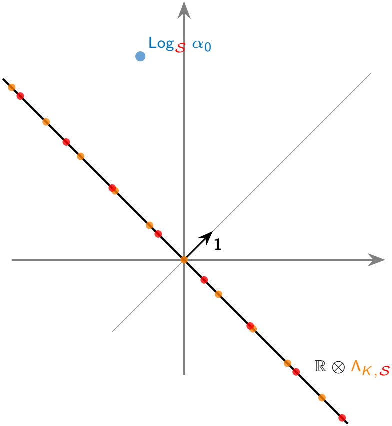


CLDL reduction algorithm (Twisted-PHS)

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

Shortest CLDL: $\alpha = s^{-1} \cdot \alpha_0$,
$\mathrm{Log}_\mathcal{S}\, \alpha \in \mathrm{Log}_\mathcal{S}\, \alpha_0 + \Lambda_{K,\mathcal{S}}$.

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

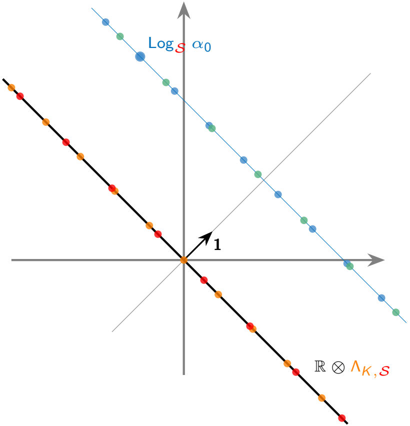


CIDL reduction algorithm (Twisted-PHS)

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

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

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

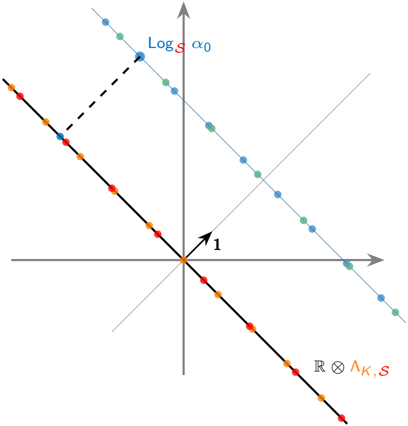


CLDL reduction algorithm (Twisted-PHS)

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

Shortest ClDL: $\alpha = s^{-1}\cdot\alpha_0$,
$\mathrm{Log}_\mathcal{S}\,\alpha \in \mathrm{Log}_\mathcal{S}\,\alpha_0 + \Lambda_{K,\mathcal{S}}$.

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

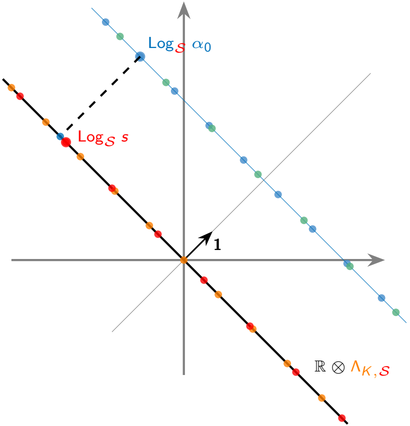


CIDL reduction algorithm (Twisted-PHS)

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

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

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

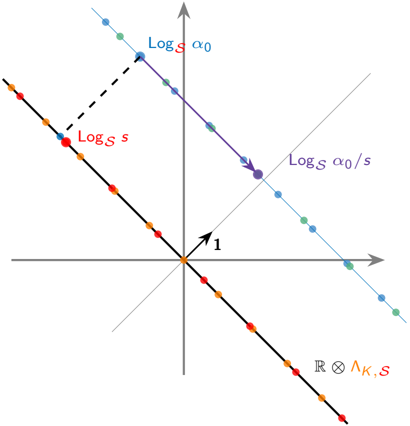


ClDL reduction algorithm (Twisted-PHS)

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

Shortest ClDL: $\alpha = s^{-1} \cdot \alpha_0$,
$\mathrm{Log}_{\mathcal{S}}\, \alpha \in \mathrm{Log}_{\mathcal{S}}\, \alpha_0 + \Lambda_{K,\mathcal{S}}$.

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

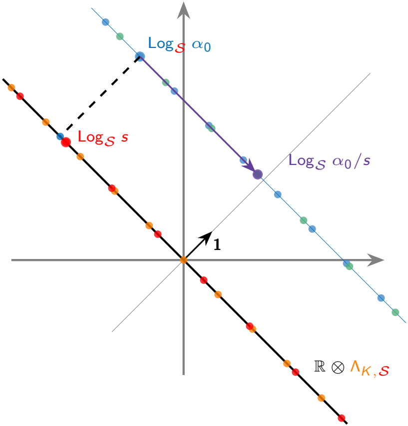


ClDL reduction algorithm (Twisted-PHS)

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

Shortest ClDL: $\alpha = s^{-1} \cdot \alpha_0$,
$\mathrm{Log}_\mathcal{S}\, \alpha \in \mathrm{Log}_\mathcal{S}\, \alpha_0 + \Lambda_{K,\mathcal{S}}$.

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



▶ For Ideal-SVP, must guarantee $v_\mathfrak{p}(\alpha) \geq 0$: drift projection in $\mathbf{1}^\perp$.

Impacts of the chosen logarithmic $\mathcal{S}$-embedding

Logarithmic $\mathcal{S}$-embedding ("twisted" representation)

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

- What is the impact of these $\ln \mathcal{N}(\mathfrak{p})$?

Theoretically: seems not to change much (same proven bounds)

1. Better chosen $\mathcal{S}$-unit combination: involving big ideals costs more.
2. Optimal factor base phenomenon: some $\mathcal{S}$ maximizes the density !

In practice: (small dimensions)

1. much better geometric indicators
2. very small approximation factors

Impacts of the chosen logarithmic $\mathcal{S}$-embedding

Logarithmic $\mathcal{S}$-embedding ("twisted" representation)

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

- What is the impact of these $\ln\mathcal{N}(\mathfrak{p})$?

Theoretically: seems not to change much (same proven bounds)

1. Better chosen $\mathcal{S}$-unit combination: involving big ideals costs more.
2. Optimal factor base phenomenon: some $\mathcal{S}$ maximizes the density !

In practice: (small dimensions)

1. much better geometric indicators
2. very small approximation factors

Impacts of the chosen logarithmic $\mathcal{S}$-embedding

Logarithmic $\mathcal{S}$-embedding ("twisted" representation)

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

- What is the impact of these $\ln \mathcal{N}(\mathfrak{p})$?

Theoretically: seems not to change much (same proven bounds)

1. Better chosen $\mathcal{S}$-unit combination: involving big ideals costs more.
2. Optimal factor base phenomenon: some $\mathcal{S}$ maximizes the density !

In practice: (small dimensions)

1. much better geometric indicators
2. very small approximation factors

Impacts of the chosen logarithmic $\mathcal{S}$-embedding

Logarithmic $\mathcal{S}$-embedding ("twisted" representation)

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

- What is the impact of these $\ln \mathcal{N}(\mathfrak{p})$?

Theoretically: seems not to change much (same proven bounds)

1. Better chosen $\mathcal{S}$-unit combination: involving big ideals costs more.
2. Optimal factor base phenomenon: some $\mathcal{S}$ maximizes the density !

In practice: (small dimensions)

1. much better geometric indicators
2. very small approximation factors

Impacts of the chosen logarithmic $\mathcal{S}$-embedding

Logarithmic $\mathcal{S}$-embedding ("twisted" representation)

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

- What is the impact of these $\ln \mathcal{N}(\mathfrak{p})$?

Theoretically: seems not to change much (same proven bounds)

1. Better chosen $\mathcal{S}$-unit combination: involving big ideals costs more.
2. Optimal factor base phenomenon: some $\mathcal{S}$ maximizes the density !

In practice: (small dimensions)

1. much better geometric indicators
2. very small approximation factors

Impacts of the chosen logarithmic $\mathcal{S}$-embedding

Logarithmic $\mathcal{S}$-embedding ("twisted" representation)

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

- What is the impact of these $\ln \mathcal{N}(\mathfrak{p})$?

Theoretically: seems not to change much (same proven bounds)

1. Better chosen $\mathcal{S}$-unit combination: involving big ideals costs more.
2. Optimal factor base phenomenon: some $\mathcal{S}$ maximizes the density !

In practice: (small dimensions)

1. much better geometric indicators
2. very small approximation factors

Impacts of the chosen logarithmic $\mathcal{S}$-embedding

Logarithmic $\mathcal{S}$-embedding ("twisted" representation)

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

- What is the impact of these $\ln \mathcal{N}(\mathfrak{p})$?

Theoretically: seems not to change much (same proven bounds)

1. Better chosen $\mathcal{S}$-unit combination: involving big ideals costs more.
2. Optimal factor base phenomenon: some $\mathcal{S}$ maximizes the density !

In practice: (small dimensions)

1. much better geometric indicators
2. very small approximation factors

Impacts of the chosen logarithmic $\mathcal{S}$-embedding

Logarithmic $\mathcal{S}$-embedding ("twisted" representation)

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

- What is the impact of these $\ln \mathcal{N}(\mathfrak{p})$?

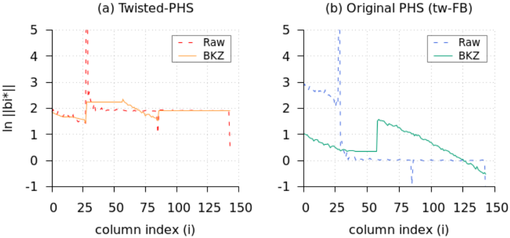
Theoretically: seems not to change much (same proven bounds)

1. Better chosen $\mathcal{S}$-unit combination: involving big ideals costs more.
2. Optimal factor base phenomenon: some $\mathcal{S}$ maximizes the density !

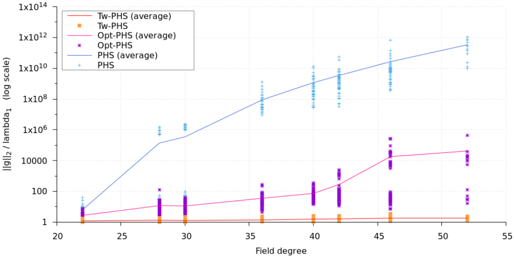
In practice: (small dimensions)

1. much better geometric indicators
2. very small approximation factors

Weights: a graphical praise



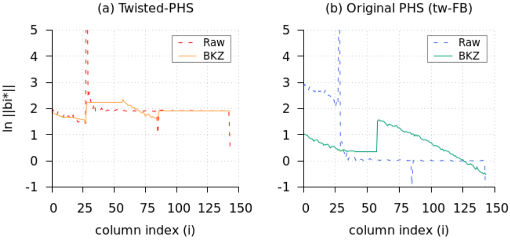
- $K = \mathbb{Q}(\zeta_{59})$, $\mathcal{S} = \{\mathfrak{p} \mid 709, 827\}$
- Log-$\mathcal{S}$-unit Gram-Schmidt log norms

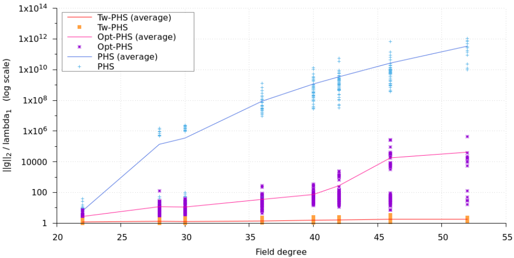


- Fields $\mathbb{Q}(\zeta_p)$, $p \leq 53$
- Exact approx factors

▶ Are these only a "small dimension effect" ?

Weights: a graphical praise





- $K = \mathbb{Q}(\zeta_{59})$,
  $\mathcal{S} = \{\mathfrak{p} \mid 709, 827\}$
- Log-$\mathcal{S}$-unit
  Gram-Schmidt log norms

- Fields $\mathbb{Q}(\zeta_p)$, $p \leq 53$
- Exact approx factors

▶ Are these only a "small dimension effect" ?

Today's à la carte

A quick summary

Let $K_m = \mathbb{Q}(\zeta_m)$, $m \not\equiv 2 \mod 4$, $n = \deg K_m$
$\mathcal{S} = \mathcal{S}_\infty \cup \{\mathfrak{L}_i \mid \ell_i \cdot \mathcal{O}_K;\ \ell_i \equiv 1 \mod m, i \in [\![1, d]\!]\}$ a set of places.

1. Circular units
2. Explicit Stickelberger generators
3. Real $\mathcal{S}^+$-units (that are not units) in K_m^+

Theorem (suppose for the presentation that all $\mathfrak{L}_i$ generate the class group)

These form a maximal set of independent $\mathcal{S}$-units, generating a subgroup (modulo torsion) of index:

$$h_m^+ \cdot (h_m^-)^{d-1} \cdot 2^b \cdot \left(2^{\frac{\varphi(m)}{2}-1} \cdot 2^a\right)^d, \quad \text{for explicitly defined } a, b.$$

A quick summary

Let $K_m = \mathbb{Q}(\zeta_m)$, $m \not\equiv 2 \mod 4$, $n = \deg K_m$
$\mathcal{S} = \mathcal{S}_\infty \cup \{\mathfrak{L}_i \mid \ell_i \cdot \mathcal{O}_K;\ \ell_i \equiv 1 \mod m, i \in [\![1, d]\!]\}$ a set of places.

1. Circular units
2. Explicit Stickelberger generators
3. Real $\mathcal{S}^+$-units (that are not units) in K_m^+

Theorem (suppose for the presentation that all $\mathfrak{L}_i$ generate the class group)

These form a maximal set of independent $\mathcal{S}$-units, generating a subgroup (modulo torsion) of index:

$$h_m^+ \cdot (h_m^-)^{d-1} \cdot 2^b \cdot \left(2^{\frac{\varphi(m)}{2}-1} \cdot 2^a\right)^d, \quad \textit{for explicitly defined } a, b.$$

A quick summary

Let $K_m = \mathbb{Q}(\zeta_m)$, $m \not\equiv 2 \mod 4$, $n = \deg K_m$
$\mathcal{S} = \mathcal{S}_\infty \cup \{\mathfrak{L}_i \mid \ell_i \cdot \mathcal{O}_K;\ \ell_i \equiv 1 \mod m, i \in [\![1, d]\!]\}$ a set of places.

1. Circular units
2. Explicit Stickelberger generators
3. Real $\mathcal{S}^+$-units (that are not units) in K_m^+

Theorem (suppose for the presentation that all $\mathfrak{L}_i$ generate the class group)

These form a maximal set of independent $\mathcal{S}$-units, generating a subgroup (modulo torsion) of index:

$$h_m^+ \cdot (h_m^-)^{d-1} \cdot 2^b \cdot \left(2^{\frac{\varphi(m)}{2}-1} \cdot 2^a\right)^d, \quad \textit{for explicitly defined } a, b.$$

A quick summary

Let $K_m = \mathbb{Q}(\zeta_m)$, $m \not\equiv 2 \mod 4$, $n = \deg K_m$
$\mathcal{S} = \mathcal{S}_\infty \cup \{\mathfrak{L}_i \mid \ell_i \cdot \mathcal{O}_K;\ \ell_i \equiv 1 \mod m, i \in [\![1, d]\!]\}$ a set of places.

1. Circular units
2. Explicit Stickelberger generators
3. Real $\mathcal{S}^+$-units (that are not units) in K_m^+

Theorem (suppose for the presentation that all $\mathfrak{L}_i$ generate the class group)

These form a maximal set of independent $\mathcal{S}$-units, generating a subgroup (modulo torsion) of index:

$$h_m^+ \cdot (h_m^-)^{d-1} \cdot 2^b \cdot \left(2^{\frac{\varphi(m)}{2}-1} \cdot 2^a\right)^d, \quad \textit{for explicitly defined } a, b.$$

A quick summary

Let $K_m = \mathbb{Q}(\zeta_m)$, $m \not\equiv 2 \mod 4$, $n = \deg K_m$
$\mathcal{S} = \mathcal{S}_\infty \cup \{\mathfrak{L}_i \mid \ell_i \cdot \mathcal{O}_K;\ \ell_i \equiv 1 \mod m, i \in [\![1, d]\!]\}$ a set of places.

1. Circular units
2. Explicit Stickelberger generators
3. Real $\mathcal{S}^+$-units (that are not units) in K_m^+

Theorem (suppose for the presentation that all $\mathfrak{L}_i$ generate the class group)

These form a maximal set of independent $\mathcal{S}$-units, generating a subgroup (modulo torsion) of index:

$$h_m^+ \cdot (h_m^-)^{d-1} \cdot 2^b \cdot \left(2^{\frac{\varphi(m)}{2}-1} \cdot 2^a\right)^d, \quad \textit{for explicitly defined } a, b.$$

- Obtain a full-rank log-$\mathcal{S}$-unit sub-lattice in dim n from $\mathcal{S}^+$-units in dim $n/2$. This is how we breach the $n \leq 80$ barrier to reach $n = 210$!

Circular units

Let $K_m = \mathbb{Q}(\zeta_m), m \not\equiv 2 \mod 4$.

Definition (Circular units)

Let V_m generated by $\left\{1 - \zeta_m^a;\ 1 \le a \le m\right\}$. The group of circular units is

$$C_m := V_m \cap \mathcal{O}_{K_m}^\times.$$

For any m, we know:

- an explicit system of fundamental circular units,
- a basis of the log-unit sublattice of circular units, moreover ([CDW21]):

$$\|\mathrm{Log}_{\mathcal{S}_\infty}(1 - \zeta_m^a)\|_2 \le 1.32\sqrt{m}.$$

- an explicit formula for the index $\left[\mathcal{O}_{K_m}^\times : C_m\right]$ ([Sin80])

Stickelberger ideal

Let $K_m = \mathbb{Q}(\zeta_m)$, $m \not\equiv 2 \mod 4$,
$G_m = \mathrm{Gal}(K_m/\mathbb{Q}) = \left\{\sigma_s : \zeta_m \mapsto \zeta_m^s;\ (s,m)=1\right\}$.

Definition (Stickelberger ideal)

Let $\mathcal{S}'_m$ be generated by $\{\theta_m(a);\ 0 < a < m\} \cup \{\frac{1}{2}N_m\}$, for:

$$\theta_m(a) = \sum_{s \in (\mathbb{Z}/m\mathbb{Z})^\times} \left\{-\frac{as}{m}\right\} \cdot \sigma_s^{-1} \in \mathbb{Q}\left[G_m\right],$$

and $N_m = \sum_{\sigma \in G_m} \sigma$. The Stickelberger ideal is $\mathcal{S}_m = \mathcal{S}'_m \cap \mathbb{Z}[G_m]$.

- Don't look too hard at the definition.
- The Stickelberger ideal gives free relations in Cl_{K_m}.
- The proof is explicit !

Stickelberger ideal

Let $K_m = \mathbb{Q}(\zeta_m)$, $m \not\equiv 2 \mod 4$,
$G_m = \mathrm{Gal}(K_m/\mathbb{Q}) = \{\sigma_s : \zeta_m \mapsto \zeta_m^s;\ (s,m) = 1\}$.

Definition (Stickelberger ideal)

Let $\mathcal{S}'_m$ be generated by $\{\theta_m(a);\ 0 < a < m\} \cup \{\frac{1}{2} N_m\}$, for:

$$\theta_m(a) = \sum_{s \in (\mathbb{Z}/m\mathbb{Z})^\times} \left\{-\frac{as}{m}\right\} \cdot \sigma_s^{-1} \in \mathbb{Q}\big[G_m\big],$$

and $N_m = \sum_{\sigma \in G_m} \sigma$. The Stickelberger ideal is $\mathcal{S}_m = \mathcal{S}'_m \cap \mathbb{Z}[G_m]$.

- Don't look too hard at the definition.
- The Stickelberger ideal gives free relations in Cl_{K_m}.
- The proof is explicit !

Stickelberger ideal

Let $K_m = \mathbb{Q}(\zeta_m)$, $m \not\equiv 2 \mod 4$,
$G_m = \mathrm{Gal}(K_m/\mathbb{Q}) = \left\{\sigma_s : \zeta_m \mapsto \zeta_m^s;\ (s,m) = 1\right\}$.

Definition (Stickelberger ideal)

Let $\mathcal{S}'_m$ be generated by $\{\theta_m(a);\ 0 < a < m\} \cup \{\frac{1}{2}N_m\}$, for:

$$\theta_m(a) = \sum_{s \in (\mathbb{Z}/m\mathbb{Z})^\times} \left\{-\frac{as}{m}\right\} \cdot \sigma_s^{-1} \in \mathbb{Q}\left[G_m\right],$$

and $N_m = \sum_{\sigma \in G_m} \sigma$. The Stickelberger ideal is $\mathcal{S}_m = \mathcal{S}'_m \cap \mathbb{Z}[G_m]$.

- Don't look too hard at the definition.
- The Stickelberger ideal gives free relations in Cl_{K_m}.
- The proof is explicit !

Stickelberger ideal

Let $K_m = \mathbb{Q}(\zeta_m)$, $m \not\equiv 2 \mod 4$,
$G_m = \mathrm{Gal}(K_m/\mathbb{Q}) = \left\{\sigma_s : \zeta_m \mapsto \zeta_m^s;\ (s,m) = 1\right\}$.

Definition (Stickelberger ideal)

Let $\mathcal{S}'_m$ be generated by $\{\theta_m(a);\ 0 < a < m\} \cup \{\frac{1}{2} N_m\}$, for:

$$\theta_m(a) = \sum_{s \in (\mathbb{Z}/m\mathbb{Z})^\times} \left\{-\frac{as}{m}\right\} \cdot \sigma_s^{-1} \in \mathbb{Q}\left[G_m\right],$$

and $N_m = \sum_{\sigma \in G_m} \sigma$. The Stickelberger ideal is $\mathcal{S}_m = \mathcal{S}'_m \cap \mathbb{Z}[G_m]$.

- Don't look too hard at the definition.
- The Stickelberger ideal gives free relations in Cl_{K_m}.
- The proof is explicit !

Explicit Stickelberger generators

Let $\mathfrak{L} \mid \ell$ be a split prime ideal, and let $\beta\theta_m(-1) \in \mathcal{S}_m$.

There is an explicit $\gamma \in K_m$ st. $\langle\gamma\rangle = \mathfrak{L}^{\beta\theta_m(-1)}$:

- $\chi_{\mathfrak{L}} : a \in \mathcal{O}_K/\mathfrak{L} \longmapsto \zeta_m^k \equiv a^{(\ell-1)/m} \mod \mathfrak{L}$, *($\ell$-th power Legendre symbol)*
- $g(\chi_{\mathfrak{L}}) = -\sum_{a\in\mathbb{F}_\ell^*} \chi_{\mathfrak{L}}(a) \cdot \zeta_\ell^a \in \mathbb{Q}[\zeta_{m\ell}]$, *(Gauss sum)*
- $\langle g(\chi_{\mathfrak{L}})^\beta \rangle = \mathfrak{L}^{\beta\theta_m(-1)}$. *(Stickelberger factorization)*

Explicit Stickelberger generators

Let $\mathfrak{L} \mid \ell$ be a split prime ideal, and let $\beta\theta_m(-1) \in \mathcal{S}_m$.

There is an explicit $\gamma \in K_m$ st. $\langle\gamma\rangle = \mathfrak{L}^{\beta\theta_m(-1)}$:

- $\chi_{\mathfrak{L}} : a \in \mathcal{O}_K/\mathfrak{L} \longmapsto \zeta_m^k \equiv a^{(\ell-1)/m} \mod \mathfrak{L}$, *($\ell$-th power Legendre symbol)*
- $g(\chi_{\mathfrak{L}}) = -\sum_{a\in\mathbb{F}_\ell^*} \chi_{\mathfrak{L}}(a) \cdot \zeta_\ell^a \quad \in \mathbb{Q}[\zeta_{m\ell}]$, *(Gauss sum)*
- $\langle g(\chi_{\mathfrak{L}})^\beta\rangle = \mathfrak{L}^{\beta\theta_m(-1)}$. *(Stickelberger factorization)*

Explicit Stickelberger generators

Let $\mathfrak{L} \mid \ell$ be a split prime ideal, and let $\beta\theta_m(-1) \in \mathcal{S}_m$.

There is an explicit $\gamma \in K_m$ st. $\langle\gamma\rangle = \mathfrak{L}^{\beta\theta_m(-1)}$:

- $\chi_{\mathfrak{L}} : a \in \mathcal{O}_K/\mathfrak{L} \longmapsto \zeta_m^k \equiv a^{(\ell-1)/m} \mod \mathfrak{L}$, *($\ell$-th power Legendre symbol)*
- $g(\chi_{\mathfrak{L}}) = -\sum_{a\in\mathbb{F}_\ell^*} \chi_{\mathfrak{L}}(a) \cdot \zeta_\ell^a \quad \in \mathbb{Q}[\zeta_{m\ell}]$, *(Gauss sum)*
- $\langle g(\chi_{\mathfrak{L}})^\beta\rangle = \mathfrak{L}^{\beta\theta_m(-1)}$. *(Stickelberger factorization)*

Explicit Stickelberger generators

Let $\mathfrak{L} \mid \ell$ be a split prime ideal, and let $\beta\theta_m(-1) \in \mathcal{S}_m$.

There is an explicit $\gamma \in K_m$ st. $\langle\gamma\rangle = \mathfrak{L}^{\beta\theta_m(-1)}$:

- $\chi_{\mathfrak{L}} : a \in \mathcal{O}_K/\mathfrak{L} \longmapsto \zeta_m^k \equiv a^{(\ell-1)/m} \mod \mathfrak{L}$, *($\ell$-th power Legendre symbol)*
- $g(\chi_{\mathfrak{L}}) = -\sum_{a\in\mathbb{F}_\ell^*} \chi_{\mathfrak{L}}(a) \cdot \zeta_\ell^a \quad \in \mathbb{Q}[\zeta_{m\ell}]$, *(Gauss sum)*
- $\langle g(\chi_{\mathfrak{L}})^\beta\rangle = \mathfrak{L}^{\beta\theta_m(-1)}$. *(Stickelberger factorization)*

Problems:

1. Compute in $\mathbb{Q}[\zeta_{m\ell}]$?
2. Coefficients grow FAST
3. We will need to 2-saturate these, so we have to start as low as possible.

Explicit Stickelberger generators

Let $\mathfrak{L} \mid \ell$ be a split prime ideal, and let $\beta\theta_m(-1) \in \mathcal{S}_m$.

There is an explicit $\gamma \in K_m$ st. $\langle\gamma\rangle = \mathfrak{L}^{\beta\theta_m(-1)}$:

- $\chi_{\mathfrak{L}} : a \in \mathcal{O}_K/\mathfrak{L} \longmapsto \zeta_m^k \equiv a^{(\ell-1)/m} \mod \mathfrak{L}$, *($\ell$-th power Legendre symbol)*
- $g(\chi_{\mathfrak{L}}) = -\sum_{a\in\mathbb{F}_\ell^*} \chi_{\mathfrak{L}}(a)\cdot\zeta_\ell^a \in \mathbb{Q}[\zeta_{m\ell}]$, *(Gauss sum)*
- $\langle g(\chi_{\mathfrak{L}})^\beta\rangle = \mathfrak{L}^{\beta\theta_m(-1)}$. *(Stickelberger factorization)*

Problems:

1. Compute in $\mathbb{Q}[\zeta_{m\ell}]$?
2. Coefficients grow FAST
3. We will need to 2-saturate these, so we have to start as low as possible.

Explicit Stickelberger generators

Let $\mathfrak{L} \mid \ell$ be a split prime ideal, and let $\beta\theta_m(-1) \in \mathcal{S}_m$.

There is an explicit $\gamma \in K_m$ st. $\langle\gamma\rangle = \mathfrak{L}^{\beta\theta_m(-1)}$:

- $\chi_{\mathfrak{L}} : a \in \mathcal{O}_K/\mathfrak{L} \longmapsto \zeta_m^k \equiv a^{(\ell-1)/m} \mod \mathfrak{L}$, *($\ell$-th power Legendre symbol)*
- $g(\chi_{\mathfrak{L}}) = -\sum_{a\in\mathbb{F}_\ell^*} \chi_{\mathfrak{L}}(a)\cdot\zeta_\ell^a \quad \in \mathbb{Q}[\zeta_{m\ell}]$, *(Gauss sum)*
- $\langle g(\chi_{\mathfrak{L}})^\beta\rangle = \mathfrak{L}^{\beta\theta_m(-1)}$. *(Stickelberger factorization)*

Problems:

1. Compute in $\mathbb{Q}[\zeta_{m\ell}]$?
2. Coefficients grow FAST
3. We will need to 2-saturate these, so we have to start as low as possible.

Explicit Stickelberger generators

Let $\mathfrak{L} \mid \ell$ be a split prime ideal, and let $\beta\theta_m(-1) \in \mathcal{S}_m$.

There is an explicit $\gamma \in K_m$ st. $\langle\gamma\rangle = \mathfrak{L}^{\beta\theta_m(-1)}$:

- $\chi_{\mathfrak{L}} : a \in \mathcal{O}_K/\mathfrak{L} \longmapsto \zeta_m^k \equiv a^{(\ell-1)/m} \mod \mathfrak{L}$, *($\ell$-th power Legendre symbol)*
- $g(\chi_{\mathfrak{L}}) = -\sum_{a\in\mathbb{F}_\ell^*} \chi_{\mathfrak{L}}(a)\cdot\zeta_\ell^a \quad \in \mathbb{Q}[\zeta_{m\ell}]$, *(Gauss sum)*
- $\langle g(\chi_{\mathfrak{L}})^\beta\rangle = \mathfrak{L}^{\beta\theta_m(-1)}$. *(Stickelberger factorization)*

Problems:

1. Compute in $\mathbb{Q}[\zeta_{m\ell}]$?
2. Coefficients grow FAST
3. We will need to 2-saturate these, so we have to start as low as possible.

Short Stickelberger relations

Short: $\beta = \sum_\sigma \varepsilon_\sigma \sigma \in \mathbb{Z}[G_m]$, with $\varepsilon_\sigma \in \{0,1\}$

Theorem (A family of short Stickelberger elements [BK21, Pr.3.1])

Let a, b st. $m \nmid a$, $m \nmid b$, $m \nmid (a+b)$. Then:

$$\theta_{a,b} = \theta_m(a) + \theta_m(b) - \theta_m(a+b)$$

is short; moreover $\|\theta_{a,b}\|_2 = \sqrt{\varphi(m)/2}$.

- Express corresponding generators by Jacobi sums: $(\langle \mathcal{J}_\mathfrak{L}(a,b)\rangle = \mathfrak{L}^{\theta_{a,b}})$
  $$\mathcal{J}_\mathfrak{L}(a,b) = -\sum_{u \in \mathcal{O}_{K_m}/\mathfrak{L}} \chi_\mathfrak{L}^a(u)\chi_\mathfrak{L}^b(1-u) \quad \in \mathbb{Q}[\zeta_m].$$ *[BK21, §5]*
- From these we can even extract a short basis for any m. *([BK21, Th.3.6])*
  $\Rightarrow$ Coefficients on $\mathbb{Z}[\zeta_m]$ stay (much much) lower, no denominators.
  This is especially crucial for the 2-saturation step in big dimensions !
- The proof gives an algorithm to compute h_m^-. *(a determinant computation)*

Short Stickelberger relations

Short: $\beta = \sum_\sigma \varepsilon_\sigma \sigma \in \mathbb{Z}[G_m]$, with $\varepsilon_\sigma \in \{0, 1\}$

Theorem (A family of short Stickelberger elements [BK21, Pr.3.1])

Let a, b st. $m \nmid a$, $m \nmid b$, $m \nmid (a+b)$. Then:

$$\theta_{a,b} = \theta_m(a) + \theta_m(b) - \theta_m(a+b)$$

is short; moreover $\|\theta_{a,b}\|_2 = \sqrt{\varphi(m)/2}$.

- Express corresponding generators by Jacobi sums: $(\langle \mathcal{J}_{\mathfrak{L}}(a,b)\rangle = \mathfrak{L}^{\theta_{a,b}})$
$$\mathcal{J}_{\mathfrak{L}}(a,b) = -\sum_{u \in \mathcal{O}_{K_m}/\mathfrak{L}} \chi_{\mathfrak{L}}^a(u)\chi_{\mathfrak{L}}^b(1-u) \in \mathbb{Q}[\zeta_m].$$
[BK21, §5]
- From these we can even extract a short basis for any m. *([BK21, Th.3.6])*
$\Rightarrow$ Coefficients on $\mathbb{Z}[\zeta_m]$ stay (much much) lower, no denominators.
This is especially crucial for the 2-saturation step in big dimensions !
- The proof gives an algorithm to compute h_m^-. *(a determinant computation)*

Short Stickelberger relations

Short: $\beta = \sum_\sigma \varepsilon_\sigma \sigma \in \mathbb{Z}[G_m]$, with $\varepsilon_\sigma \in \{0,1\}$

Theorem (A family of short Stickelberger elements [BK21, Pr.3.1])

Let a, b st. $m \nmid a$, $m \nmid b$, $m \nmid (a+b)$. Then:

$$\theta_{a,b} = \theta_m(a) + \theta_m(b) - \theta_m(a+b)$$

is short; moreover $\|\theta_{a,b}\|_2 = \sqrt{\varphi(m)/2}$.

- Express corresponding generators by Jacobi sums: *($\langle \mathcal{J}_{\mathfrak{L}}(a,b)\rangle = \mathfrak{L}^{\theta_{a,b}}$)*
$$\mathcal{J}_{\mathfrak{L}}(a,b) = -\sum_{u \in \mathcal{O}_{K_m}/\mathfrak{L}} \chi_{\mathfrak{L}}^a(u)\chi_{\mathfrak{L}}^b(1-u) \quad \in \mathbb{Q}[\zeta_m].$$
[BK21, §5]
- From these we can even extract a short basis for any m. *([BK21, Th.3.6])*
$\Rightarrow$ Coefficients on $\mathbb{Z}[\zeta_m]$ stay (much much) lower, no denominators.
This is especially crucial for the 2-saturation step in big dimensions !
- The proof gives an algorithm to compute h_m^-. *(a determinant computation)*

Short Stickelberger relations

Short: $\beta = \sum_\sigma \varepsilon_\sigma \sigma \in \mathbb{Z}[G_m]$, with $\varepsilon_\sigma \in \{0,1\}$

Theorem (A family of short Stickelberger elements [BK21, Pr.3.1])

Let a, b st. $m \nmid a$, $m \nmid b$, $m \nmid (a+b)$. Then:

$$\theta_{a,b} = \theta_m(a) + \theta_m(b) - \theta_m(a+b)$$

is short; moreover $\|\theta_{a,b}\|_2 = \sqrt{\varphi(m)/2}$.

- Express corresponding generators by Jacobi sums: $(\langle \mathcal{J}_{\mathfrak{L}}(a,b)\rangle = \mathfrak{L}^{\theta_{a,b}})$
$$\mathcal{J}_{\mathfrak{L}}(a,b) = -\sum_{u\in\mathcal{O}_{K_m}/\mathfrak{L}} \chi_{\mathfrak{L}}^a(u)\chi_{\mathfrak{L}}^b(1-u) \quad \in \mathbb{Q}[\zeta_m].$$
[BK21, §5]
- From these we can even extract a short basis for any m. *([BK21, Th.3.6])*
  $\Rightarrow$ Coefficients on $\mathbb{Z}[\zeta_m]$ stay (much much) lower, no denominators.
  This is especially crucial for the 2-saturation step in big dimensions !
- The proof gives an algorithm to compute h_m^-. *(a determinant computation)*

Today's à la carte

What do we want ?

Breach the small dimension barrier for $\mathcal{S}$-unit attacks:

1. Geometric characteristics of log-$\mathcal{S}$-unit (sub)lattices
2. Better Approx Factors than predicted by theory ? Also in higher regimes ?
3. We only have a picture for degree ≤ 70 for (1), degree ≤ 52 for (2)

- Necessary to gather more experimental observations before predicting things

Climbing degrees is classically HARD !!

What do we want ?

Breach the small dimension barrier for $\mathcal{S}$-unit attacks:

1. Geometric characteristics of log-$\mathcal{S}$-unit (sub)lattices
2. Better Approx Factors than predicted by theory ? Also in higher regimes ?
3. We only have a picture for degree ≤ 70 for (1), degree ≤ 52 for (2)

- Necessary to gather more experimental observations before predicting things

Climbing degrees is classically HARD !!

What do we want ?

Breach the small dimension barrier for $\mathcal{S}$-unit attacks:

1. Geometric characteristics of log-$\mathcal{S}$-unit (sub)lattices
2. Better Approx Factors than predicted by theory ? Also in higher regimes ?
3. We only have a picture for degree ≤ 70 for (1), degree ≤ 52 for (2)

- Necessary to gather more experimental observations before predicting things

Climbing degrees is classically HARD !!

What do we want ?

Breach the small dimension barrier for $\mathcal{S}$-unit attacks:

1. Geometric characteristics of log-$\mathcal{S}$-unit (sub)lattices
2. Better Approx Factors than predicted by theory ? Also in higher regimes ?
3. We only have a picture for degree ≤ 70 for (1), degree ≤ 52 for (2)

- Necessary to gather more experimental observations before predicting things

Climbing degrees is classically HARD !!

What do we want ?

Breach the small dimension barrier for $\mathcal{S}$-unit attacks:

1. Geometric characteristics of log-$\mathcal{S}$-unit (sub)lattices
2. Better Approx Factors than predicted by theory ? Also in higher regimes ?
3. We only have a picture for degree ≤ 70 for (1), degree ≤ 52 for (2)

▶ Necessary to gather more experimental observations before predicting things

Climbing degrees is classically HARD !!

What do we have ?

Let $K_m = \mathbb{Q}(\zeta_m), m \not\equiv 2 \mod 4$
$\mathcal{S} = \mathcal{S}_\infty \cup \{\mathfrak{L}_i \mid \ell_i \cdot \mathcal{O}_K;\ \ell_i \equiv 1 \mod m, i \in [\![1, d]\!]\}$ a set of places.

Compute:

1. Circular units
2. $\mathcal{S}^+$-units (of norm > 1)
3. Stickelberger generators $\mathcal{J}_\mathfrak{L}(a,b)$ of a basis of $\theta_{a,b}$'s of $\mathcal{S}_m$
4. 2-saturation of these to remove the 2^{HUGE} in the index in $\mathcal{O}^\times_{K_m,\mathcal{S}}$

- Obtain "Twisted-PHS like" log-$\mathcal{S}$-unit sub-lattices, for $\deg \mathbb{Q}(\zeta_m) \leq 210$.
  Remaining index: $\approx (h_m^-)^{d-1}$
- This is only a degraded mode of Twisted-PHS, for example in $\mathbb{Q}(\zeta_{211})$:
  - $\min \mathrm{Vol}^{1/\dim} L_{\mathrm{sat}} = 11.39$, reached for $d = 1$
  - $\min \mathrm{Vol}^{1/\dim} L_{\mathrm{su}} = 9.6$, reached for $d_{\max} = 7$ (*uncomputable*)

What do we have ?

Let $K_m = \mathbb{Q}(\zeta_m), m \not\equiv 2 \mod 4$
$\mathcal{S} = \mathcal{S}_\infty \cup \{\mathfrak{L}_i \mid \ell_i \cdot \mathcal{O}_K;\ \ell_i \equiv 1 \mod m, i \in [\![1, d]\!]\}$ a set of places.

Compute:

1. Circular units
2. $\mathcal{S}^+$-units (of norm > 1)
3. Stickelberger generators $\mathcal{J}_\mathfrak{L}(a, b)$ of a basis of $\theta_{a,b}$'s of $\mathcal{S}_m$
4. 2-saturation of these to remove the 2^{HUGE} in the index in $\mathcal{O}^\times_{K_m,\mathcal{S}}$

- Obtain "Twisted-PHS like" log-$\mathcal{S}$-unit sub-lattices, for $\deg \mathbb{Q}(\zeta_m) \leq 210$.
  Remaining index: $\approx (h_m^-)^{d-1}$
- This is only a degraded mode of Twisted-PHS, for example in $\mathbb{Q}(\zeta_{211})$:
  - $\min \mathrm{Vol}^{1/\dim} L_{\mathrm{sat}} = 11.39$, reached for $d = 1$
  - $\min \mathrm{Vol}^{1/\dim} L_{\mathrm{su}} = 9.6$, reached for $d_{\max} = 7$ (*uncomputable*)

What do we have ?

Let $K_m = \mathbb{Q}(\zeta_m), m \not\equiv 2 \mod 4$
$\mathcal{S} = \mathcal{S}_\infty \cup \{\mathfrak{L}_i \mid \ell_i \cdot \mathcal{O}_K;\ \ell_i \equiv 1 \mod m, i \in [\![1, d]\!]\}$ a set of places.

Compute:

1. Circular units
2. $\mathcal{S}^+$-units (of norm > 1)
3. Stickelberger generators $\mathcal{J}_{\mathfrak{L}}(a, b)$ of a basis of $\theta_{a,b}$'s of $\mathcal{S}_m$
4. 2-saturation of these to remove the 2^{HUGE} in the index in $\mathcal{O}^\times_{K_m,\mathcal{S}}$

- Obtain "Twisted-PHS like" log-$\mathcal{S}$-unit sub-lattices, for $\deg \mathbb{Q}(\zeta_m) \le 210$.
  Remaining index: $\approx (h_m^-)^{d-1}$
- This is only a degraded mode of Twisted-PHS, for example in $\mathbb{Q}(\zeta_{211})$:
  - $\min \mathrm{Vol}^{1/\dim} L_{\mathrm{sat}} = 11.39$, reached for $d = 1$
  - $\min \mathrm{Vol}^{1/\dim} L_{\mathrm{su}} = 9.6$, reached for $d_{\max} = 7$ (*uncomputable*)

What do we have ?

Let $K_m = \mathbb{Q}(\zeta_m), m \not\equiv 2 \mod 4$
$\mathcal{S} = \mathcal{S}_\infty \cup \{\mathfrak{L}_i \mid \ell_i \cdot \mathcal{O}_K;\ \ell_i \equiv 1 \mod m, i \in [\![1, d]\!]\}$ a set of places.

Compute:

1. Circular units
2. $\mathcal{S}^+$-units (of norm > 1)
3. Stickelberger generators $\mathcal{J}_{\mathfrak{L}}(a, b)$ of a basis of $\theta_{a,b}$'s of $\mathcal{S}_m$
4. 2-saturation of these to remove the 2^{HUGE} in the index in $\mathcal{O}^\times_{K_m,\mathcal{S}}$

- Obtain "Twisted-PHS like" log-$\mathcal{S}$-unit sub-lattices, for $\deg \mathbb{Q}(\zeta_m) \leq 210$. Remaining index: $\approx (h_m^-)^{d-1}$
- This is only a degraded mode of Twisted-PHS, for example in $\mathbb{Q}(\zeta_{211})$:
  - $\min \mathrm{Vol}^{1/\dim} L_{\mathrm{sat}} = 11.39$, reached for $d = 1$
  - $\min \mathrm{Vol}^{1/\dim} L_{\mathrm{su}} = 9.6$, reached for $d_{\max} = 7$ *(uncomputable)*

What do we have ?

Let $K_m = \mathbb{Q}(\zeta_m)$, $m \not\equiv 2 \mod 4$
$\mathcal{S} = \mathcal{S}_\infty \cup \{\mathfrak{L}_i \mid \ell_i \cdot \mathcal{O}_K;\ \ell_i \equiv 1 \mod m, i \in [\![1, d]\!]\}$ a set of places.

Compute:

1. Circular units
2. $\mathcal{S}^+$-units (of norm > 1)
3. Stickelberger generators $\mathcal{J}_{\mathfrak{L}}(a, b)$ of a basis of $\theta_{a,b}$'s of $\mathcal{S}_m$
4. 2-saturation of these to remove the 2^{HUGE} in the index in $\mathcal{O}^\times_{K_m,\mathcal{S}}$

- Obtain "Twisted-PHS like" log-$\mathcal{S}$-unit sub-lattices, for $\deg \mathbb{Q}(\zeta_m) \leq 210$.
  Remaining index: $\approx (h_m^-)^{d-1}$

- This is only a degraded mode of Twisted-PHS, for example in $\mathbb{Q}(\zeta_{211})$:
  - $\min \mathrm{Vol}^{1/\dim} L_{\mathrm{sat}} = 11.39$, reached for $d = 1$
  - $\min \mathrm{Vol}^{1/\dim} L_{\mathrm{su}} = 9.6$, reached for $d_{\max} = 7$ (*uncomputable*)

What do we have ?

Let $K_m = \mathbb{Q}(\zeta_m)$, $m \not\equiv 2 \mod 4$
$\mathcal{S} = \mathcal{S}_\infty \cup \{\mathfrak{L}_i \mid \ell_i \cdot \mathcal{O}_K;\ \ell_i \equiv 1 \mod m, i \in [\![1, d]\!]\}$ a set of places.

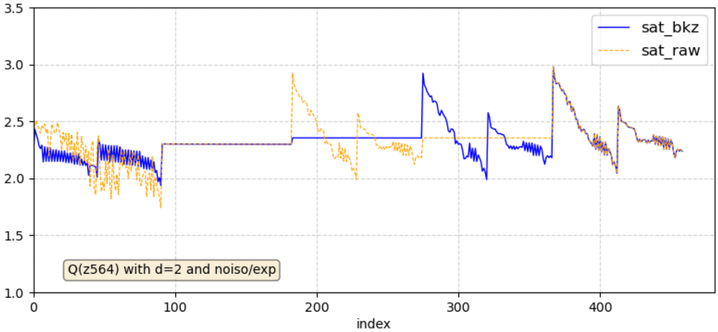
Compute:

1. Circular units
2. $\mathcal{S}^+$-units (of norm > 1)
3. Stickelberger generators $\mathcal{J}_{\mathfrak{L}}(a, b)$ of a basis of $\theta_{a,b}$'s of $\mathcal{S}_m$
4. 2-saturation of these to remove the 2^{HUGE} in the index in $\mathcal{O}^\times_{K_m,\mathcal{S}}$

- Obtain "Twisted-PHS like" log-$\mathcal{S}$-unit sub-lattices, for $\deg \mathbb{Q}(\zeta_m) \leq 210$.
  Remaining index: $\approx (h_m^-)^{d-1}$
- This is only a degraded mode of Twisted-PHS, for example in $\mathbb{Q}(\zeta_{211})$:
  - $\min \mathrm{Vol}^{1/\dim} L_{\mathrm{sat}} = 11.39$, reached for $d = 1$
  - $\min \mathrm{Vol}^{1/\dim} L_{\mathrm{su}} = 9.6$, reached for $d_{\max} = 7$ (*uncomputable*)

Geometric characteristics

Example: $\mathbb{Q}(\zeta_{564})$ for $d = 2$ split orbits in $\mathcal{S}$,
Gram-Schmidt log norms for 2-saturated family of $\mathcal{S}$-units.

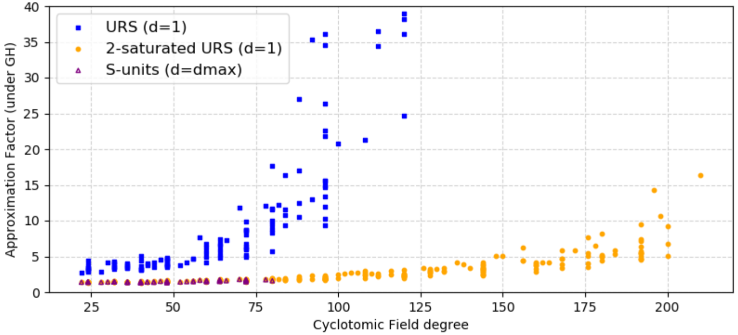


Same shape: (same geometric observations than in Twisted-PHS)

- across all cyclotomic fields of degree ≤ 210 (even in largest dimensions)
- for all choices of factor base $\mathcal{S}$, any sublattice (saturated or not)

▶ This is a very general geometric phenomenon

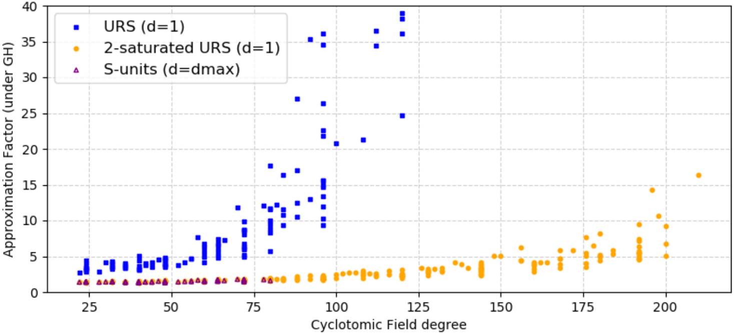
Approximation factor upper bound



- Upper bounds the performance of $\mathcal{S}$-unit attacks beyond degree 100
- Shows no catastrophic impact of $\mathcal{S}$-unit attacks, neither reassuring
- Strong connection between AF and $\mathrm{Vol}^{1/\dim}$

▶ Opens the way to a high dimension simulator.

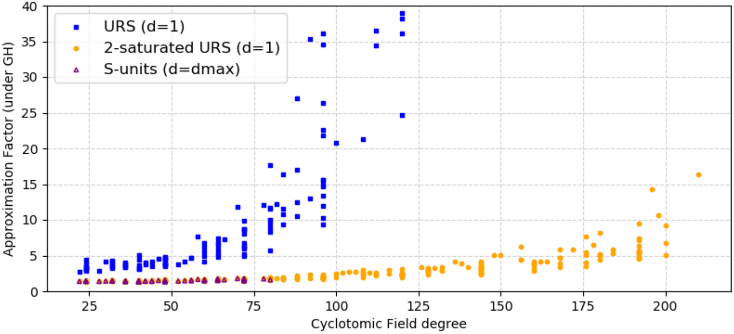
Approximation factor upper bound



- Upper bounds the performance of $\mathcal{S}$-unit attacks beyond degree 100
- Shows no catastrophic impact of $\mathcal{S}$-unit attacks, neither reassuring
- Strong connection between AF and $\mathrm{Vol}^{1/\dim}$

▶ Opens the way to a high dimension simulator.

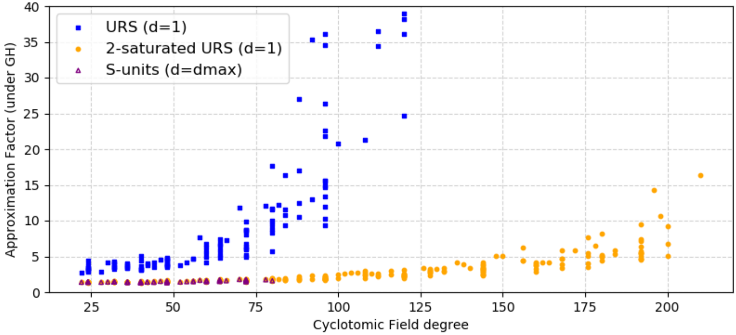
Approximation factor upper bound



- Upper bounds the performance of $\mathcal{S}$-unit attacks beyond degree 100
- Shows no catastrophic impact of $\mathcal{S}$-unit attacks, neither reassuring
- Strong connection between AF and $\mathrm{Vol}^{1/\dim}$

▶ Opens the way to a high dimension simulator.

Approximation factor upper bound



- Upper bounds the performance of $\mathcal{S}$-unit attacks beyond degree 100
- Shows no catastrophic impact of $\mathcal{S}$-unit attacks, neither reassuring
- Strong connection between AF and $\mathrm{Vol}^{1/\dim}$

▶ Opens the way to a high dimension simulator.

Today's à la carte

Future work

1. Derive a reliable estimator of Twisted-PHS performances.
   - Use extended data to reliably support heuristics and estimations.
   - Explain the strong connection between final AF and $\mathrm{Vol}^{1/d}\, L$.
2. Obtain full log-$\mathcal{S}$-unit lattices:
   - *for real subfield with $h_m^+ > 1$ (just a technical wizardry issue);*
   - for higher degree cyclotomic fields ($n \geq 80$) for several Galois orbits;
   - for other families of number fields (multi-quadratics).

Future work

1. Derive a reliable estimator of Twisted-PHS performances.
   - Use extended data to reliably support heuristics and estimations.
   - Explain the strong connection between final AF and $\mathrm{Vol}^{1/d} L$.
2. Obtain full log-$\mathcal{S}$-unit lattices:
   - *for real subfield with $h_m^+ > 1$ (just a technical wizardry issue);*
   - for higher degree cyclotomic fields ($n \geq 80$) for several Galois orbits;
   - for other families of number fields (multi-quadratics).

Questions ?