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], and 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

Abstract. In 2020, Bernard and Roux-Langlois introduced the Twisted-PHS algorithm to solve Approx-Svp for ideal lattices on any number field, based on the PHS algorithm by Pellet-Mary, Hanrot and Stehlé in 2019. They performed experiments for prime conductors cyclotomic fields of degrees at most 70, reporting approximation factors reached in practice. The main obstacle for these experiments is the computation of a log-$\mathcal{S}$-unit lattice, which requires classical subexponential time.
In this paper, our main contribution is to extend these experiments to 192 cyclotomic fields of any conductor m and of degree up to 190. Building upon new results from Bernard and Kučera on the Stickelberger ideal, we construct a maximal set of independent $\mathcal{S}$-units lifted from the maximal real subfield using explicit Stickelberger generators obtained *via* Jacobi sums. Hence, we obtain full-rank log-$\mathcal{S}$-unit sublattices fulfilling the role of approximating the full Tw-PHS lattice. Notably, our obtained approximation factors match those from Bernard and Roux-Langlois using the original log-$\mathcal{S}$-unit lattice in small dimensions.
As a side result, we use the knowledge of these explicit Stickelberger elements to remove almost all quantum steps in the CDW algorithm, by Cramer, Ducas and Wesolowski in 2021, under the mild restriction that the plus part of the class number verifies $h_m^+ \leq O(\sqrt{m})$.

Keywords: Ideal lattices, Approx-SVP, Stickelberger, S-units, Twisted-PHS

1 Introduction

The ongoing NIST Post-Quantum Competition illustrates the importance of the Learning With Errors (LWE) problem as an intermediate building block for a wide variety of cryptographic schemes. Most of these cryptographic schemes rely on a *structured* version of the LWE problem allowing for much more satisfactory performance, compared to schemes based on the *unstructured* LWE problem. The first structured variant of LWE, later known as the Ring-LWE problem, is shown to be at least as hard as the approximate Shortest Vector Problem on ideal lattices (Approx-id-Svp) using quantum worst-case to average-case reduction [SSTX09,LPR10]. However, there exists the possibility that this improved efficiency comes at the cost of degrading the security of the scheme, since the hardness hypothesis is more restricted.

In the case of arbitrary lattices, Approx-Svp is a well-studied hard problem. Its goal is to find relatively short vectors of a given lattice, within an approximation factor of the shortest vector. The best known algorithm to solve this problem is the BKZ algorithm [Sch87], which can be seen as an improvement of the well-known LLL algorithm. The BKZ algorithm actually offers trade-offs between the running time and the reachable approximation factor, known as Schnorr's hierarchy [Sch87]: for $\alpha \in (0,1)$, BKZ can reach an approximation factor $2^{\tilde{O}(n^{\alpha})}$ in time $2^{\tilde{O}(n^{1-\alpha})}$. Moving to the particular case of ideal lattices, that correspond to ideals of the ring of integers $\mathcal{O}_K$ of a number field K, the restriction of Approx-Svp could potentially allow for more efficient reduction algorithms, by exploiting the additional structure. This conjecture would not necessarily come as a surprise since those number theoretical tools are precisely what makes Ring-LWE a more efficient building block for cryptographic schemes. Nevertheless, how to exploit those number theoretical structures is not yet fully decided: at the moment, the best known classical algorithms to solve this problem on ideal lattices remain the same as for arbitrary lattices, and in a quantum world, polynomial time algorithms only reach subexponential approximation factors.

Cryptanalysis of Approx-id-Svp has gradually gathered more attention, as shown by a series of works starting with [EHKS14,CGS14,BS16,CDPR16]. Earlier works on this subject aimed at the more restricted case of *principal* ideal Approx-Svp. A classical strategy for this case is devised as a two parts algorithm. The first part requires solving the Principal Ideal Problem (Pip), hence finding a generator of the ideal; the second part requires solving a Closest Vector Problem (Cvp) in the so called *log-unit lattice*, in the hope of finding the shortest generator of the ideal. At the end, this short generator is expected to solve Approx-Svp for an adequate approximation factor. Building on [EHKS14], it was claimed in [CGS14], without formal proofs, that this strategy works in quantum polynomial time and that the Cvp in the log-unit lattice of cyclotomic fields is easy to solve and indeed yields a short generator. For the first part, results from [BS16] yielded a fully proven quantum polynomial-time algorithm to compute $\mathcal{S}$-units, a generalization of the units of $\mathcal{O}_K$, in arbitrary number fields; the authors also showed how the computation of $\mathcal{S}$-units can be used to obtain class groups as well as to solve Pip. As for the second part, [CDPR16] subsequently formalised these claims and proved, for cyclotomic fields of prime power conductors, that in this case Approx-id-Svp on principal ideals is solvable in quantum polynomial time, but only reaching an approximation factor $2^{\tilde{O}(\sqrt{n})}$.

From there, subsequent works as [CDW17,CDW21] aimed at extending the results from [CDPR16] to *arbitrary* ideal lattices over *any* cyclotomic fields and evaluating their performance. One of their contribution is the introduction of the Close Principal Multiple Problem (Cpmp) that reduces the problem on any ideal lattice to the problem on principal ideal lattices. A new key technical ingredient, related to cyclotomic fields, was the use of the *Stickelberger ideal* for which good properties are known. First, this ideal annihilates the class group and second, when viewed as a $\mathbb{Z}$-module, a family of relatively short generating vectors are explicitly known, allowing a good decoding of the lattice. In [DPW19], the practical consequences of this method were concretely experimented, and simulations results suggested that this algorithm might only beat the BKZ algorithm with block size 300 for cyclotomic fields of quite large degree (more than 20000).

On another direction, authors of [PHS19,BR20] generalized the previous results from [CDPR16,CDW17] to arbitrary number fields using $\mathcal{S}$-units, a formalism underlying the work [PHS19] and explicitly used and described in [BR20]. The PHS algorithm is split in a preprocessing phase and a query phase. The preprocessing phase consists of the preparation of the decoding of a particular lattice depending only on the number field K, *via* the computation of a hint following Laarhoven's CVP with preprocessing algorithm [Laa16]. This lattice allows to express any Approx-id-SVP instance in K as an Approx-CVP instance, and Laarhoven's hint is used during the query phase to effectively solve this CVP instance. Note this lattice was introduced with the idea of combining the two main resolution steps of [CDW17] in only one CVP instance, with the hope of globally optimizing the output. Following this work, [BR20] proposed Tw-PHS, a so-called "Twisted" version of the PHS algorithm using a fundamental modification of the underlying lattice. Namely, they explicitly described it as a logarithmic $\mathcal{S}$-unit lattice, leading to a proper normalisation of the logarithmic $\mathcal{S}$-embedding that weights coordinates according to factor basis prime ideal norms, thus the name "Twisted". Conceptually, the problem of retrieving a short element is expected to be better encoded with this modified embedding, leading to better outputs. Even though the theoretically proven bound for the Tw-PHS algorithm is the same as for the PHS algorithm, experimentally, very significant improvements compared to the original PHS algorithm have been illustrated in [BR20, Fig. 5.3.]. In particular, the experiments implemented in [BR20] allow to test the Tw-PHS algorithm in number fields of degree up to 60, while achieving much better approximation factors than the original [PHS19] implementation.

Our contributions. One of our major contribution is to extend the experiments performed in [BR20] for the Twisted-PHS algorithm. Whereas their experiments on cyclotomic fields where bound to prime conductor fields of degree at most 70, due to the classical complexity of computing full $\mathcal{S}$-unit groups, we compute full rank sublattices of the log-$\mathcal{S}$-unit lattice for 192 cyclotomic fields of *any* conductor from degree 20 up to degree 190. Though, as we will explain later, our sublattices are a lot sparser than the full log-$\mathcal{S}$-unit lattice used in [BR20], our results already give promising approximation factors, as shown in Fig. 1.1, and match, under the Gaussian Heuristic, the *exact* approximation factors obtained in [BR20, Fig. 1.1] when we have the full log-$\mathcal{S}$-unit lattice, i.e. up to degree 80.

To obtain these results, our main contribution is, for cyclotomic fields K_m of *any* conductor $m \not\equiv 2 \mod 4$, to exhibit in §3 a full rank family of *independent* $\mathcal{S}$-units lifted from the maximal real subfield K_m^+, using explicit Stickelberger generators (see §3.3) that are easy to compute using Jacobi sums. Hence,

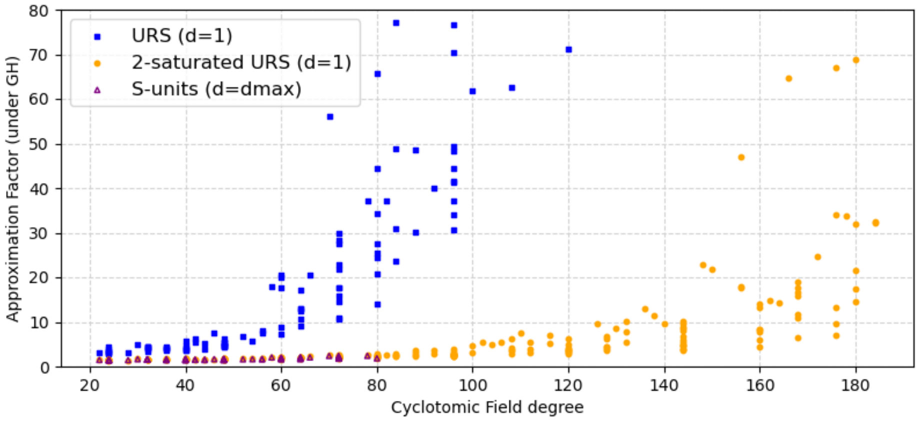

Fig. 1.1 – Approximation factors, estimated with Gaussian Heuristic, reached by Tw-PHS for cyclotomic fields of degree $\varphi(m) < 190$ with $h_m^+ = 1$ on lattices L_{urs}, L_{sat} and L_{su} (when available).

we obtain a full rank sublattice of the log-$\mathcal{S}$-unit lattice, at the much lower cost of computing class group relations in the maximal real subfield of half degree. We also provide in Th. 3.13 a closed formula for the multiplicative index of this full-rank family inside the whole $\mathcal{S}$-unit group. This index is huge, but can be mitigated to some extent using classical saturation techniques recalled in §3.6.

Finally, as a minor contribution, we also apply these results to show in §4 how to benefit from these explicit Stickelberger generators to remove most quantum steps of the CDW algorithm [CDW21], namely the last Pip resolution, and also, under a relatively harmless restriction that the plus part of the class number verifies $h_m^+ \leq O(\sqrt{m})$ (Hyp. A.1), the random walk to the relative class group, replaced by a single call to a quantum class group computation in dimension $\varphi(m)/2$. The latter should also yield in practice better approximation factors, by allowing to choose the finite places of $\mathcal{S}$ of smallest possible norms.

Technical overview. Let $\mathcal{S}$ be a set of places where the finite places correspond to a collection of full Galois orbits of split prime ideals. Our full rank family $\mathfrak{F}$ of independent $\mathcal{S}$-units is composed of three parts:

1. circular units, defined e.g. in [Was97, §8] and for which an explicit basis can be found in [Kuč92, Th. 6.1];
2. Stickelberger generators, as explicitly given by the proof of Stickelberger's theorem, see for example [Sin80, Eq. (3.4)];
3. real $\mathcal{S}^+$-units (apart from real units), where $\mathcal{S}^+$ is the set $\mathcal{S} \cap K_m^+$ of places of $\mathcal{S}$ restricted to the maximal real subfield K_m^+ of K_m.

In the context of the cryptanalysis of id-Svp, the set of circular units has already been used in [CDPR16,CDW17] for m being a prime power, in [Hol17] when m has two coprime factors and finally in [CDW21] in the general case. Using free relations in the class group Cl_m coming from Stickelberger's theorem was suggested in [CDW17,CDW21], where many *short* relations were identified [CDW21, Lem. 4.4]. We use two novelties here:

- First, we use the knowledge of an explicit *short* $\mathbb{Z}$-*basis* of the Stickelberger ideal for *any* conductor [BK21, Th. 3.6]: apart from aesthetic reasons, this should induce in practice slightly better approximation factors compared to [CDW21, Cor. 2.2] where a sublattice of possibly large index is used;
- Second, using the well-known explicit factorization from the proof of Stickelberger's theorem ([Sin80, §3]), we effectively compute generators corresponding to the above short relations, using Jacobi sums as in [BK21, §5].

We note that using a Hermite Normal Form or a LLL reduction to derive a basis from the short generating set W of [CDW21, §4.2] increases dramatically the coefficients of the corresponding generators, or forces to handle *huge* rational numbers, in a way that significantly hinders subsequent computations. Finally, adding relative norm relations $\mathcal{N}_{K_m/K_m^+}(\mathfrak{L}) = \mathfrak{L}^{1+\tau}$ when the $\mathfrak{L}$'s are chosen in the relative class group was suggested in [CDW17] to obtain the so-called "extended Stickelberger lattice". We extend this result by considering the lattice of real class relations between the relative norms of ideals of any class.

The multiplicative index of this family in the full $\mathcal{S}$-unit group is explicited by our Th. 3.13. This index contains a large power of 2 that can be removed using classical 2-saturation techniques of §3.6, leading to a family $\mathfrak{F}_{\mathsf{sat}}$. Unfortunately, when the number of orbits in $\mathcal{S}$ is strictly greater than 1, this index contains *huge* factors coming from the relative class number, due to the fact that the Stickelberger ideal misses all relations between ideals of distinct Galois orbits.

In the context of the CDW algorithm, we first propose in §4 an equivalent rewriting of [CDW21, Alg. 7] that enlightens some hidden steps that reveal useful for subsequent modifications. Then, we plug the explicit Stickelberger generators and real generators described above to remove the last call to the quantum Pip solver. Finally, by considering the module of *all* real class group relations, we remove the need of a random walk mapping any ideal of K_m into Cl_m^-, at the small price of restricting to cyclotomic fields such that $h_m^+ \leq O(\sqrt{m})$ (Hyp. A.1), whereas [CDW21, Ass. 2] uses $h_m^+ \leq \mathrm{poly}(m)$. Then, only two quantum steps remain: the first is performed only once in dimension $\frac{\varphi(m)}{2}$ to compute real class group relations and generators, the second is for solving the ClDl for each query.

Finally, we apply the Tw-PHS algorithm [BR20] on our full-rank sublattices of the log-$\mathcal{S}$-unit lattice. We stress that this is actually a *degraded* mode of the Tw-PHS algorithm. Indeed, Tw-PHS uses the full log-$\mathcal{S}$-unit lattice for an optimal number $d = d_{\max}$ of orbits, that we estimated using the analytic class number formula. However, in our case, the family $\mathfrak{F}_{\mathsf{sat}}$ has index roughly $(h_m^-)^{d-1}$, which is sufficiently large so that the optimal factor base phenomenon of [BR20, Alg. 4.1] does not hold. More precisely, the density of the log-$\mathcal{S}$-unit sublattice associated to $\mathfrak{F}_{\mathsf{sat}}$ decreases as soon as $d > 1$.

We fully implemented the construction of the lattices associated to $\mathfrak{F}$, $\mathfrak{F}_{\mathsf{sat}}$ and to fundamental elements of the full $\mathcal{S}$-unit group $\mathfrak{F}_{\mathsf{su}}$ when available (up to degree 80) for the first d split prime orbits with $d \in [\![1, d_{\max}]\!]$, including the computation of Stickelberger generators and real generators. We evaluate the geometry of all these lattices with standard indicators described in §2.5, and observed consistently the same phenomenons already observed in [BR20, §5.1 and 5.2], that indicate close to orthogonal lattices. Moreover, as computing ClDL solutions for random targets is not possible, we simulate the query phase *via* random targets. The approximation factors obtained in this degraded mode still seem promising, and give a crude-but-reliable upper bound on the approximation factor that can be expected when using Tw-PHS. We stress that, up to degree 80 when the full $\mathcal{S}$-unit group is computable, our results match, under the Gaussian Heuristic, the *exact* approximation factors obtained by [BR20, Fig. 1.1]. The full implementation is available at `https://github.com/ob3rnard/Tw-Sti`.

Remark. Similar techniques for the construction of $\mathcal{S}$-units may be used in a concurrent work by Bernstein, Eisenträger, Rubin, Silverberg and van Vredendaal, as announced in a talk by Bernstein on 20th August 2021 at SIAM Conference.

2 Preliminaries

Notations. For any $i, j \in \mathbb{Z}$ with $i \le j$, the set of all integers between i and j is denoted by $[\![i,j]\!]$. For any $x \in \mathbb{Q}$, let $\{x\}$ denote its fractional part, i.e. such that $0 \le \{x\} < 1$ and $x - \{x\} \in \mathbb{Z}$. A vector is materialized by a bold letter $\mathbf{v}$, and for any $p \in \mathbb{N}^* \cup \{\infty\}$, its ℓ_p-norm is written $\|\mathbf{v}\|_p$. The n-dimensional vector with all 1's is denoted by $\mathbf{1}_n$. All matrices are given using *row* vectors.

2.1 Cyclotomic fields

We denote the cyclotomic field of conductor m, $m \not\equiv 2 \mod 4$, by $K_m = \mathbb{Q}[\zeta_m]$, where ζ_m is a primitive m-th root of unity. It has degree $n = \varphi(m)$ and its discriminant, which is of order n^n, is given precisely by [Was97, Pr. 2.7]:

$$\varDelta_{K_m} = \left(-1\right)^{\varphi(m)/2} \frac{m^{\varphi(m)}}{\prod_{p|m} p^{\varphi(m)/(p-1)}}. \tag{2.1}$$

The maximal order of K_m is $\mathcal{O}_{K_m} = \mathbb{Z}\left[\zeta_m\right]$ (see e.g. [Was97, Th. 2.6]).

In this paper, we consider *any* conductor $m > 1$ of the general prime factorization $m = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$, $m \not\equiv 2 \mod 4$, and let $q_i = p_i^{e_i}$ for all $i \in [\![1, t]\!]$. In particular, m has exactly t distinct prime divisors. Let G_m denote the Galois group of K_m, which can be explicited by [Was97, Th. 2.5]:

$$G_m = \left\{\sigma_s : \zeta_m \longmapsto \zeta_m^s;\ 0 < s < m, (s,m) = 1\right\} \simeq \left(\mathbb{Z}/m\mathbb{Z}\right)^\times.$$

In particular, we denote by $\sigma_s \in G_m$ the automorphism sending any m-th root of unity to its s-th power. For convenience, the automorphism induced by complex conjugation is written $\tau = \sigma_{-1}$.

The algebraic norm of $\alpha \in K_m$ is defined by $\mathcal{N}(\alpha) = \prod_{\sigma \in G_m} \sigma(\alpha)$, hence the absolute norm element in the integral group ring $\mathbb{Z}[G_m]$ is $N_m = \sum_{\sigma \in G_m} \sigma$.

Maximal real subfield. The maximal real subfield of K_m, denoted by K_m^+, is the fixed subfield of K_m under complex conjugation, i.e. $K_m^+ := K_m^{\langle\tau\rangle} = \mathbb{Q}\bigl(\zeta_m + \zeta_m^{-1}\bigr)$. Its maximal order is $\mathcal{O}_{K_m^+} = \mathbb{Z}\bigl[\zeta_m + \zeta_m^{-1}\bigr]$ (see e.g. [Was97, Pr. 2.16]).

By Galois theory, since $\langle\tau\rangle$ is a normal subgroup of G_m, the maximal real subfield of K_m is a Galois extension of $\mathbb{Q}$ with Galois group $G_m^+ := \mathrm{Gal}\bigl(K_m^+/\mathbb{Q}\bigr)$ isomorphic to $G_m/\langle\tau\rangle$. We will consistently identify G_m^+ with the following system of representatives modulo τ restricted to K_m^+:

$$G_m^+ = \bigl\{\sigma_s|_{K_m^+};\ 0 < s < \tfrac{m}{2}, (s,m) = 1\bigr\}.$$

Technically, each $\sigma_s|_{K_m^+} \in G_m^+$ extends in G_m to either σ_s or $\tau\sigma_s = \sigma_{-s}$. For simplicity, we always choose to lift $\sigma_s|_{K_m^+} \in G_m^+$ to $\sigma_s \in G_m$ and drop the restriction to K_m^+ which should be clear from the context. This slight abuse of notation appears to be very practical. For example, the corestriction $\mathrm{Cor}_{K_m/K_m^+}\bigl(\sigma_s|_{K_m^+}\bigr)$, defined as the sum of all elements of G_m that restricts to $\sigma_s|_{K_m^+}$, namely $\sigma_s + \tau\sigma_s$, is written using the much simpler expression $(1+\tau)\cdot\sigma_s$.

2.2 Real and relative class groups

Fractional ideals of K_m are written using gothic letters $\mathfrak{b}$. They form a multiplicative group $\mathcal{I}_m$ containing the normal subgroup $\mathcal{P}_m := \bigl\{\langle\alpha\rangle;\ \alpha \in K_m\bigr\}$ of principal ideals. The quotient group $\mathcal{I}_m/\mathcal{P}_m$ is called the *class group* of K_m and denoted by Cl_m. It is finite and its cardinal h_m is called the *class number* of K_m. For any ideal $\mathfrak{b} \in \mathcal{I}_m$, the class of $\mathfrak{b}$ in Cl_m is written $\bigl[\mathfrak{b}\bigr]$.

The integral group ring $\mathbb{Z}[G_m]$ acts naturally on $\mathcal{I}_m$; more precisely, for any element $\alpha = \sum_{\sigma\in G_m} a_\sigma\sigma \in \mathbb{Z}[G_m]$, and any $\mathfrak{b} \in \mathcal{I}_m$, $\mathfrak{b}^\alpha := \prod_{\sigma\in G_m}\sigma\bigl(\mathfrak{b}\bigr)^{a_\sigma}$. The class group and class number of the maximal real subfield K_m^+ are denoted respectively by Cl_m^+ and h_m^+. The relative norm map $\mathcal{N}_{K_m/K_m^+}$ induces an homomorphism from Cl_m to Cl_m^+, whose kernel is the so-called *relative class group*, written Cl_m^- and of cardinal the *relative class number* h_m^-. Hence, by construction, for any $\mathfrak{b}$ st. $\bigl[\mathfrak{b}\bigr] \in \mathrm{Cl}_m^-$, $\mathfrak{b}^{1+\tau} \cap K_m^+$ is principal. One important specificity of cyclotomic fields is that the real class group Cl_m^+ embeds into Cl_m *via* the natural inclusion map, which to each ideal class $\bigl[\mathfrak{b}\bigr] \in \mathrm{Cl}_m^+$ associates the ideal class $\bigl[\mathfrak{b}\cdot\mathcal{O}_{K_m}\bigr] \in \mathrm{Cl}_m$ [Was97, Th. 4.14]. Concretely, it implies that $h_m = h_m^+ \cdot h_m^-$ is the product of the plus part and the relative part of the class number.

Plus part and relative part of the class number. Generally, not much is known about the class number of a number field, and the analytic class number formula [Neu99, Cor. 5.11(ii)] allows to obtain a rough upper bound $h_m \le \tilde{O}\bigl(\sqrt{|\Delta_{K_m}|}\bigr)$.

In the case of cyclotomic fields though, the structure of the relative class group is better understood. Using analytic means, the relative class number has the following explicit expression [Was97, Th. 4.17]:

$$h_m^- = Qw \cdot \prod_{\chi\ \mathrm{odd}}\Bigl(-\tfrac{1}{2}B_{1,\chi}\Bigr), \tag{2.2}$$

m	$\varphi(m)$	h_m^+	m	$\varphi(m)$	h_m^+	m	$\varphi(m)$	h_m^+	m	$\varphi(m)$	h_m^+	m	$\varphi(m)$	h_m^+	m	$\varphi(m)$	h_m^+
225	120	1	213	140	1	205	160	2	203	168	1	460	176	1	416	192	1
231	120	1	219	144	1	352	160	1	215	168	1	552	176	1	448	192	1
244	120	1	285	144	1	400	160	1	245	168	1	209	180	1	576	192	1
248	120	4	296	144	1	440	160	5	261	168	1	217	180	1	612	192	1
308	120	1	304	144	1	492	160	1	392	168	1	279	180	1	672	192	1
372	120	1	380	144	1	528	160	1	516	168	1	297	180	1	275	200	1
396	120	1	432	144	1	600	160	1	588	168	1	235	184	1	375	200	1
384	128	1	444	144	1	660	160	1	267	176	1	564	184	1	500	200	1
201	132	1	540	144	1	243	162	1	345	176	1	291	192	1			
207	132	1	237	156	1	249	164	1	368	176	1	357	192	1			

TABLE 2.1 – Officially unpublished values of h_m^+ for some m with $\varphi(m) \leq 200$.

where $w = 2m$ if m is odd and $w = m$ if m is even, $Q = 1$ if m is a prime power and $Q = 2$ otherwise, and $B_{1,\chi}$ is defined by $\frac{1}{f}\sum_{a=1}^{f} a\cdot\chi(a)$ for any odd primitive character χ modulo m of conductor f dividing m. Computing this value is in practice very efficient, using adequate representations of Dirichlet characters.

The really hard part of cyclotomic class numbers computations is to obtain the plus part h_m^+, and relatively few are known. We will use the values from [Was97, Tab. §4], [Mil14, Th. 1.1 and 1.2] and [BFHP21, Tab. 1], consistently assuming the *Generalized Riemann Hypothesis* (GRH). We also provide in Tab. 2.1 58 officially unpublished values, easily obtained using SageMath v9.0 [Sag20], each in less than 3 hours on a Intel® Core™ i7-8650U @3.2GHz CPU.

The fact that the plus part of the class number seems so much smaller than the relative part is striking. On the theoretical side, Weber's conjecture claims that $h_{2^e}^+ = 1$ for any $e > 1$, and Buhler, Pomerance and Robertson [BPR04] argue, based on Cohen-Lenstra heuristics, that for all but finitely many pairs (p, e), where p is a prime and e is a positive integer, $h_{p^{e+1}}^+ = h_{p^e}^+$; hence, for prime power conductors, this conjecture claims that the plus part is asymptotically constant.

On the practical side, these conjectures are backed up by Schoof's extensive calculations [Sch03] in the prime conductor case, and by the above explicit values. In particular, under GRH, Miller proved Weber's conjecture up to $m = 512$, and we note that according to Schoof's table, $h_m^+ \leq \sqrt{m}$ holds for more than 96.6% of all prime conductors $m = p < 10000$.

Prime ideal classes generators. When picking a set of prime ideals in the algorithms of this paper, an important feature is that they generate the class group. In general, even assuming GRH, only a large bound on the norm of generators is known, indeed Bach proved [Bac90, Th. 4] that $\mathcal{N}(\mathfrak{L}_{\max}) \leq 12\ln^2|\varDelta_{K_m}|$, where $\mathfrak{L}_{\max}$ is the biggest ideal inside a generating set of Cl_m of minimum norm. In practice though, this bound seems very pessimistic [BDF08, §6].

On the other hand, as prime ideals belong to Cl_m^- only with probability roughly $1/h_m^+$, searching for generators of the *subgroup* Cl_m^- mechanically increases the provable upper bound on generators. More precisely, writing as $\mathfrak{L}_{\max}^-$ the biggest ideal of a generating set of Cl_m^-, Wesolowski proved [Wes18, Rem. 2] that $\mathcal{N}(\mathfrak{L}_{\max}^-) \leq \left(2.71 h_m^+ \cdot \ln|\varDelta_{K_m}| + 4.13\right)^2$.

Finally, we use the notation $h_{m,(\mathfrak{L}_1,\ldots,\mathfrak{L}_k)}$ to denote the cardinal of the subgroup of Cl_m generated by the k classes $\big[\mathfrak{L}_i\big]$, i.e. the determinant of the kernel of:

$$\mathfrak{f}_{\mathfrak{L}_1,\ldots,\mathfrak{L}_k} : \big(e_1,\ldots,e_k\big) \in \mathbb{Z}^k \longmapsto \prod_{1\leq i\leq k} \big[\mathfrak{L}_i\big]^{e_i} \in \mathrm{Cl}_m\,.$$

2.3 Logarithmic $\mathcal{S}$-embeddings

The idea of using $\mathcal{S}$-units instead of units for the cryptanalysis of id-SVP has been underlying the work of [PHS19], and explicitly formalized in [BR20]. We briefly introduce log-$\mathcal{S}$-unit lattices and discuss proper normalization by the Product Formula that was at the heart of the practical improvements of [BR20].

Places of the cyclotomic field K_m are usually split in two parts: the set $\mathcal{S}_\infty$ of *infinite* places can be identified with the (complex) embeddings of K_m into $\mathbb{C}$, up to conjugation; the set $\mathcal{S}_0$ of *finite* places is specified by the infinite set of prime ideals of K_m, each prime ideal $\mathfrak{p}$ inducing an embedding of K_m into its $\mathfrak{p}$-adic completion $K_{m,\mathfrak{p}}$. Hence, any place $v \in \mathcal{S}_\infty \cup \mathcal{S}_0$ induces an absolute value $|\cdot|_v$ on K_m, and Ostrowski's theorem for number fields [Nar04, Th. 3.3] shows that all possible absolute values on K_m are obtained in this way. Concretely, for $\alpha \in K_m$:

$$\forall \sigma \in \mathcal{S}_\infty, \quad |\alpha|_\sigma = \big|\sigma(\alpha)\big| \qquad \text{and} \qquad \forall \mathfrak{p} \in \mathcal{S}_0, \quad |\alpha|_\mathfrak{p} = p^{-v_\mathfrak{p}(\alpha)}, \tag{2.3}$$

where $v_\mathfrak{p}(\cdot)$ is the valuation of α at $\mathfrak{p}$ and $\langle p\rangle = \mathfrak{p} \cap \mathbb{Z}$. A remarkable fact is that all these absolute values are tied by the *Product Formula* [Nar04, Th. 3.5]:

$$\forall \alpha \in K_m, \qquad \prod_{v\in\mathcal{S}_\infty\cup\mathcal{S}_0} |\alpha|_v^{[K_{m,v}:\mathbb{Q}_v]} = 1. \tag{2.4}$$

The infinite part of this product is $\big|\mathcal{N}(\alpha)\big|$, as for $\sigma \in \mathcal{S}_\infty$, $K_{m,\sigma} = \mathbb{C}$ and $\mathbb{Q}_\sigma = \mathbb{R}$, so that $[K_{m,\sigma} : \mathbb{Q}_\sigma] = 2$. Similarly, for $\mathfrak{p} \in \mathcal{S}_0$, we have $|\alpha|_\mathfrak{p}^{[K_{m,\mathfrak{p}}:\mathbb{Q}_p]} = \mathcal{N}(\mathfrak{p})^{-v_\mathfrak{p}(\alpha)}$.

$\mathcal{S}$-unit group structure. Fix a finite set $\mathcal{S}$ of places; in this paper we shall consider that $\mathcal{S}$ *always* contains $\mathcal{S}_\infty$. The so-called $\mathcal{S}$-unit group of K_m, denoted by $\mathcal{O}^\times_{K_m,\mathcal{S}}$, is the multiplicative subgroup of K_m generated by all elements whose valuations are non zero only at the finite places of $\mathcal{S}$. Formally:

$$\mathcal{O}^\times_{K_m,\mathcal{S}} = \Big\{\alpha \in K_m;\ \langle\alpha\rangle = \prod_{\mathfrak{p}\in\mathcal{S}\cap\mathcal{S}_0} \mathfrak{p}^{v_\mathfrak{p}(\alpha)}\Big\} = \Big\{\alpha \in K_m;\ \prod_{v\in\mathcal{S}} |\alpha|_v^{[K_{m,v}:\mathbb{Q}_v]} = 1\Big\}.$$

Note that when $\mathcal{S} = \mathcal{S}_\infty$, we get the definition of the unit group $\mathcal{O}^\times_{K_m}$ as the multiplicative subgroup of elements of algebraic norm ± 1.

Theorem 2.1 (Dirichlet-Chevalley-Hasse [Nar04, Th. III.3.12, Cor.1]). *The $\mathcal{S}$-unit group is the direct product of the group of root of unity $\mu\big(\mathcal{O}^\times_{K_m}\big)$ and a free abelian group with $|\mathcal{S}|-1$ generators. There exists a fundamental system of $\mathcal{S}$-units $\varepsilon_1,\ldots,\varepsilon_{|\mathcal{S}|-1}$ st. any $\varepsilon \in \mathcal{O}^\times_{K_m,\mathcal{S}}$ uniquely writes as $\varepsilon = \mu\cdot\prod_{i=1}^{|\mathcal{S}|-1}\varepsilon_i^{k_i}$, where $\mu \in \big\langle \pm\zeta_m\big\rangle$ is a root of unity and $k_i \in \mathbb{Z}$.*

Log-$\mathcal{S}$-unit lattice. A fundamental ingredient of the proof of this theorem is to build an embedding of $\mathcal{O}_{K_m,\mathcal{S}}^{\times}$ into the real space of dimension $|\mathcal{S}|$, whose kernel is $\mu\big(\mathcal{O}_{K_m}^{\times}\big)$ and whose image is a lattice of dimension $\big(|\mathcal{S}|-1\big)$. This embedding is called the *logarithmic $\mathcal{S}$-embedding*, and its image is called the log-$\mathcal{S}$-unit lattice.

Several equivalent definitions of this logarithmic $\mathcal{S}$-embedding are acceptable for the proof. However, for cryptanalytic purposes, experimental evidence [BR20] suggests that it is crucial to use a properly normalized embedding for the decodability of the log-$\mathcal{S}$-unit lattice. Thus, we define [Nar04, §3, p.98]:

$$\mathrm{Log}_{\mathcal{S}}\, \alpha = \Big(\big[K_{m,v} : \mathbb{Q}_v\big] \cdot \ln|\alpha|_v \Big)_{v\in\mathcal{S}} = \Big(\big\{ \ln|\sigma(\alpha)| \big\}_{\sigma\in\mathcal{S}_\infty}, \big\{ -v_{\mathfrak{p}}(\alpha) \ln \mathcal{N}(\mathfrak{p}) \big\}_{\mathfrak{p}\in\mathcal{S}_0} \Big)$$

From the definition of $\mathcal{O}_{K_m,\mathcal{S}}^{\times}$, it is easy to see that $\mathbb{R}\otimes\mathrm{Log}_{\mathcal{S}}\, \mathcal{O}_{K_m,\mathcal{S}}^{\times}$ is included in the hyperplane orthogonal to $\mathbf{1}_{|\mathcal{S}|}$. Showing that its dimension is at least $|\mathcal{S}|-1$ is more involved.

A basis of the log-$\mathcal{S}$-unit lattice is given by the images $\mathrm{Log}_{\mathcal{S}}\, \varepsilon_i$ of the fundamental system of $\mathcal{S}$-units of Th. 2.1, as in [BR20, Eq. (2.7)]. Actually, we shall use later that for any maximal set of independent $\mathcal{S}$-units, their images under any logarithmic $\mathcal{S}$-embedding form a full rank sublattice of the corresponding log-$\mathcal{S}$-unit lattice. We have [BR20, Pr. 2.2 and Eq. (2.8)]:

$$\mathrm{Vol}\big(\mathrm{Log}_{\mathcal{S}}\, \mathcal{O}_{K_m,\mathcal{S}}^{\times}\big) = \sqrt{\tfrac{\varphi(m)}{2}} \cdot R_m h_{m,(\mathcal{S}\cap\mathcal{S}_0)} \cdot \prod_{\mathfrak{p}\in\mathcal{S}\cap\mathcal{S}_0} \ln \mathcal{N}(\mathfrak{p}), \tag{2.5}$$

where $h_{m,(\mathcal{S}\cap\mathcal{S}_0)}$ is the cardinal of the subgroup of Cl_m generated by the classes of the finite places of $\mathcal{S}$, and R_m is the regulator of K_m, i.e. the determinant of the square matrix obtained from the log-unit lattice $\mathrm{Log}_{\mathcal{S}_\infty}\, \mathcal{O}_{K_m}^{\times}$ by removing any column. Note that the $\sqrt{\cdot}$ part is due to the rank defect, and the other part is actually the $\mathcal{S}$-regulator of K_m (see e.g. [BR20, Pr. 2.2]), which could not be defined without the proper normalization due to the Product Formula.

As mentioned in [PHS19,BDPW20,BR20], a convenient trick in the context of the cryptanalysis of id-Svp is to consider an *expanded* version of the logarithmic $\mathcal{S}$-embedding, halving and repeating twice $\mathcal{S}_\infty$-coordinates, namely:

$$\overline{\mathrm{Log}}_{\mathcal{S}}\, \alpha = \Big(\big\{ \ln|\sigma(\alpha)|, \ln|\sigma(\alpha)| \big\}_{\sigma\in\mathcal{S}_\infty}, \big\{ [K_{m,\mathfrak{p}} : \mathbb{Q}_p] \cdot \ln|\alpha|_{\mathfrak{p}} \big\}_{\mathfrak{p}\in\mathcal{S}\setminus\mathcal{S}_\infty} \Big).$$

In particular, this reduces the volume of the log-$\mathcal{S}$-unit lattice, as shown by [BR20, Pr. 2.3]. In practice though, we did not observe any fundamental difference between the approximation factors obtained using $\mathrm{Log}_{\mathcal{S}}$ or $\overline{\mathrm{Log}}_{\mathcal{S}}$.

2.4 Hard problems in Number Theory

One of the most difficult classical step of the Approx-id-Svp algorithms proposed in [CDW17,PHS19,BR20,CDW21] is to find a solution to the ClDl defined below.

Problem 2.2 (Class Group Discrete Logarithm (ClDL)). Given a basis of prime ideals $\big\{\mathfrak{L}_1, \ldots, \mathfrak{L}_k\big\}$, and a challenge ideal $\mathfrak{b}$, find $\alpha \in K_m$ and integers $v_1, \ldots, v_k$ such that $\langle\alpha\rangle = \mathfrak{b} \cdot \prod_i \mathfrak{L}_i^{v_i}$, if this decomposition exists.

In this definition, we also ask for an *explicit* element α of the field, contrary to the definition of, e.g., [CDW17, Pr. 2]. Nevertheless, we note that in both quantum and classical worlds, the standard way to solve this problem boils down to computing $\mathcal{S}$-units, for $\mathcal{S}$ containing $\mathfrak{b}$ and the $\mathfrak{L}_i$'s, so that this explicit element is a byproduct of the resolution. Furthermore, put in this form it encompasses the well-known *Principal Ideal Problem* (PIP), using an empty set of ideals.

The *Shortest Generator Problem* (SGP) asks, from a generator α of a principal ideal, for the shortest generator α' such that $\langle\alpha\rangle = \langle\alpha'\rangle$. Similarly, we define:

Problem 2.3 (Shortest Class Group Discrete Logarithm (S-ClDL)). Given a solution $\langle\alpha\rangle = \mathfrak{b} \cdot \prod_i \mathfrak{L}_i^{v_i}$ to the ClDL problem, find $w_1, \ldots, w_k \in \mathbb{Z}_{\geq 0}$ and $\alpha' \in K_m$ such that $\langle\alpha'\rangle = \mathfrak{b} \cdot \prod_i \mathfrak{L}_i^{w_i}$ and α' is the smallest possible one.

The condition for the w_i's to be positive is crucial. Note that all recent algorithms for Approx-id-SVP that are not bound to principal ideals eventually output an approximate solution of the S-ClDL [CDW21,PHS19,BR20]. Also, if the set of prime ideals is sufficiently large wrpt. $\mathfrak{b}$, then S-ClDL is exactly id-SVP.

We also mention the Close Principal Multiple (CPM) problem which, given an ideal $\mathfrak{b}$, asks to find $\mathfrak{c}$ such that $\mathfrak{bc}$ is principal and $\mathcal{N}(\mathfrak{c})$ is small. This specific problem is used in [CDW21], and the authors prove that under GRH and using a factor base containing all prime ideals of norm up to $m^{4+o(1)}$, there exists a solution $\mathfrak{c}$ with $\mathcal{N}(\mathfrak{c}) \leq \exp\big(\tilde{O}(m^{1+o(1)})\big)$ [CDW21, §1.3.4].

Complexities. As shown in [BS16], class groups, unit groups, class group discrete logarithms and principal ideal generator computations can be reduced to $\mathcal{S}$-units computations for appropriate sets of places $\mathcal{S}$. Thus, we are mostly interested in the running time $\mathrm{T}_{\mathsf{Su}}(K_m)$ of $\mathcal{S}$-unit groups computations in K_m.

Under GRH, in a quantum setting, $\mathrm{T}_{\mathsf{Su}}(K_m) = \tilde{O}(\ln|\Delta_{K_m}|)$ is polynomial in the degree of K_m, using generalizations of Shor's algorithm from [EHKS14,BS16]. On the other hand, in a classical setting, $\mathrm{T}_{\mathsf{Su}}(K_m) = \exp\tilde{O}(\ln^{1/2}|\Delta_{K_m}|)$ is subexponential in the degree of the cyclotomic field K_m, by [BEF+17].

2.5 Lattices

Let L be a Euclidean lattice of full rank n. The first minimum $\lambda_1(L)$ of L is defined as the ℓ_2-norm of the smallest vector $\mathbf{v} \in L$, and the ℓ_2 distance from $\mathbf{t}$ to L, for any $\mathbf{t}$ in the span $L \otimes \mathbb{R}$ of L, is defined by $\mathrm{dist}_2(L, \mathbf{t}) = \min_{\mathbf{v}\in L} \|\mathbf{t} - \mathbf{v}\|_2$.

The *Approximate Shortest Vector Problem* (Approx-SVP) is, given a lattice L and an approximation factor af, to find $\mathbf{v} \in L$ such that $\|\mathbf{v}\|_2 \leq \mathrm{af} \cdot \lambda_1(L)$. Similarly, the *Approximate Closest Vector Problem* (Approx-CVP) asks, given a lattice L, an approximation factor af and a target $\mathbf{t}$ in the span $L \otimes \mathbb{R}$ of L, for a vector $\mathbf{v} \in L$ such that $\|\mathbf{t} - \mathbf{v}\|_2 \leq \mathrm{af} \cdot \mathrm{dist}_2(L, \mathbf{t})$. A practical Approx-CVP oracle is given by Babai's Nearest Plane algorithm [Bab86].

Bounding approximation factors. An ideal lattice of K_m is the full-rank image under the Minkowski embedding in $\mathbb{R}^{\varphi(m)}$ of a fractional ideal $\mathfrak{b}$ of K_m. Unlike generic lattices, a lower bound of the first minimum is implied by the arithmetic-geometric mean inequality, using that for any $b \in \mathfrak{b}$, $\mathcal{N}(\mathfrak{b})$ divides $|\mathcal{N}(b)|$. Thus:

$$\sqrt{n} \cdot \mathcal{N}(\mathfrak{b})^{1/n} \leq \lambda_1(\mathfrak{b}) \leq \sqrt{n} \cdot \mathcal{N}(\mathfrak{b})^{1/n} \sqrt{|\Delta_{K_m}|}^{1/n}, \tag{2.6}$$

where $n = \varphi(m) = \deg K_m$ and the right inequality is Minkowski's inequality. Actually, the Gaussian Heuristic applied to ideal lattices gives that on average, $\lambda_1(\mathfrak{b}) \approx \sqrt{\frac{n}{2\pi e}} \cdot \mathrm{Vol}^{1/n}(\mathfrak{b})$, where $\mathrm{Vol}(\mathfrak{b}) = \mathcal{N}(\mathfrak{b})\sqrt{|\Delta_{K_m}|}$.

For any $\mathbf{x} \in \mathfrak{b}$, let $\mathrm{af}(\mathbf{x}) = \|\mathbf{x}\|_2/\lambda_1(\mathfrak{b})$ denote the approximation factor reached by $\mathbf{x}$ wrpt the SVP in the ideal lattice $\mathfrak{b}$. In general, $\lambda_1(\mathfrak{b})$ is not known, but Eq. (2.6) imply the bounds $\mathrm{af}_{\mathsf{inf}}(\mathbf{x}) \leq \mathrm{af}(\mathbf{x}) \approx \mathrm{af}_{\mathsf{gh}}(\mathbf{x}) \leq \mathrm{af}_{\mathsf{sup}}(\mathbf{x})$, where:

$$\begin{gathered} \mathrm{af}_{\mathsf{inf}}(\mathbf{x}) := \frac{\|\mathbf{x}\|_2}{\sqrt{n} \cdot \mathrm{Vol}^{1/n}(\mathfrak{b})}, \qquad \mathrm{af}_{\mathsf{sup}}(\mathbf{x}) := \frac{\|\mathbf{x}\|_2}{\sqrt{n} \cdot \mathcal{N}(\mathfrak{b})^{1/n}}, \\ \mathrm{af}_{\mathsf{gh}}(\mathbf{x}) := \sqrt{2\pi e} \cdot \mathrm{af}_{\mathsf{inf}}(\mathbf{x}). \end{gathered} \tag{2.7}$$

We will mostly compare to the Gaussian Heuristic, which seems to give very realistic estimations when the exact id-SVP is solvable.

Quality of a lattice basis. Several indicators have been used in the litterature to attempt to measure the quality of a lattice basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ wrpt the SVP or the CVP. We will focus on the following three standard quantities:

1. the root-Hermite Factor $\delta_0(B)$, defined by $\delta_0^n(B) = \|\mathbf{b}_1\|_2/\mathrm{Vol}^{1/n} B$, is commonly used to compare lattice reduction algorithms like LLL [LLL82] or BKZ [CN11]. On average, LLL reaches $\delta_0 \approx 1.022$ [GN08] whereas BKZ with blocksize $b \geq 50$ heuristically yields $\delta_0 \approx \left(\frac{b}{2\pi e}(\pi b)^{1/b}\right)^{1/(2b-2)}$ [Che13].
2. the (normalized) orthogonality defect $\delta(B)$, given by $\delta^n(B) = \prod_i \left(\frac{\|\mathbf{b}_i\|_2}{\mathrm{Vol}^{1/n} B}\right)$ [MG02, Def. 7.5] involves all vectors of the basis. By Minkowski's second theorem, its smallest possible value is upper bounded by $\sqrt{1 + \frac{n}{4}}$.
3. the logarithms of the norms of *Gram-Schmidt Orthogonalization* (GSO) vectors $\mathbf{b}_i^\star$ give also valuable information. For example, a rapid decrease in the sequence $\ln\|\mathbf{b}_i^\star\|_2$ at $i \geq 2$ indicates that $\mathbf{b}_i$ is rather not orthogonal to the previously generated subspace $\langle \mathbf{b}_1, \ldots, \mathbf{b}_{i-1} \rangle$.

3 An explicit full-rank family of S-units, or exceptional sets of algebraic elements in cyclotomic fields

In this section, we exhibit a full rank family of *independent* $\mathcal{S}$-units, where the finite places $\mathcal{S}$ correspond to a collection of full Galois orbits of split prime ideals. As mentioned in introduction, this family is composed of three parts. After a technical part on useful subsets of $[\![1, m]\!]$ (§3.1), we detail these three parts:

1. Circular units are given in §3.2 using the material from [Kuč92, Th. 6.1];
2. Stickelberger generators are given in §3.3, sticking to the exposition of [BK21];
3. Real $\mathcal{S}^+$-units (apart from real units), where $\mathcal{S}^+ = \mathcal{S} \cap K_m^+$, are in §3.4.

The index of our family in the full $\mathcal{S}$-unit group is proven in §3.5 and the 2-saturation process used to mitigate this index is described in §3.6.

3.1 Two special subsets of $[\![1, m]\!]$

We recall here from resp. [Kuč92, p.293] and [BK21, Eq. (11)] the definition of two subsets M_m^+ and M_m' of $[\![1, m]\!]$ that are useful to describe resp. a fundamental family of circular units and a short $\mathbb{Z}$-basis of the Stickelberger ideal of K_m.

Recall that m has prime factorization $m = q_1 q_2 \cdots q_t \not\equiv 2 \mod 4$, where $q_i = p_i^{e_i} > 2$ for $i \in [\![1, t]\!]$. Let X_m be the set of all positive integers $a < m$ that are either divisible by q_i or relatively prime to q_i for each $i \in [\![1, t]\!]$, i.e. :

$$X_m = \left\{ a \in \mathbb{Z};\ 0 < a < m, \left(a, \tfrac{m}{(a,m)}\right) = 1 \right\}.$$

Let $M_m^{\pm} \subseteq X_m$ be the sets of all $a \in X_m$ satisfying ([Kuč92, p.293]):[4]

- for all $i \in [\![1, t]\!]$, if $q_i \nmid a$ then $a \not\equiv -(a, m) \mod q_i$,
- if $a \nmid m$, let $k = \max\{i \in [\![1, t]\!];\ a \not\equiv (a, m) \mod q_i\}$, then $\left\{ \frac{a}{(a,m) q_k} \right\} < \frac{1}{2}$,
- if $a \mid m$ then the set $\{i \in [\![1, t]\!];\ q_i \nmid a\}$ has an even (resp. odd) number of elements when defining M_m^+ (resp. when defining M_m^-).

Finally, the set M_m' is defined from the previous set M_m^- using [BK21, Eq. (11)]:

$$M_m' = \left\{ a \in M_m^-;\ \forall i \in [\![1, t]\!], \tfrac{m}{q_i} \nmid a \right\} \cup \left(\bigcup_{i=1}^{t} \left\{ \tfrac{mb}{q_i};\ 1 \le b \le \tfrac{\varphi(q_i)}{2} \right\} \right). \tag{3.1}$$

Note that M_m^+ (resp. M_m') contains $\frac{\varphi(m)}{2} - 1$ elements (resp. $\frac{\varphi(m)}{2}$ elements). Both sets are obviously easy to compute, using only simple arithmetic criteria.

3.2 Circular units

Circular units are sometimes called *cyclotomic units* in the litterature, as in [Was97, §8]. We prefer to use the historical terminology from algebraic number theory, see e.g. Sinnott [Sin78, §4] and Kučera [Kuč92, §2], in order to avoid any confusion with the whole unit group $\mathcal{O}_{K_m}^\times$ of the m-th cyclotomic field.

Definition 3.1 (Circular units [Was97, §8.1]). *Let V_m be the multiplicative subgroup of $K_m^\times$ generated by $\{1 - \zeta_m^a;\ 1 \le a \le m\}$. The group of* circular units *is the intersection $C_m := V_m \cap \mathcal{O}_{K_m}^\times$.*

Note that V_m contains the torsion of K_m, since $-\zeta_m = (1 - \zeta_m)/(1 - \zeta_m^{-1})$. The circular units form a subgroup of $\mathcal{O}_{K_m}^\times$ of finite index, more precisely:

Proposition 3.2 ([Sin78, Th. p.107]). *The index of C_m in $\mathcal{O}_{K_m}^\times$ is finite:*

$$\left[\mathcal{O}_{K_m}^\times : C_m\right] = 2^b \cdot h_m^+, \qquad \text{with } b = \begin{cases} 0 & \text{if } t = 1, \\ 2^{t-2} + 1 - t & \text{else.} \end{cases}$$

Hence, circular units actually provide a very large subgroup of $\mathcal{O}_{K_m}^\times$: indeed, as noted in §2.2, the real part of the class number is expected to be small, and the other factor grows at most linearly in m.

[4] Actually, the set M_+ defined in [Kuč92, p.293] is $M_+ = M_m^+ \cup \{0\}$.

An explicit system of fundamental circular units for any m has been given in [GK89] and independently in [Kuč92, Th. 6.1]. More precisely, for $0 < a < m$, define the following special circular units, where $m_i = m/p_i^{e_i}$ [Kuč92, p.176]:

$$v_a = \begin{cases} 1 - \zeta_m^a & \text{if } \forall i \in [\![1, t]\!],\ m_i \nmid a, \\ \dfrac{1 - \zeta_m^a}{1 - \zeta_m^{m_i}} & \text{else, for the unique } m_i \mid a. \end{cases} \tag{3.2}$$

Then, a system of fundamental circular units is given by the following theorem, where M_m^+ is defined in §3.1. In particular, it is very easy to compute.

Theorem 3.3 ([Kuč92, Th. 6.1]). *The set $\{v_a;\ v_a \in M_m^+\}$ is a system of fundamental circular units of K_m: for any circular unit $\eta \in C_m$, there exist uniquely determined $k(a) \in \mathbb{Z}$ and root of unity $\mu \in \langle \pm\zeta_m \rangle$ st. $\eta = \mu \cdot \prod_{a \in M_m^+} v_a^{k(a)}$.*

A crucial point for the cryptanalysis of id-Svp in [CDW21] is that the logarithmic embedding of these elements is short. Namely, expliciting the constants that appear in the proof of [CDW21, Lem. 3.5], we have for any $0 < a < m$:

$$\|\mathrm{Log}_{\mathcal{S}_\infty}(1 - \zeta_m^a)\|_2 \leq 1.32 \cdot \sqrt{m}. \tag{3.3}$$

3.3 Stickelberger generators

In this section, we use [BK21, Th. 3.1] to describe a short *basis* of the so-called Stickelberger ideal, viewed as a $\mathbb{Z}$-module. These Stickelberger short relations correspond to principal ideals whose generators are surprisingly easy to compute using Jacobi sums as in [BK21, §6]. Following Sinnott [Sin80], for all $a \in \mathbb{Z}$, let:

$$\theta_m(a) = \sum_{s \in (\mathbb{Z}/m\mathbb{Z})^\times} \left\{ -\frac{as}{m} \right\} \cdot \sigma_s^{-1} \in \mathbb{Q}[G_m], \tag{3.4}$$

and let N_m be the absolute norm element $N_m = \sum_{\sigma \in G_m} \sigma$. It is easy to check that $a \equiv b \mod m$ implies $\theta_m(a) = \theta_m(b)$ and that $\theta_m(a) + \theta_m(-a) = N_m$ whenever $m \nmid a$.

Definition 3.4 (Stickelberger ideal [Sin80, p.189]). *Let $\mathcal{S}'_m$ be the $\mathbb{Z}$-module of $\mathbb{Q}[G_m]$ generated by $\{\theta_m(a);\ 0 < a < m\} \cup \{\frac{1}{2} N_m\}$. The* Stickelberger ideal *of K_m is the intersection $\mathcal{S}_m = \mathcal{S}'_m \cap \mathbb{Z}[G_m]$.*

As in [CDW21], we shall refer to the *Stickelberger lattice* when $\mathcal{S}_m$ is viewed as a $\mathbb{Z}$-module. Note that in some references, like in [Was97, §6.2], the Stickelberger ideal is defined as the smaller ideal $\mathbb{Z}[G_m] \cap \theta_m(-1)\mathbb{Z}[G_m]$, which coincides with Def. 3.4 if and only if m is a prime power [Kuč86, Pr. 4.3].

Theorem 3.5 (Stickelberger's theorem [Sin80, Th. 3.1]). *The Stickelberger ideal $\mathcal{S}_m$ of K_m annihilates the class group of K_m. Hence, for any ideal $\mathfrak{b}$ of K_m and any $\alpha = \sum_{\sigma \in G_m} a_\sigma \sigma \in \mathcal{S}_m$, the ideal $\mathfrak{b}^\alpha = \prod_{\sigma \in G_m} \sigma(\mathfrak{b})^{a_\sigma}$ is principal.*

An outstanding point is that the proof of this important result is completely explicit, i.e. for any $\alpha \in \mathcal{S}_m$, and any fractional ideal $\mathfrak{b}$ of K_m, an explicit $\gamma \in K_m$ such that $\langle\gamma\rangle = \mathfrak{b}^\alpha$ is constructed. It appears that when α is a short element of $\mathcal{S}_m$, this explicit generator is efficiently computable.

We shall first exhibit a family of short elements of $\mathcal{S}_m$ and describe a short $\mathbb{Z}$-basis of the Stickelberger lattice. These results are taken from [BK21].

A large family of short Stickelberger elements. An element of the integral group ring $\mathbb{Z}[G_m]$ is called *short* if it is of the form $\sum_{\sigma\in G_m} a_\sigma\sigma \in \mathbb{Z}[G_m]$, where $a_\sigma \in \{0,1\}$ for all $\sigma \in G_m$. Short elements of $\mathcal{S}_m$ have been identified in [Sch08, Th. 9.3(i) and Ex. 9.3] in the prime conductor case, and the proof has been adapted to any conductor in [CDW21, Lem. 4.4] to prove the shortness of the following generating set:

$$W = \{w_a;\ a \in [\![2, m]\!]\}, \quad \text{with } w_a = \theta_m(1) + \theta_m(a-1) - \theta_m(a). \tag{3.5}$$

Note that using $\theta_m(a) + \theta_m(-a) = N_m$ when $m \nmid a$, we obtain $w_a = w_{m-a+1}$ whenever $1 < a < m$, and that $w_m = N_m$ using also $\theta_m(m) = 0$. Hence, W is the set $\{w_a;\ 2 \le a \le \lceil \frac{m}{2} \rceil\} \cup \{N_m\}$.

In order to find a short basis of the Stickelberger lattice for any conductor, it is necessary to extend this family to a much bigger set of elements as is done in [BK21, §3.1]. Knowing many short lattice vectors certainly helps to solve the Cvp, as noted in [DPW19, §4.1], so that this result is of independent interest.

Proposition 3.6 ([BK21, Pr. 3.1]). *Let a, $b \in \mathbb{Z}$ satisfying $m \nmid a$, $m \nmid b$ and $m \nmid (a+b)$. Then $\alpha = \theta_m(a) + \theta_m(b) - \theta_m(a+b)$ is a short element of $\mathcal{S}_m$. Moreover, $(1+\tau)\cdot\alpha = N_m$, so exactly one half of the coefficients of α are zeros.*

This family clearly encompasses $W \setminus \{N_m\}$. Note that the second part of the proposition specifies [CDW21, Lem. 4.4(3)]: for any $w \in W\setminus\{N_m\}$, it implies that the ℓ_2-norm of w, viewed as a vector in $\mathbb{Z}^{\varphi(m)} \simeq_{\mathbb{Z}} \mathbb{Z}[G_m]$, is *exactly* $\sqrt{\varphi(m)/2}$.

A short basis of the Stickelberger lattice. Only knowing a generating set of short elements as in [CDW21] is not necessarily sufficient. Indeed, working in some sublattice of possibly large index to solve the Cvp like in [CDW21, Cor. 2.2] could in practice arguably yield inferior approximation factors. Moreover, in order to best approach log-$\mathcal{S}$-units lattices, we need to capture the entire Stickelberger lattice, while still being able to compute and manipulate the corresponding explicit generators. Using a Hermite Normal Form computation, or a suitable LLL reduction, increases dramatically the height of the (possibly rational) generators coefficients and significantly hinder subsequent computations.

Hence, sticking to the exposition of [BK21, §3.2], we describe here how to extract a short basis of the Stickelberger lattice from the family of short elements of Pr. 3.6, using the set M'_m defined in §3.1.

Recall m has prime power factorization $m = q_1 \cdots q_t$ with $q_i = p_i^{e_i} > 2$. For any positive $b \in \mathbb{Z}$, define J_b as the set $\{i \in [\![1, t]\!];\ q_i \mid b\}$. Hence, $r_b = \prod_{i\in J_b} q_i$

is the maximal divisor of (b, m) such that $\left(r_b, \frac{m}{r_b}\right) = 1$. Let $J'_b = [\![1, t]\!] \setminus J_b$ be the set of indices i such that $q_i \nmid b$. If $b < m$, then $J'_b \neq \emptyset$ and $\alpha_m(b)$ is defined by:

1. If $J'_b = \{j\}$, then $b = c \cdot \frac{m}{q_j}$ for $0 < c < q_j$, and [BK21, Eq. (16) and (15)]:

$$\alpha_m(b) = \begin{cases} 2\theta_m\left(\frac{\varphi(q_j)\cdot m}{2\cdot q_j}\right) - \theta_m\left(\frac{\varphi(q_j)\cdot m}{q_j}\right) & \text{if } c = 1, \\ \theta_m\left(\frac{m}{q_j}\right) + \theta_m\left(b - \frac{m}{q_j}\right) - \theta_m(b) & \text{otherwise.} \end{cases}$$

2. If $\left|J'_b\right| > 1$, let $u = q_i$ for some $i \in J'_b$ and $v = \frac{m}{u r_b}$. Since $(u, v) = 1$, there exist $x, y \in \mathbb{Z}$ such that $ux + vy = 1$, and [BK21, Eq. (14)]:

$$\alpha_m(b) = \theta_m(bux) + \theta_m(bvy) - \theta_m(b).$$

It is shown in [BK21, Lem. 3.2] that these elements satisfy the conditions of Pr. 3.6. In particular, for any $b \in \mathbb{Z}$ such that $0 < b < m$, it implies $\alpha_m(b) \in \mathcal{S}_m$ is short and $(1 + \tau) \cdot \alpha_m(b) = N_m$. This leads to the following short basis.

Theorem 3.7 ([BK21, Th. 3.6]). *The set $\left\{\alpha_m(b);\ b \in M'_m\right\} \cup \left\{N_m\right\}$ is a $\mathbb{Z}$-basis of the Stickelberger lattice $\mathcal{S}_m$ of K_m having only short elements.*

We stress that when m is a prime, this basis coincides with the one given by [Sch08, Th. 9.3(i)] and with the set W in Eq. (3.5).

Effective Stickelberger generators using Jacobi sums. As previously mentioned, the proof of Th. 3.5 is explicit, i.e. for any $\alpha \in \mathcal{S}_m$ and any fractional ideal $\mathfrak{b}$ of K_m, it builds an explicit $\gamma \in K_m$ such that $\langle\gamma\rangle = \mathfrak{b}^\alpha$. When α is a short element from Pr. 3.6, it turns out γ has a simple expression using Jacobi sums. How to build such a generator can be derived from [Was97, §6.2], [Sin80, §3.1] or for these particular α's in [BK21, §5]. We only treat the split case here, but everything generalizes to any (unramified) prime (see [BK21, §5] for details).

Let $\ell \in \mathbb{Z}$ be a prime such that $\ell \equiv 1 \mod m$, and let $\mathfrak{L}$ be any fixed (split) prime ideal of K_m above ℓ, so that $\mathbb{F} = \mathcal{O}_{K_m}/\mathfrak{L}$ is the finite field with $\mathcal{N}(\mathfrak{L}) = \ell$ elements. Let $\chi_\mathfrak{L}$ be the m-th power Legendre symbol relatively to $\mathfrak{L}$, i.e. $\chi_\mathfrak{L} : \mathbb{F}^\times \to \langle\zeta_m\rangle$ is determined by the congruence $\chi_\mathfrak{L}(a) \equiv a^{(\ell-1)/m} \mod \mathfrak{L}$ for any $a \in \mathbb{F}^\times$, and extended as usual to $\mathbb{F}$ by setting $\chi_\mathfrak{L}(0) = 0$.[5] For any integer b, define the following Gauss sum [Sin80, Eq. (3.2)]:

$$g_\mathfrak{L}(b) = -\sum_{a\in\mathbb{F}} \chi_\mathfrak{L}^b(a)\zeta_\ell^a \quad \in K_{m\ell}. \tag{3.6}$$

This is the key element for the proof of Stickelberger's theorem. Since $\chi_\mathfrak{L}^m$ is trivial, $g_\mathfrak{L}(b)^m \in K_m$ [Was97, Lem. 6.4], and the famous Stickelberger factorization writes [Sin80, Eq. (3.4)] as $g_\mathfrak{L}(b)^m \cdot \mathcal{O}_{K_m} = \mathfrak{L}^{m\theta_m(b)}$. Applying this to elements $\alpha = \theta_m(a) + \theta_m(b) - \theta_m(a + b)$ of Pr. 3.6 yields:

$$\mathfrak{L}^{m\cdot\alpha} = \left(\frac{g_\mathfrak{L}(a)g_\mathfrak{L}(b)}{g_\mathfrak{L}(a+b)}\right)^m \cdot \mathcal{O}_{K_m}. \tag{3.7}$$

[5] Note that $\chi_\mathfrak{L}$ is the conjugate character of the character "ω^{-d}" used in [Was97, §6.2].

By [Was97, Cor. 6.3], the generator on the right hand side belongs to $\left(K_m^\times\right)^m$, so that the exponent m can actually be removed on both sides. By [Was97, Lem. 6.2(d)], using the hypothesis $m \nmid (a+b)$, the remaining quotient can be expressed as the Jacobi sum $\mathcal{J}_{\mathfrak{L}}(a,b)$, defined by [Was97, p.88]:

$$\mathcal{J}_{\mathfrak{L}}(a,b) = -\sum_{u\in\mathbb{F}} \chi_{\mathfrak{L}}^a(u)\chi_{\mathfrak{L}}^b(1-u) \quad \in K_m. \tag{3.8}$$

This discussion is summarized in the following proposition, taken from [BK21].

Proposition 3.8 ([BK21, Pr. 5.1]). *Let a, $b \in \mathbb{Z}$ be as in Pr. 3.6, i.e. such that $m \nmid a$, $m \nmid b$ and $m \nmid a+b$. Then for $\alpha = \theta_m(a)+\theta_m(b)-\theta_m(a+b)$ we have:*

$$\mathfrak{L}^\alpha = \mathcal{J}_{\mathfrak{L}}(a,b)\cdot \mathcal{O}_{K_m}.$$

When $\alpha = \alpha_m(c)$ for $c \in M'_m$, we shall write $\gamma^-_{\mathfrak{L},c}$ for the generator of $\mathfrak{L}^{\alpha_m(c)}$.

Using a discrete logarithm table for the elements $(1-u) \in \mathbb{F}^\times$ in the sum in Eq. (3.8), the computation, for a fixed prime $\mathfrak{L}$, of all Jacobi sums corresponding to the short basis $\left\{\alpha_m(b);\ b \in M'_m\right\}$ is very fast. As noted in [BK21, §5], the Galois group also acts on the involved Jacobi sums in a way that allows to replace some of the Jacobi sum computations by the application of a suitable automorphism. By contrast, computing directly the quotient of Eq. (3.7) in $K_{m\ell}$ would be rapidly intractable, even using sparse polynomials modulo $x^{m\ell}-1$ and replacing the division by the relation $\pm\ell = g_{\mathfrak{L}}(c)g_{\mathfrak{L}}(-c)$ [Was97, Lem. 6.1(b)].

Finally, as a direct consequence of [Was97, Lem. 6.1], all these Jacobi sums are ℓ-Weil numbers, i.e. for any a, b such that $m \nmid a$, $m \nmid b$, $m \nmid (a+b)$, they verify the Weil relation $\mathcal{J}_{\mathfrak{L}}(a,b)\overline{\mathcal{J}_{\mathfrak{L}}(a,b)} = \ell$. This implies $\left|\sigma\left(\mathcal{J}_{\mathfrak{L}}(a,b)\right)\right| = \sqrt{\ell}$ for all $\sigma \in G_m$, meaning that any of these elements is the *shortest* generator of its corresponding $\mathfrak{L}^\alpha$, where $\alpha = \theta_m(a)+\theta_m(b)-\theta_m(a+b)$.

On the rank of the Stickelberger lattice. A consequence of Th. 3.7 is that the Stickelberger lattice $\mathcal{S}_m$ only has rank $\varphi(m)/2+1$ in $\mathbb{Z}\left[G_m\right]$; in particular, it is not full rank, therefore it cannot be directly used as a lattice of class relations.

However, as noted in [CDW21, §4.3], the Stickelberger lattice modulo $(1+\tau)$ is a lattice of class relations for the relative class group, which we recall is the kernel of the relative norm map $\mathcal{N}_{K_m/K_m^+} : \mathrm{Cl}_m \to \mathrm{Cl}_m^+$. We shall follow a quite different exposition here, using Sinnott's formalism from [Sin78,Sin80].

Let $\mathcal{R}_m = \mathbb{Z}\left[G_m\right]$. For any submodule $M \subseteq \mathcal{R}_m$, the kernel of the multiplication by $(1+\tau)$ in M is denoted by M^-. In particular:

$$\mathcal{R}_m^- = \left\{\alpha \in \mathcal{R}_m;\ (1+\tau)\alpha = 0\right\} \quad \text{and} \quad \mathcal{S}_m^- = \left\{\alpha \in \mathcal{S}_m;\ (1+\tau)\alpha = 0\right\}.$$

Clearly, we have $\mathcal{R}_m^- = (1-\tau)\mathcal{R}_m$ and $(1-\tau)\mathcal{S}_m \subsetneq \mathcal{S}_m^-$. Let $\pi : \mathcal{R}_m \longrightarrow \mathcal{R}_m^-$ be the natural projection that associates $(1-\tau)\alpha \in \mathcal{R}_m^-$ to any $\alpha \in \mathcal{R}_m$. A basis of $\mathcal{R}_m^-$, as a $\mathbb{Z}$-module, is given by [Kuč86, Th. 3.1]:

$$\left\{\beta_s;\ 0 < s < \tfrac{m}{2}, (s,m) = 1\right\}, \quad \text{where } \beta_s = \pi\left(\sigma_s\right) = \sigma_s - \sigma_{-s}. \tag{3.9}$$

Hence, $\mathcal{R}_m^-$ is isomorphic, as a $\mathbb{Z}$-module, to $\mathbb{Z}^{\varphi(m)/2}$. Note that the map π defined above corresponds to the projection map $\mathcal{R}_m \to \mathcal{R}_m/\langle 1+\tau\rangle$ of [CDW21], as shown by the expression given in the proof of [CDW21, Lem. 4.6].

Theorem 3.9 **([Sin78, Th. p.107]).** *The index of $\mathcal{S}_m^-$ in $\mathcal{R}_m^-$ is finite:*

$$\left[\mathcal{R}_m^- : \mathcal{S}_m^-\right] = 2^a \cdot h_m^-, \quad \textit{where } a = \begin{cases} 0 & \textit{if } t = 1, \\ 2^{t-2} - 1 & \textit{if } t \geq 2. \end{cases}$$

In particular, $\mathcal{S}_m^-$ has full rank $\frac{\varphi(m)}{2}$ in $\mathcal{R}_m^-$. The restriction to the relative class group means that the action of $(1+\tau)$ factors through the projection in $\mathcal{S}_m^-$, hence $\mathcal{S}_m^-$ can be used as a lattice of class relations for G_m-orbits of Cl_m^-.

Remark 3.10. We note that the projected Stickelberger lattice $(1-\tau)\mathcal{S}_m$ used in [CDW21] is *strictly smaller* than $\mathcal{S}_m^- = \mathcal{S}_m \cap \mathcal{R}_m^-$. In fact, a consequence of the proof of Lem. 3.14 is that $\left[\mathcal{S}_m^- : (1-\tau)\mathcal{S}_m\right] = 2^{\varphi(m)/2-1}$.

3.4 Real $\mathcal{S}^+$-units

In previous works, obtaining a full rank lattice in $\mathbb{Z}[G_m]$ from $\mathcal{S}_m$ was done by the adjonction of $(1+\tau)\mathbb{Z}[G_m]$ [CDW17, Def. 2], which annihilates the relative class group Cl_m^-. The obtained $\mathcal{S}_m + (1+\tau)\mathbb{Z}[G_m]$, called *augmented* Stickelberger lattice, has full rank in $\mathbb{Z}[G_m]$ as shown in [CDW17, Lem. 2].

We generalize this result by considering the module of all real class group relations between relative norm ideals of ideals from the entire class group Cl_m. We stress that, as opposed to other modules like $\mathcal{S}_m^-$ or $\mathcal{S}_m + (1+\tau)\mathbb{Z}\left[G_m\right]$, these real class group relations will actually depend on the underlying prime ideals.

On one hand, this affects negatively the shortness of the obtained relation vectors: putting those in Hermite Normal Form, we shall see later that each relation, viewed as a vector of integer valuations, has ℓ_2-norm at most h_m^+. On the other hand, removing the constraint to belong to the relative class group brings a significant practical and theoretical gap: first, it allows to choose prime ideals of smallest possible norms, which as shown in [BR20, §3.3] or [CDW21, Th. 4.8] lowers in practice the obtained approximation factor; second, whereas prime ideals of norm at most Bach's bound are sufficient to generate the entire class group, prime generators for the *relative* class group are only proven to be of norm bounded by the *larger* bound $(2.71 \cdot h_m^+ \cdot \ln \Delta_{K_m} + 4.13)^2$ from [Wes18].

Lifting real class group relations. Let $\ell_1, \ldots, \ell_d$ be distinct prime integers satisfying $\ell_i \equiv 1 \mod m$, so that ℓ_i is split in K_m, for all i in $[\![1, d]\!]$. For each i, fix a prime ideal $\mathfrak{L}_i \mid \ell_i$ in K_m of norm ℓ_i, and let $\mathfrak{l}_i = \mathcal{N}_{K_m/K_m^+}\left(\mathfrak{L}_i\right) = \mathfrak{L}_i^{1+\tau} \cap K_m^+$ be the relative norm ideal of $\mathfrak{L}_i$. Since $\mathfrak{L}_i$ is a split prime ideal of K_m dividing ℓ_i, the ideal $\mathfrak{l}_i$ is a split prime ideal of K_m^+ of norm ℓ_i, and by Kummer-Dedekind's theorem we have $\mathfrak{l}_i \cdot \mathcal{O}_{K_m} = \mathfrak{L}_i^{1+\tau}$. This justifies the slight abuse of notation of writing $\mathfrak{l}_i^\sigma = \mathfrak{L}_i^{(1+\tau)\sigma} \cap K_m^+$, for any $\sigma \in G_m$.

We are interested in the real class group relations between all prime ideals in the G_m^+-orbits of the $\mathfrak{l}_i$, i.e. between the following prime ideals of K_m^+:

$$\left\{\mathfrak{l}_i^{\sigma_s};\ i \in [\![1,d]\!], 0 < s < \tfrac{m}{2}, (s,m) = 1\right\}. \tag{3.10}$$

The important point is, any class relation in K_m^+ between ideals from Eq. (3.10) translates to a class relation in K_m using repeatedly $\mathfrak{l}_i^{\sigma} \cdot \mathcal{O}_{K_m} = \mathfrak{L}_i^{(1+\tau)\sigma}$. More precisely, let $\big(r_1, \dots, r_d\big) \in \mathbb{Z}\big[G_m^+\big]^d$ represent a real class relation in K_m^+ between ideals $\left\{\mathfrak{l}_i^{\sigma_s}\right\}$ of Eq. (3.10), i.e., there exists $\gamma_r^+ \in K_m^+$ such that $\gamma_r^+ \mathcal{O}_{K_m^+} = \prod_{i=1}^d \mathfrak{l}_i^{r_i}$. Then, this relation lifts naturally to a class relation $\big((1+\tau)\cdot r_1, \dots, (1+\tau)\cdot r_d\big)$ in K_m between prime ideals in the G_m-orbits $\left\{\mathfrak{L}_i^{\sigma};\ i \in [\![1,d]\!], \sigma \in G_m\right\}$ as:

$$\gamma_r^+ \cdot \mathcal{O}_{K_m} = \prod_{i=1}^{d} \mathfrak{L}_i^{(1+\tau) r_i}. \tag{3.11}$$

Let $C^+_{\mathfrak{l}_1,\dots,\mathfrak{l}_d}$ denote the lattice of class relations between elements of all G_m^+-orbits of $\{\mathfrak{l}_i;\ i \in [\![1,d]\!]\}$. Concretely, it is the kernel of the following map:

$$\mathfrak{f}_{\mathfrak{l}_1,\dots,\mathfrak{l}_d} : \big(r_{i,s}\big)_{\substack{1 \le i \le d,\\ 0<s<m/2, (s,m)=1}} \in \mathbb{Z}^{d\cdot\frac{\varphi(m)}{2}} \longmapsto \prod_{i,s} \big[\mathfrak{l}_i^{\sigma_s}\big]^{r_{i,s}} \in \mathrm{Cl}_m^+ . \tag{3.12}$$

Using the canonical isomorphism of $\mathbb{Z}$-modules $\mathbb{Z}^{d\cdot\frac{\varphi(m)}{2}} \simeq_{\mathbb{Z}} \mathbb{Z}[G_m^+]^d$, the lattice of class relations $C^+_{\mathfrak{l}_1,\dots,\mathfrak{l}_d}$ may be viewed as a $\mathbb{Z}$-submodule of $\mathbb{Z}[G_m^+]^d$. Lifting all these relations back to K_m as in Eq. (3.11), we therefore obtain the submodule $(1+\tau)\cdot C^+_{\mathfrak{l}_1,\dots,\mathfrak{l}_d} \subseteq (1+\tau)\cdot\mathbb{Z}[G_m]^d$, that we shall call the lattice of *real class relations* between the G_m-orbits of $\{\mathfrak{L}_i;\ i \in [\![1,d]\!]\}$.

Remark 3.11. When $h_m^+ = 1$, $C^+_{\mathfrak{l}_1,\dots,\mathfrak{l}_d}$ is isomorphic to d copies of the integral group ring $\mathbb{Z}[G_m^+]$ and the lattice of real class relations is simply $(1+\tau)\cdot\mathbb{Z}[G_m]^d$.

Euclidean norm of real class relations. We now identify a real class group relation from $C^+_{\mathfrak{l}_1,\dots,\mathfrak{l}_d}$ to a vector in $\mathbb{Z}^{d\cdot\frac{\varphi(m)}{2}}$. In other words, we consider only the valuations of these relations on the G_m^+-orbits of the prime ideals $\mathfrak{l}_1, \dots, \mathfrak{l}_d$. Furthermore, $C^+_{\mathfrak{l}_1,\dots,\mathfrak{l}_d}$ is put in Hermite Normal Form, conveniently for the proof. Better bounds might be easily obtained using e.g. the LLL algorithm.

Proposition 3.12. *Suppose the lattice $C^+_{\mathfrak{l}_1,\dots,\mathfrak{l}_d}$ of real class relations is in HNF. Then, for all $\mathbf{w} \in C^+_{\mathfrak{l}_1,\dots,\mathfrak{l}_d} \subseteq \mathbb{Z}[G_m^+]^d$, we have $\|\mathbf{w}\|_2 \le \|\mathbf{w}\|_1 \le h_m^+$.*

This means that $(1+\tau)\cdot C^+_{\mathfrak{l}_1,\dots,\mathfrak{l}_d}$ can be used in the CDW algorithm instead of $(1+\tau)\cdot\mathbb{Z}[G_m]$, as we will see in §4, while still reaching the same asymptotic approximation factor as long as $h_m^+ \le O\big(\sqrt{\varphi(m)}\big)$. This slightly more restrictive hypothesis (see the discussion in §2.2) will be more than compensated by the fact that it removes the need for the $\mathfrak{l}_i$'s to be principal, which has a significant impact in practice on the algebraic norm of the chosen ideals, and thus on the final approximation factor reached in [CDW21, Alg. 6].

Proof. The image of the map $\mathfrak{f}_{\mathfrak{l}_1,\ldots,\mathfrak{l}_d}$ given in Eq. (3.12) is a subgroup of Cl_m^+, so the volume of its kernel $C^+_{\mathfrak{l}_1,\ldots,\mathfrak{l}_d}$ is at most h_m^+. By definition of the Hermite Normal Form,[6] $C^+_{\mathfrak{l}_1,\ldots,\mathfrak{l}_d}$ has diagonal elements $h_1, \ldots, h_{\varphi(m)/2} > 0$, and the j-th column contains integers c_{ij} such that $0 \leq c_{ij} < h_j$ for $i < j$ and $c_{ij} = 0$ for $i > j$. We shall prove $h_i + \sum_{i<j} c_{ij} \leq h_i \cdot \prod_{i<j} h_j$ for any row of fixed index $i \in [\![1, \frac{\varphi(m)}{2}]\!]$, which yields the result. This is done by induction on the dimension, using repeatedly the fact that for any integers $x, y \geq 1$, $x + (y-1) \leq (xy)$. ☐

Explicit real generators. For each relation $r = \big(r_1, \ldots, r_d\big) \in C^+_{\mathfrak{l}_1,\ldots,\mathfrak{l}_d}$, we compute an explicit $\gamma_r^+ \in K_m^+ \subsetneq K_m$ that verifies Eq. (3.11). Together with the unit group $\mathcal{O}^\times_{K_m^+}$ of K_m^+, they form a fundamental system of $\mathcal{S}^+$-units, where the finite places of $\mathcal{S}^+$ are the G_m^+-orbits of the relative norm ideals $\mathfrak{l}_i$.

In the next section, we shall see that adding the explicit Stickelberger generators of §3.3 to these real generators yields a maximal set of independent $\mathcal{S}$-units in the degree $\varphi(m)$ cyclotomic field K_m, at the much smaller cost of computing a fundamental system of real $\mathcal{S}^+$-units in K_m^+ of degree only $\frac{\varphi(m)}{2}$.

In practice, though this remains the main bottleneck of our experimental setting, it allows us to push effectively our experiments up to degree $\varphi(m) = 184$, whereas the (full) $\mathcal{S}$-units computations of [BR20] were bound to $\varphi(m) = 70$.

3.5 A $\mathcal{S}$-unit subgroup of finite index

As in §3.4, let $\ell_1, \ldots, \ell_d$ be prime integers satisfying $\ell_i \equiv 1 \mod m$; for each i, fix a (split) prime ideal $\mathfrak{L}_i \mid \ell_i$ in K_m and let $\mathfrak{l}_i = \mathfrak{L}_i \cap K_m^+$. Let $\mathcal{S}$ be a set of places containing, apart the infinite places of K_m, all G_m-orbits of the $\mathfrak{L}_i$'s. Combining the results of §3.2, §3.3 and §3.4, we get the following family of $\mathcal{S}$-units:

$$\mathfrak{F} = \big\{v_a;\ a \in M_m^+\big\} \cup \big\{\gamma^-_{\mathfrak{L}_i,b};\ i \in [\![1,d]\!], b \in M'_m\big\} \cup \big\{\gamma_r^+;\ r \in C^+_{\mathfrak{l}_1,\ldots,\mathfrak{l}_d}\big\} \quad (3.13)$$

where the first set is the set of *circular units* given by Th. 3.3, the second is the set of explicit *Stickelberger generators* given by Pr. 3.8 and the last one is the set of *real generators* as in Eq. (3.11).

This family has $\big(\varphi(m)/2-1\big)+d\cdot\varphi(m)$ elements, which matches precisely the multiplicative rank of the full $\mathcal{S}$-unit group modulo torsion $\mathcal{O}^\times_{K_m,\mathcal{S}}/\mu\big(\mathcal{O}^\times_{K_m}\big)$.[7] In this section, we prove that these $\mathcal{S}$-units are indeed independent and explicit the index of the subgroup of $\mathcal{O}^\times_{K_m,\mathcal{S}}$ they generate.

Theorem 3.13. *Let $h_{m,(\mathfrak{L}_1,\ldots,\mathfrak{L}_d)}$ (resp. $h^+_{m,(\mathfrak{l}_1,\ldots,\mathfrak{l}_d)}$) be the cardinal of the subgroup of Cl_m (resp. Cl_m^+) generated by the G_m-orbits of $\mathfrak{L}_1, \ldots, \mathfrak{L}_d$ (resp. the G_m^+-orbits of $\mathfrak{l}_1, \ldots, \mathfrak{l}_d$). The family $\mathfrak{F}$ given in Eq. (3.13) is a maximal set of independent $\mathcal{S}$-units. The subgroup generated by $\mathfrak{F}$ in $\mathcal{O}^\times_{K_m,\mathcal{S}}/\mu\big(\mathcal{O}^\times_{K_m}\big)$ has index:*

$$\left(\frac{h_m \cdot h^+_{m,(\mathfrak{l}_1,\ldots,\mathfrak{l}_d)}}{h_{m,(\mathfrak{L}_1,\ldots,\mathfrak{L}_d)}}\right) \cdot 2^b \cdot \big(h_m^-\big)^{d-1} \cdot \Big(2^{\frac{\varphi(m)}{2}-1} \cdot 2^a\Big)^d,$$

[6] In this proof, we consider an upper-triangular HNF with row vectors.

[7] Note that for our purpose, the torsion units play no role and can thus be put aside.

where $a = b = 0$ if m is a prime power, and $a = 2^{t-2} - 1$, $b = 2^{t-2} + 1 - t$ whenever m has t distinct prime divisors.

Note that when the G_m-orbits of the $\mathfrak{L}_i$'s generate Cl_m, the first term in this index equals h_m^+. As we shall see in §3.6, the powers of 2 can be killed by standard saturation techniques, so the real problem comes from the $(h_m^-)^{d-1}$ part, which has generically *huge* prime factors. Intuitively, this comes from the fact that the Stickelberger relations miss all class group relations that exist between two (or more) distinct G_m-orbits.

First, we show that the lattice obtained by adding one copy of the Stickelberger ideal per G_m-orbit, to the lattice $(1+\tau) \cdot C^+_{\mathfrak{l}_1,\dots,\mathfrak{l}_d}$ of real class relations, yields a full-rank submodule of $\mathbb{Z}[G_m]^d$. Hence, we have obtained a full-rank lattice of class relations for the union of all G_m-orbits above $\ell_1, \dots, \ell_d$.

We begin by restricting our attention to the case $d = 1$. We need the following lemma, which extends and proves an observation already made in [DPW19, Rem. 3] in the prime conductor case:

Lemma 3.14. *The index of $\mathcal{S}_m + (1+\tau)\cdot\mathbb{Z}[G_m^+]$ in $\mathbb{Z}[G_m]$ is finite:*

$$\big[\mathbb{Z}[G_m] : \mathcal{S}_m + (1+\tau)\cdot\mathbb{Z}[G_m^+]\big] = 2^{\varphi(m)/2-1}\cdot 2^a \cdot h_m^-,$$

where $a = 0$ if $t = 1$ and $a = 2^{t-2} - 1$ else, where m has t prime divisors.

Proof. The proof is due to R. Kučera. First, note that $(1+\tau)\cdot\mathbb{Z}[G_m]$ contains N_m, hence by Th. 3.7, $\mathcal{S}_m + (1+\tau)\cdot\mathbb{Z}[G_m^+]$ is generated by the following $\varphi(m)$ elements:

$$\big\{\alpha_m(b);\ b \in M'_m\big\} \cup \big\{(1+\tau)\sigma_s;\ 0 < s < \tfrac{m}{2}, (s,m) = 1\big\}.$$

Therefore, its index is given by the absolute value of the determinant of the transition matrix from the canonical basis of $\mathbb{Z}[G_m]$ to the above generating set:

$$\big[\mathbb{Z}[G_m] : \mathcal{S}_m + (1+\tau)\cdot\mathbb{Z}[G_m^+]\big] = \left|\det\begin{pmatrix} \multicolumn{5}{c}{\Big\{a_{b,s}\Big\}_{\substack{b\in M'_m\\ 0<s<m,\,(s,m)=1}}} \\ \hline & & 1 \quad 1 & & \\ & \iddots & & \ddots & \\ 1 & & & & 1 \end{pmatrix}\right|,$$

where for any $b \in M'_m$, we write $\alpha_m(b) = \sum_{\sigma_s\in G_m} a_{b,s}\sigma_s$. Subtracting suitable combinations of rows of the lower half of this matrix to rows of the upper half to cancel the upper right block, this is the absolute value of the determinant of the square matrix of dimension $\frac{\varphi(m)}{2}$ with coefficients $\big\{a_{b,s} - a_{b,-s}\big\}$, for $b \in M'_m$ and s prime with m such that $0 < s < \frac{m}{2}$. By Pr. 3.6, we have $a_{b,s} + a_{b,-s} = 1$, which implies that $a_{b,s} - a_{b,-s} = 2a_{b,s} - 1$. Therefore, we recognize the matrix appearing at the very end of the proof of [BK21, Cor. 4.1] with each coefficient being multiplied by 2. Combining this with [BK21, Eq. (26)], we obtain:

$$\big[\mathbb{Z}[G_m] : \mathcal{S}_m + (1+\tau)\cdot\mathbb{Z}[G_m^+]\big] = 2^{\frac{\varphi(m)}{2}}\cdot\tfrac{1}{2}\big[\mathcal{R}_m^- : \mathcal{S}_m^-\big],$$

and the result follows from Th. 3.9. ∎

When $h_m^+ = 1$, the lattice of real class relations is always $(1+\tau)\cdot\mathbb{Z}[G_m^+]$, and Lem. 3.14 gives the whole story. In the general case $h_m^+ \neq 1$, we deduce:

Lemma 3.15. *Let ℓ be a prime integer that splits in K_m, let $\mathfrak{L} \mid \ell$ in K_m and let $\mathfrak{l} = \mathfrak{L}^{1+\tau} \cap K_m^+$. Let $h_{m,(\mathfrak{l})}^+$ be the cardinal of the subgroup of Cl_m^+ generated by the G_m^+-orbit of $\mathfrak{l}$ in K_m^+. The $\mathbb{Z}$-module generated by $\mathcal{S}_m$ and the lattice $(1+\tau)\cdot C_\mathfrak{l}^+$ of real class relations of the G_m-orbit of $\mathfrak{L}$, has finite index in $\mathbb{Z}[G_m]$:*

$$\big[\mathbb{Z}[G_m] : \mathcal{S}_m + (1+\tau)\cdot C_\mathfrak{l}^+\big] = 2^{\varphi(m)/2-1}\cdot 2^a \cdot h_m^- \cdot h_{m,(\mathfrak{l})}^+,$$

where $a = 0$ if $t = 1$ and $a = 2^{t-2}-1$ else, where m has t prime divisors.

Proof. By definition of $C_\mathfrak{l}^+$ as the kernel of the map $\mathfrak{f}_\mathfrak{l}$ of Eq. (3.12), we have:

$$\big[\mathbb{Z}[G_m^+] : C_\mathfrak{l}^+\big] = h_{m,(\mathfrak{l})}^+ = \big[(1+\tau)\cdot\mathbb{Z}[G_m^+] : (1+\tau)\cdot C_\mathfrak{l}^+\big].$$

Note also that N_m belongs to $(1+\tau)\cdot C_\mathfrak{l}^+ \subseteq (1+\tau)\cdot\mathbb{Z}[G_m^+]$, hence, again by means of transition matrix:

$$\big[\mathcal{S}_m + (1+\tau)\cdot\mathbb{Z}[G_m^+] : \mathcal{S}_m + (1+\tau)\cdot C_\mathfrak{l}^+\big] = \big[(1+\tau)\cdot\mathbb{Z}[G_m^+] : (1+\tau)\cdot C_\mathfrak{l}^+\big].$$

Finally, putting things together with Lem. 3.14, the result comes from:

$$\begin{aligned}\big[\mathbb{Z}[G_m] : \mathcal{S}_m + (1+\tau)\cdot C_\mathfrak{l}^+\big] &= \big[\mathbb{Z}[G_m] : \mathcal{S}_m + (1+\tau)\cdot\mathbb{Z}[G_m^+]\big]\\ &\quad\cdot\big[\mathcal{S}_m + (1+\tau)\cdot\mathbb{Z}[G_m^+] : \mathcal{S}_m + (1+\tau)\cdot C_\mathfrak{l}^+\big]\\ &= \big(2^{\varphi(m)/2-1}\cdot 2^a\cdot h_m^-\big)\cdot\big[\mathbb{Z}[G_m^+] : C_\mathfrak{l}^+\big].\end{aligned}$$ □

Finally, for the case where there are $d \geq 1$ orbits, a reasoning very similar to the proofs of Lem. 3.14 and 3.15 leads to:

Proposition 3.16. *Let $h_{m,(\mathfrak{l}_1,\ldots,\mathfrak{l}_d)}^+$ be the cardinal of the subgroup of Cl_m^+ generated by all G_m^+-orbits of $\mathfrak{l}_1,\ldots,\mathfrak{l}_d$. Then, the $\mathbb{Z}$-module generated by the lattice $(1+\tau)\cdot C_{\mathfrak{l}_1,\ldots,\mathfrak{l}_d}^+ \subseteq (1+\tau)\cdot\mathbb{Z}[G_m^+]^d$ of real class relations between the G_m-orbits of the $\mathfrak{L}_i$'s, and the diagonal block matrix of d copies of $\big(\mathcal{S}_m \setminus N_m\mathbb{Z}\big)$, verifies:*

$$\big[\mathbb{Z}[G_m]^d : \mathcal{S}_m^d + (1+\tau)\cdot C_{\mathfrak{l}_1,\ldots,\mathfrak{l}_d}^+\big] = \big(2^{\varphi(m)/2-1}\cdot 2^a\cdot h_m^-\big)^d\cdot h_{m,(\mathfrak{l}_1,\ldots,\mathfrak{l}_d)}^+.$$

Proof of Th. 3.13. The independence comes from Pr. 3.16 and the trivial fact that circular units are independent from Stickelberger and real generators. The index of the subgroup generated by $\mathfrak{F}$ in $\mathcal{O}_{K_m,\mathcal{S}}^\times/\mu\big(\mathcal{O}_{K_m}^\times\big)$ is given by:

$$\big[\mathcal{O}_{K_m}^\times : C_m\big]\cdot\frac{\big[\mathbb{Z}[G_m]^d : \mathcal{S}_m^d + (1+\tau)\cdot C_{\mathfrak{l}_1,\ldots,\mathfrak{l}_d}^+\big]}{\big|\det\big(\ker\mathfrak{f}_\mathcal{S}\big)\big|},$$

where $\ker\mathfrak{f}_\mathcal{S}$ is the lattice of all class group relations between finite places of $\mathcal{S}$. The first term is given by Pr. 3.2, the numerator of the second term is given by Pr. 3.16, and by definition of $\mathcal{O}_{K_m,\mathcal{S}}^\times$, the denominator is precisely $h_{m,(\mathfrak{L}_1,\ldots,\mathfrak{L}_d)}$. Rearranging terms adequately yields the result. □

3.6 Saturation

First, remark that the index given by Th. 3.13 is divisible by a large power of 2. In order to mitigate this exponential growth, we shall 2-saturate our sets.

Saturation is a standard tool of computational algebraic number theory used in various contexts like ($\mathcal{S}$-)units and class groups computations, which can be tracked back at least to [PZ89, §5.7]. In the following, we briefly describe the 2-saturation procedure and refer to e.g. [BFHP21, §4.3] for a formal exposition.

Recognizing squares. Let $U = \langle g_1, \ldots, g_k \rangle$ be a finitely generated multiplicative subgroup of $\mathcal{O}_{K_m,\mathcal{S}}^\times$. The first step of the 2-saturation process is to recognize squares in $U \cap (\mathcal{O}_{K_m,\mathcal{S}}^\times)^2$. This is done by using local information provided by quadratic characters.

Fix a prime $\mathfrak{p} \notin \mathcal{S}$ such that $\mathcal{N}(\mathfrak{p}) \equiv 1 \mod \operatorname{lcm}(m, 2)$. Define $\chi_\mathfrak{p}$ as the Legendre symbol such that $\chi_\mathfrak{p}(a) \equiv a^{(\mathcal{N}(\mathfrak{p})-1)/2} \mod \mathfrak{p}$ for any $a \in U$. As $\mathfrak{p} \notin \mathcal{S}$ and $a \in \mathcal{O}_{K_m,\mathcal{S}}^\times$, we have $\chi_\mathfrak{p}(a) \in \{-1, 1\}$. If a is a square, $\chi_\mathfrak{p}(a) = 1$ as a is still a square modulo $\mathfrak{p}$. The converse is not true, but by considering many characters $\chi_{\mathfrak{p}_1}, \ldots, \chi_{\mathfrak{p}_N}$ as above, it is expected that at least one of them evaluates to -1. Hence, recognizing squares boils down to compute the kernel of:

$$\begin{aligned} \log_{-1,\chi} : U &\longrightarrow \mathbb{F}_2^N \\ a &\longmapsto \big\{ \log_{-1} \chi_{\mathfrak{p}_i}(a);\ i \in [\![1, N]\!] \big\}. \end{aligned}$$

An element of this kernel is still not guaranteed to be a square. Nevertheless, a standard heuristic, first stated in the context of integer factorization [BLP93, §8] and also used in multiquadratic fields [BBV+17, §4.2], [BV18, H. 4.3], is to assume that if the $\mathfrak{p}_i$ are all distinct (split) prime ideals, then the $\log_{-1} \chi_{\mathfrak{p}_i}$ behave as independent uniform random elements of $\operatorname{Hom}\big(U / \big(U \cap (K_m^\times)^2\big), \mathbb{F}_2\big)$. Concretely, this means that these should span this dual with probability at least $\big(1 - 1/2^{N-k}\big)$ [BLP93, Lem. 8.2]; in that case, any element of the kernel of $\log_{-1,\chi}$ is indeed a square. In other words, if $\sum_{1 \le i \le k} v_i \log_{1,\chi} g_i = 0$, then with high probability the product $g = \prod_{1 \le i \le k} g_i^{v_i}$ indeed belongs to $U \cap (\mathcal{O}_{K_m,\mathcal{S}}^\times)^2$.

Square roots algorithm. Once we have identified combinations of elements of U that are $\mathcal{S}$-unit squares, it remains to compute their square roots explicitly.

First, we note that it is useful to systematically reduce those products modulo all squared circular units C_m^2 to contain the coefficients size. This is done as usual by projecting the logarithmic embedding $\operatorname{Log}_{\mathcal{S}_\infty} g$ of the obtained $g \in (\mathcal{O}_{K_m,\mathcal{S}}^\times)^2$ into $2 \cdot \operatorname{Log}_{\mathcal{S}_\infty} C_m$, finding a closest vector $y = \operatorname{Log}_{\mathcal{S}_\infty} u^2$ and replacing g by g/u^2.

The traditional method to compute the square root of an element $g \in (K_m^\times)^2$ is to factor the polynomial $x^2 - g$ in $K_m[x]$, using e.g. Trager's method [Coh93, Alg. 3.6.4] or Belabas' p-adic method [Bel04]. As, according to Th. 3.13, we have many square roots to compute, we choose instead to use a batch strategy in the spirit of [LPS20, Alg. 5] using complex embeddings approximations.

Since LLL seminal paper [LLL82], it is known that one can retrieve an algebraic number from approximations of one of its complex embeddings. Indeed, fix an embedding $\sigma \in G_m$ and a $\mathbb{Q}$-basis $\big(\omega_1, \ldots, \omega_n\big)$ of $\mathcal{O}_{K_m}$, and LLL-reduce:

$$B_\kappa := \begin{pmatrix} -\sigma(\omega_1) & C & 0 & \ldots & 0 \\ -\sigma(\omega_2) & 0 & C & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ -\sigma(\omega_n) & 0 & \ldots & 0 & C \end{pmatrix}.$$

where $C > 0$ is a constant and approximations are computed at precision $\kappa \in \mathbb{N}$. Then, for any $g \in \mathcal{O}_{K_m}$, applying e.g. Babai's Nearest Plane algorithm on the LLL basis of B_κ and target $\big(\sigma(g), 0, \ldots, 0\big)$ gives a combination $(g_1, \ldots, g_n)$ such that $g = \sum_{i=1}^{n} g_i \omega_i$. As explained in [LPS20], it is possible to mutualize the computation of B_κ and reuse the unitary transformation to hasten computations when increasing κ is required.

We use an improvement that benefits from the existence of the maximal real subfield K_m^+. Each $g \in K_m = K_m^+[\zeta_m]$ can be uniquely written as $g = g_0 + g_1 \cdot \zeta_m$, with $g_0, g_1 \in K_m^+$. For $\sigma \in G_m^+$, the *relative Minkowski embedding* of σ relatively to the extension K_m/K_m^+ is defined by $\sigma_{K_m/K_m^+}(g_0^\sigma, g_1^\sigma) = \big(g^\sigma, \overline{g^\sigma}\big) \in \mathbb{C}^2$. This is a linear homomorphism of $\mathbb{C}^2$. When $g = h^2$, its square root $h_0 + h_1\zeta_m$ can be retrieved from approximations of h_0^σ and h_1^σ instead of h^σ, as follows:

1. Compute $\sigma_{K_m/K_m^+}(g_0^\sigma, g_1^\sigma) = \big(g^\sigma, \overline{g^\sigma}\big) \in \mathbb{C}^2$;
2. Choose one complex square root z of g^σ and apply $\sigma^{-1}_{K_m/K_m^+}$ to $(z, \overline{z})$ to get potential approximations $\big(\tilde{h}_0^\sigma, \tilde{h}_1^\sigma\big)$ of h_0^σ and h_1^σ respectively;
3. Using LLL as above in K_m^+ on $\tilde{h}_0^\sigma$ and $\tilde{h}_1^\sigma$, obtain $\big(\tilde{h}_0, \tilde{h}_1\big)$ in K_m^+, which are candidates for resp. h_0 and h_1.
4. If $(\tilde{h}_0 + \tilde{h}_1 \cdot \zeta_m)^2 \neq g$, then increase κ using the fast method of [LPS20].

Hence, this method amounts to LLL reducing a matrix of size $\frac{n}{2} \times (\frac{n}{2} + 1)$ and decoding using e.g. Babai's Nearest Plane algorithm. This offers a great speed-up compared to reducing a $n \times (n+1)$ matrix. For further details and generalizations to higher order polynomial roots, we refer the interested reader to [Les21].

Rebuilding a basis. After the square root step, we obtain new elements $h_1, \ldots, h_r$, where $r = \dim\big(\ker \log_{-1,\chi}\big)$. To extract a set of k independent elements from the extended set $\big\{h_1, \ldots, h_r, g_1, \ldots, g_k\big\}$, we compute an LLL-basis of the matrix constituted of their valuations at the places of $\mathcal{S}$. Note that this matrix can be computed entirely from the valuations of the initial set $\{g_i\}$ and the basis of $\ker \log_{-1,\chi}$. Using the same trick as for matrix A in [BBV+17, Alg. 5.2], this contains the height of the transformation matrix, sufficiently for our needs.

After a few passes of this entire process we obtain a maximal set of independent $\mathcal{S}$-units of index given by Th. 3.13 where no factor 2 remains.

Remark 3.17. Note that this whole 2-saturation can easily be adapted to track any e-th power, using if necessary a generalized Montgomery's e-th root algoritm [Tho12, §3]. Though, the relative class number h_m^- in the index of Th. 3.13 hides *huge* prime factors that at first glance renders this strategy hopeless in general.

4 Quantum improvements of the CDW algorithm

The complete material for this section is given in §A, and the main points are briefly summarized here. The CDW algorithm for solving Approx-SVP was introduced in [CDW17] for cyclotomic fields of prime power conductors, and extended to all conductors in [CDW21]. Its main feature is the use of short relations of the Stickelberger ideal.

In this section, we show how to benefit from the results of §3.3 and §3.4 to remove most quantum steps of [CDW21]. More precisely, we first propose in §A.2 an equivalent rewriting of [CDW21, Alg. 7] that enlightens some hidden steps that reveal useful for subsequent modifications. Then, in §A.3, we plug the explicit generators of Pr. 3.8 and Eq. (3.11), for relative class group orbits, to remove the last call to the quantum PIP solver. Finally, by considering the module of *all* real class group relations like in Pr. 3.16, we remove in §A.4 the need of a random walk mapping any ideal of K_m into Cl_m^-, at the (small) price of restricting to cyclotomic fields such that $h_m^+ \leq O(\sqrt{m})$ (Hyp. A.1).

An equivalent rewriting of CDW (§A.2). Omitting details, the CDW algorithm works as follow, for any challenge ideal $\mathfrak{a}$ of K_m [CDW21, Alg. 7, 6 and 2]:

1. Random walk to Cl_m^-: find $\mathfrak{b}$ such that $\left[\mathfrak{a}\mathfrak{b}\right] \in \mathrm{Cl}_m^-$.
2. Solve the ClDL of $\mathfrak{a}\mathfrak{b}$ on G_m-orbits of the prime ideals $\mathfrak{L}_1, \ldots, \mathfrak{L}_d$ of Cl_m^-. This gives a vector $\alpha = (\alpha_1, \ldots, \alpha_d) \in \mathbb{Z}[G_m]^d$ such that $\mathfrak{a}\mathfrak{b} \cdot \prod_i \mathfrak{L}_i^{\alpha_i}$ is principal.
3. Solve the CPMP by projecting each α_i in $\pi(\mathcal{S}_m) = (1-\tau)\mathcal{S}_m$, find a close vector $v_i = y_i \cdot \pi(\mathcal{S}_m)$ and lift v_i to get some β_i st. $\pi(\beta_i) = v_i$, $\|\alpha - \beta\|_1$ is small *with positive coordinates*, and $\mathfrak{a}\mathfrak{b} \cdot \prod_i \mathfrak{L}_i^{\alpha_i - \beta_i}$ is principal.
4. Apply the PIP algorithm of [BS16] to get a generator of this principal ideal.
5. Reduce the obtained generator by circular units like in [CDPR16].

This eventually outputs $h \in \mathfrak{a}$ of length $\|h\|_2 \leq \exp\big(\tilde{O}(\sqrt{m})\big) \cdot \mathcal{N}(\mathfrak{a})^{1/\varphi(m)}$.

We focus on the lift procedure of Step 3. In [CDW21], a vector $v \in \pi(\mathcal{S}_m)$ is lifted to β by keeping positive coordinates for β_σ and sending opposite of negative coordinates to $\beta_{\tau\sigma}$. This works because for any $\mathfrak{c} \in \mathrm{Cl}_m^-$, $[\mathfrak{c}]^{-1} = [\mathfrak{c}^\tau]$, but hides which exact product of relative norm ideals is involved.

We propose a totally equivalent lift procedure: from $v = y \cdot \pi(\mathcal{S}_m)$, consider the preimage $\tilde{\beta} = y \cdot \mathcal{S}_m$, from which we remove $\min\big\{\tilde{\beta}_\sigma, \tilde{\beta}_{\tau\sigma}\big\}$ to each $\tilde{\beta}_\sigma$ coordinate to obtain β. Now, it is obvious that β is a combination y of relations in $\mathcal{S}_m$, and of relative norm relations given by the min part. Details are in Alg. A.6.

Using explicit Stickelberger generators (§A.3). Each element w_a of the generating set W of $\mathcal{S}_m$ corresponds to a generator $\mathcal{J}_{\mathfrak{L}}(1, a-1)$ as defined in Pr. 3.8. Similarly, each relative norm ideal writes $\langle \gamma_s^+ \rangle = \mathfrak{L}^{(1+\tau)\sigma_s}$ (see §3.4). Hence, from an (explicit) ClDL solution $\langle g \rangle = \mathfrak{a}\mathfrak{b} \cdot \mathfrak{L}^\alpha$, and given, as rewritten above, a CPMP solution $\beta = y \cdot W + u \cdot (1+\tau) \cdot \mathbb{Z}[G_m^+]$, we have that a generator of $\mathfrak{a}\mathfrak{b} \cdot \mathfrak{L}^{\alpha - \beta}$ is directly given by $g / \big(\prod_a \mathcal{J}_{\mathfrak{L}}(1, a-1)^{y_a} \prod_s (\gamma_s^+)^{u_s}\big)$. Knowing this allows to remove the quantum PIP in dimension n in step 4 (for each query). In exchange, we need to compute (only once) all real generators for relative norm relations, which can be done in dimension $\varphi(m)/2$ by [BS16, Alg. 2].

Avoiding the random walk (§A.4). Finally, note that several quantum steps are performed (for each query) in the random walk that maps ideals to Cl_m^-. Using the results of §3.4, we replace the module $(1+\tau)\cdot\mathbb{Z}[G_m]^d$ by the module of all real class group relations. Asymptotically, we prove that this does not change the bound on the approximation factor Pr. A.7, as long as we restrict to fields K_m with $h_m^+ \leq O(\sqrt{m})$ (Hyp. A.1). This tiny restriction is largely compensated by the fact that only two quantum steps remain: one is performed only once in dimension $\varphi(m)/2$ to compute real class group relations and generators, and the second is solving the ClDL for each query (see Tab. A.1).

5 Computing log-S-unit sublattices in higher dimension

Our main goal is to simulate the Tw-PHS algorithm for high degree cyclotomic fields. To this end, we compute full-rank sublattices of the full log-unit lattice using the knowledge of the maximal set $\mathfrak{F}$ of independent $\mathcal{S}$-units defined by Eq. (3.13) and its 2-saturated counterpart $\mathfrak{F}_{\mathsf{sat}}$ from §3.6. These sets are easily lifted from a complete set of real $\mathcal{S}^+$-units (see §3.4), hence at the classically subexponential cost of working in the half degree maximal real subfield. However, as by Th. 3.13 the index of these families grows rapidly as the number of orbits increases, this *degraded* mode only gives us a crude-but-reliable upper bound on the approximation factors that can be expected when using Tw-PHS.

The Tw-PHS algorithm is briefly recalled in §5.1, and our experimental setting detailed in §5.2. Then, we analyse in §5.3 the geometric characteristics of our log-$\mathcal{S}$-unit sublattices and the obtained approximation factors in §5.4.

5.1 The Twisted-PHS algorithm

The Tw-PHS algorithm [BR20] was introduced as an improvement of the PHS algorithm [PHS19]. Both aim at solving Approx-id-SVP in any number field and have the same theoretically proven bounds for running time and reached approximation factors. However, the explicit $\mathcal{S}$-units formalism in [BR20] lead to a proper normalization of the used log-$\mathcal{S}$-embedding, weighting coordinates according to finite places norms. This turned out to give experimentally significant improvements on the lattices decodability and on reached approximation factors.

Both algorithms are split in a *preprocessing phase*, performed only once for a fixed number field, and a *query phase*, for each challenge ideal. More precisely:

1. The preprocessing phase consists in choosing a set of finite places $\mathcal{S}$ generating the class group, computing the corresponding log-$\mathcal{S}$-unit lattice for an appropriate log-$\mathcal{S}$-embedding, and preparing the lattice for subsequent Approx-CVP requests using the Laarhoven's algorithm from [Laa16];
2. For each challenge ideal $\mathfrak{b}$, the query phase consists in first solving the ClDL wrpt. $\mathcal{S}$ to obtain $\langle\alpha\rangle = \mathfrak{b}\cdot\prod_{\mathfrak{L}\in\mathcal{S}}\mathfrak{L}^{v_\mathfrak{L}}$. Then, this element is projected into the span of the above log-$\mathcal{S}$-unit lattice, and a close vector of this lattice gives a $\mathcal{S}$-unit s st. α/s is hopefully small. Here, guaranteeing that $\alpha/s \in \mathfrak{b}$ is achieved by applying a drift parameterized by some β on the target.

In the Tw-PHS case, since the obtained lattice, after proper normalization, appears to have exceptionally good geometric characteristics, it was proposed to replace Laarhoven's algorithm by a lazy BKZ reduction in the preprocessing phase and Babai's Nearest Plane algorithm in the query phase [BR20, Alg. 4.2 and 4.3]. We will consider only this practical version in our experiments.

In details, for a number field K, the log-$\mathcal{S}$-unit lattice used in the Tw-PHS algorithm is defined as $\varphi_{\mathsf{tw}}(\mathcal{O}_{K,\mathcal{S}}^{\times})$, where φ_{tw} is the log-$\mathcal{S}$-embedding given by $f_H \circ \overline{\mathrm{Log}}_{\mathcal{S}}$ [BR20, Eq. (4.1)], for an isometry f_H from the span H of $\overline{\mathrm{Log}}_{\mathcal{S}}$ to $\mathbb{R}^k$, where k equals the multiplicative rank of $\mathcal{O}_{K,\mathcal{S}}^{\times}$ modulo torsion.

Among the consequences of the proper normalization induced by $\overline{\mathrm{Log}}_{\mathcal{S}}$, the authors showed how to optimally choose a set of finite places that generate the class group [BR20, Alg. 4.1]. Namely, taking ideals of increasing prime norms in the set $\mathcal{S}$, they noticed that the density of the associated (twisted) log-$\mathcal{S}$-unit lattice $\varphi_{\mathsf{tw}}(\mathcal{O}_{K,\mathcal{S}}^{\times})$ increases up to an optimal value before decreasing.

Finally, a tricky aspect of the resolution resides in guaranteeing that the output solution is indeed an element of the challenge ideal, i.e. that $v_{\mathfrak{L}}(\alpha/s) \geq 0$ for all $\mathfrak{L} \in \mathcal{S} \cap \mathcal{S}_0$. In [BR20], this is done by applying a drift vector in the span of the log-$\mathcal{S}$-unit lattice, parameterized by some β whose optimal value is searched using a dichotomic strategy in the query phase. Concretely [BR20, Eq. (4.7)]:

$$\mathbf{t} = f_H\left(\left\{\ln|\alpha|_\sigma - \frac{k\beta + \ln\mathcal{N}(\mathfrak{b}) - \sum_{\mathfrak{L}\in\mathcal{S}} \ln\mathcal{N}(\mathfrak{L})}{[K:\mathbb{Q}]}\right\}_\sigma, \left\{\ln|\alpha|_{\mathfrak{L}}^{[K_{\mathfrak{L}}:\mathbb{Q}_\ell]} + \beta - \ln\mathcal{N}(\mathfrak{L})\right\}_{\mathfrak{L}\in\mathcal{S}}\right).$$

5.2 Experimental settings

Computing the full group of $\mathcal{S}$-units in a classical way is rapidly intractable, even in the case of cyclotomic fields; therefore, experiments on Tw-PHS performed in [BR20] were bound to $\varphi(m) \leq 70$. We apply the Tw-PHS algorithm using our full-rank sublattices of the whole log-$\mathcal{S}$-unit lattice induced by the independent family $\mathfrak{F}$ of Eq. (3.13), its 2-saturated counterpart $\mathfrak{F}_{\mathsf{sat}}$ (§3.6) and, when possible, a fundamental system $\mathfrak{F}_{\mathsf{su}}$ for the full $\mathcal{S}$-unit group. These degraded modes should however already give a glimpse on how Tw-PHS scales in higher dimensions.

Source code and hardware description. All experiments have been implemented using SageMath v9.0 [Sag20], except for the full $\mathcal{S}$-unit groups computations for which we used Magma [BCP97], which appears much faster for this particular task and also offers an indispensable product ("Raw") representation. Moreover, fplll [FpL16] was used to perform all lattice reduction algorithms. The entire source code is provided on `https://github.com/ob3rnard/Tw-Sti`.

Most of the computations were performed in less than two weeks on a server with 72 Intel® Xeon® E5-2695v4 @2.1GHz with 768GB of RAM, using 2TB of storage for the precomputations. Real class group computations were performed on a single Intel® Core™ i7-8650U @3.2GHz CPU using 10GB of RAM.

Targetted cyclotomic fields. We consider cyclotomic fields of *any* conductor m st. $20 < \varphi(m) < 190$ with known real class number $h_m^+ = 1$, including those from

m	$\varphi(m)$	h_m^+	m	$\varphi(m)$	h_m^+	m	$\varphi(m)$	h_m^+	m	$\varphi(m)$	h_m^+	m	$\varphi(m)$	h_m^+
136	64	2	248	120	4	284	140	†	205	160	2	332	164	†
212	104	5	272	128	2	292	144	†	328	160	†	344	168	†
145	112	2	408	128	2	504	144	4	440	160	5	356	176	†
183	120	4	268	132	†	316	156	†	163	162	4	376	184	†

TABLE 5.1 – List of ignored conductors (†: failure to compute Cl_m^+ within a day).

Tab. 2.1. The restriction to $h_m^+ = 1$ is only due to technical interface obstructions, i.e. we are not aware of how to access the non-trivial real class group relations internally computed by SAGEMATH. Additionally, for some of the conductors, we were not able to obtain the real class group within a day. Thus, we are left with 192 distinct cyclotomics fields, and Tab. 5.1 lists all ignored conductors.

Finite places choice. The optimal set of places computed by [BR20, Alg. 4.1] yields a number $d_{\max}$ of split G_m-orbits of smallest norms maximizing the density of the corresponding full log-$\mathcal{S}$-unit lattice. However, the index of our log-$\mathcal{S}$-unit *sublattices*, given by Th. 3.13, grows too quickly, roughly in $(h_m^-)^{d-1}$, so that their density always decrease as soon as $d > 1$. This remark motivates us to compute all log-$\mathcal{S}$-unit sublattices for $d = 1$ to $d_{\max}$ first split G_m-orbits.

Full rank log-$\mathcal{S}$-unit sublattices. The first maximal set of independent $\mathcal{S}$-units that we consider is $\mathfrak{F}$ from Eq. (3.13). The 2-saturation process of §3.6 mitigates the huge index of $\mathfrak{F}$, yielding family $\mathfrak{F}_{\mathsf{sat}}$. A fundamental system $\mathfrak{F}_{\mathsf{su}}$ of the full $\mathcal{S}$-unit group $\mathcal{O}_{K_m,\mathcal{S}}^{\times}$ (modulo torsion) is also used whenever it is computable in reasonable time, i.e. up to $\varphi(m) < 80$. As noted in §2.3, their images under any log-$\mathcal{S}$-embedding φ form full-rank sublattices resp. L_{urs}, L_{sat}, L_{su}, generated by resp. $\varphi(\mathfrak{F})$, $\varphi(\mathfrak{F}_{\mathsf{sat}})$, $\varphi(\mathfrak{F}_{\mathsf{su}})$, of the corresponding full log-$\mathcal{S}$-unit lattice $\varphi(\mathcal{O}_{K_m,\mathcal{S}}^{\times})$.

We consider several choices of the log-$\mathcal{S}$-embedding φ. Namely, we tried to evaluate the advantage of using the expanded $\overline{\mathrm{Log}}_{\mathcal{S}}$ (exp) over $\mathrm{Log}_{\mathcal{S}}$, labelled tw (as twisted by $[\mathbb{C} : \mathbb{R}] = 2$). We also considered versions with (iso) or without (noiso) the isometry f_H of [BR20, Eq. (4.2)]. This yields four choices for φ, e.g. tag noiso/tw is $\varphi = \mathrm{Log}_{\mathcal{S}}$ and iso/exp gives the original $\varphi_{\mathsf{tw}} = f_H \circ \overline{\mathrm{Log}}_{\mathcal{S}}$.

Compact product representation. In order to avoid the exponential growth of algebraic integers viewed in $\mathbb{Z}[x]/\langle \Phi_m(x) \rangle$, we use a compact product representation, so that any element α in $\mathfrak{F}$ (resp. $\mathfrak{F}_{\mathsf{sat}}$ or $\mathfrak{F}_{\mathsf{su}}$) is written on a set $g_1, \ldots, g_N$ of N small elements as $\alpha = \prod_{i=1}^{N} g_i^{e_i}$. Hence, besides the g_i's, each α is stored as a vector $e \in \mathbb{Z}^N$, and for any choice of φ, we have $\varphi(\alpha) = \sum_{i=1}^{N} e_i \cdot \varphi(g_i)$. This allows to compute φ without the coefficient explosion encountered in [BR20, §5].

Lattice reductions. For each of the constructed log-$\mathcal{S}$-unit sublattices, i.e. for each number of orbits $d \in [\![1, d_{\max}]\!]$, for each family of independent $\mathcal{S}$-units $\mathfrak{F}$, $\mathfrak{F}_{\mathsf{sat}}$ and (when available) $\mathfrak{F}_{\mathsf{su}}$, and for each choice of log-$\mathcal{S}$-embedding, we compare several levels of reduction: no reduction ("raw"), LLL-reduction and BKZ_{40}-reduction.

m	d	set	k	$\mathrm{Vol}^{1/k}$	δ_0 raw	δ_0 LLL	δ_0 bkz$_{40}$	δ raw	δ LLL	δ bkz$_{40}$
152	1	urs	107	8.691	0.999	0.997	0.997	2.016	1.588	1.577
		sat	107	6.928	1.001	0.999	0.999	4.398	1.790	1.820
		su	107	6.928	1.000	0.999	0.999	28.396	1.810	1.811
	2	urs	179	9.683	0.999	0.998	0.998	2.157	1.630	1.612
		sat	179	7.384	1.000	0.999	0.999	7.670	1.885	1.898
		su	179	6.816	1.000	1.000	1.000	65.355	2.225	2.309
149	1	urs	221	12.192	0.999	0.999	0.999	2.828	2.092	2.028
		sat	221	9.697	1.000	1.000	1.000	12.473	2.307	2.266
	2	urs	369	13.353	0.999	0.999	0.999	3.134	2.234	2.173
		sat	369	10.150	1.000	1.000	1.000	14.472	2.509	2.483
	3	urs	517	13.962	0.999	0.999	0.999	3.269	2.271	2.213
		sat	517	10.410	1.000	1.000	1.000	22.211	2.569	2.552
	4	urs	665	14.415	1.000	1.000	1.000	3.327	2.301	2.244
		sat	665	10.632	1.000	1.000	1.000	20.731	2.606	2.594
564	1	urs	275	12.264	1.000	0.999	0.999	2.551	2.035	2.085
		sat	275	9.750	1.001	1.000	1.000	14.624	2.387	2.384
	2	urs	459	13.384	1.000	0.999	0.999	2.831	2.193	2.248
		sat	459	10.168	1.000	1.000	1.000	15.707	2.656	2.643
	3	urs	643	14.393	1.000	0.999	0.999	2.984	2.236	2.291
		sat	643	10.724	1.000	1.000	1.000	17.342	2.728	2.714
	4	urs	827	15.032	1.000	0.999	0.999	3.029	2.253	2.313
		sat	827	11.080	1.000	1.000	1.000	18.829	2.759	2.743

TABLE 5.2 – Geometric characteristics of L_{urs}, L_{sat} and L_{su} for $\mathbb{Q}(\zeta_{152})$, $\mathbb{Q}(\zeta_{149})$ and $\mathbb{Q}(\zeta_{564})$ with log-$\mathcal{S}$-embedding of type noiso/exp.

5.3 Geometry of the lattices

For all described choices of log-$\mathcal{S}$-unit sublattices, we first evaluate several geometrical parameters (see §2.5): reduced volume $V^{1/k}$, root-Hermite factor δ_0, orthogonality defect δ. For clarity's sake, we only give here a few examples giving a glimpse of what happens in general, and additional data can be found in §B.1.

Table 5.2 contains data for cyclotomic fields $\mathbb{Q}(\zeta_{152})$, $\mathbb{Q}(\zeta_{149})$ and $\mathbb{Q}(\zeta_{564})$ of degrees 72, 148 and 184. All values correspond to the noiso/exp log-$\mathcal{S}$-embedding, i.e. $\varphi = \varphi_{\mathsf{tw}}$. Indeed, as illustrated by Tab. B.2, we experimentally note that using (no)iso/exp seems geometrically slightly better than using (no)iso/tw.

We stress that we observe the same behaviour for the data presented here as for all other fields. As expected, the reduced volumes are smaller for L_{sat} than for L_{urs}, and both increase significantly with the number of orbits. The root-Hermite factor δ_0 is always very close to 1, confirming observations of [BR20, Tab. B.1]. We also retrieve the evolution of the orthogonality defect: indeed, the raw basis corresponding to L_{urs} seems to be already well reduced, and all lattices have small orthogonality defect δ after LLL reduction. Moreover, observe that BKZ$_{40}$ does not seem to improve much the orthogonality defect of the bases.

Norms of the Gram-Schmidt Orthogonalization. We then look at the logarithm of the Gram-Schmidt norms, for every described choice of log-$\mathcal{S}$-unit sublattices.

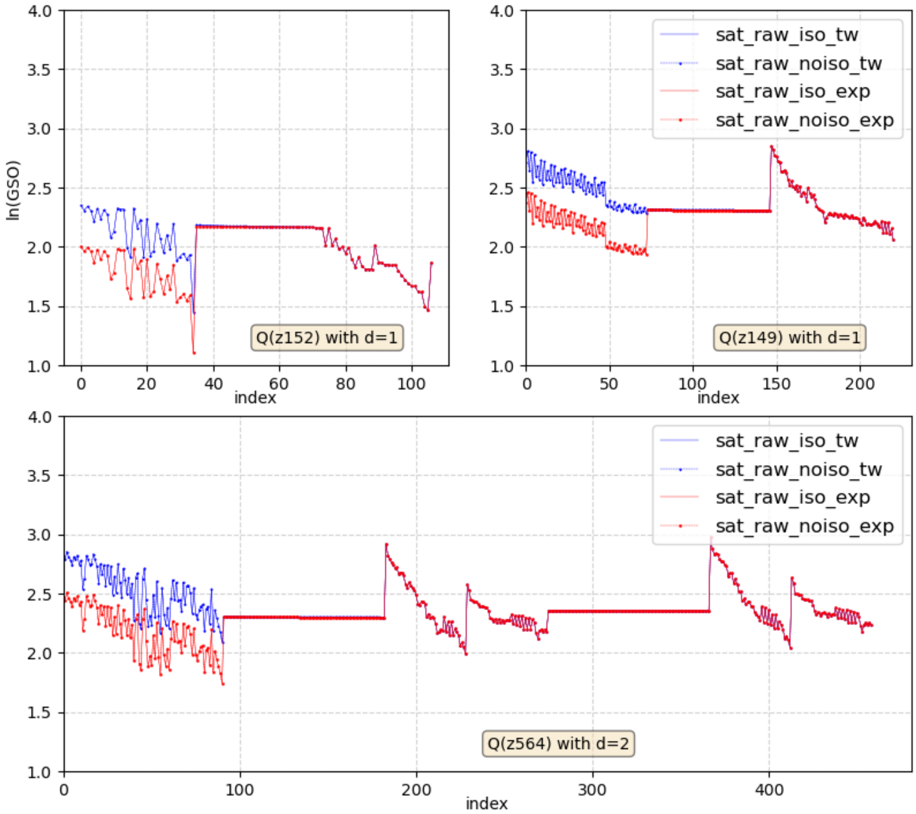

FIG. 5.1 – L_{sat} lattices for $\mathbb{Q}(z_{149}), \mathbb{Q}(z_{159})$ and $\mathbb{Q}(z_{564})$: effect of the log-$\mathcal{S}$-embedding choices iso/noiso and exp/tw.

Figure 5.1 shows the evolution of the norms for one or two orbits of the *unreduced* basis $\varphi(\mathfrak{F}_{\mathsf{sat}})$ for all four options of the log-$\mathcal{S}$-embedding φ. Again, we stress that these curves are similar for all fields. As expected, the isometry f_H has absolutely no influence on the Gram-Schmidt norms. On the other hand, using $\mathrm{Log}_{\mathcal{S}}$ or $\overline{\mathrm{Log}}_{\mathcal{S}}$ seems to alter only the first norms, and in a very small way. We note that increasing the number of orbits does not influence these behaviours.

Figure 5.2 plots the Gram-Schmidt log norms before and after BKZ reduction of the same lattices L_{sat} as in Fig. 5.1, using the original iso/exp log-$\mathcal{S}$-embedding. As in [BR20, Fig. B.1–10], for each field the two curves are almost superposed, which is consistent with the previous observations on the orthogonality defect.

5.4 Evaluation of the approximation factor

In [BR20], evaluating in practice the approximation factors reached by the Tw-PHS algorithm is done by choosing random split ideals of prime norm, solving the ClDL for these challenges and comparing the length of the obtained algebraic integer with the length of the exact shortest element. As the degree of the fields grow, solving the ClDL and exact id-SVP becomes rapidly intractable. Hence, we

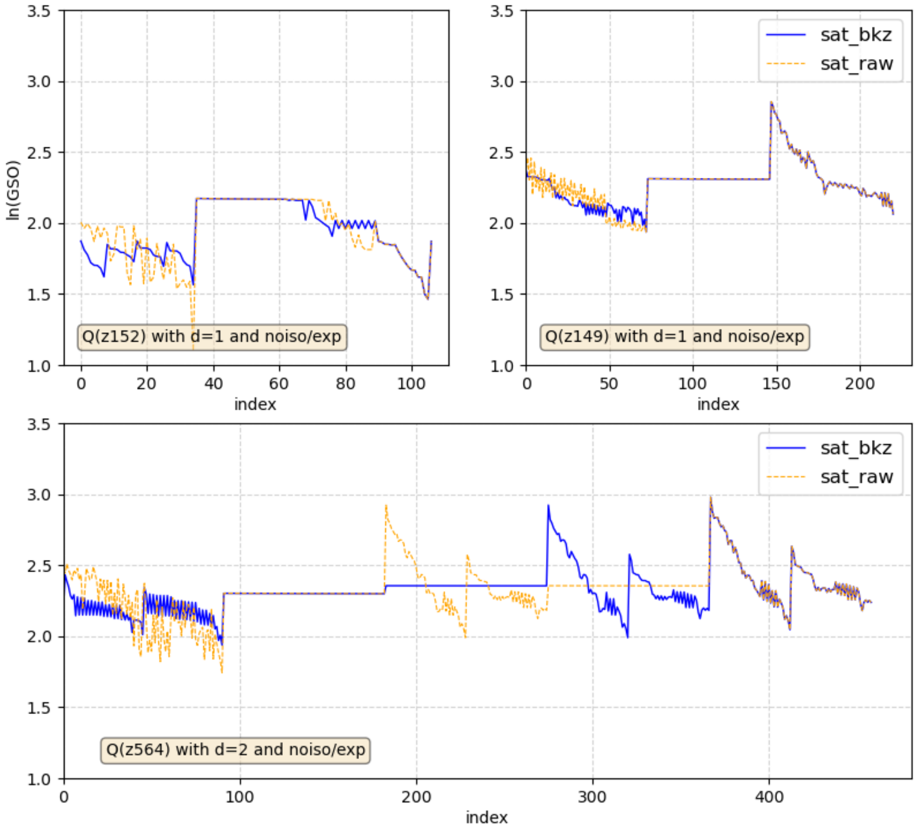

FIG. 5.2 – L_{sat} lattices for $\mathbb{Q}(z_{152}), \mathbb{Q}(z_{149})$ and $\mathbb{Q}(z_{564})$: Gram-Schmidt log norms before and after reduction by BKZ_{40}.

resort to simulating random outputs of the ClDL, similarly to [DPW19, Hyp. 8], and estimate the obtained approximation factors with inequalities from Eq. (2.7).

Simulation of ClDL solutions. To simulate targets that heuristically correspond to the output α of the ClDL, we assume that for each ideal $\mathfrak{L}_i \in \mathcal{S}$, the vector $\left(v_{\mathfrak{L}_i^\sigma}(\alpha)\right)_{\sigma \in G_m}$ of $\mathbb{Z}[G_m]$ is uniform modulo the lattice of class relations, and that after projection along the $\mathbf{1}$-axis, $\left(\ln|\sigma(\alpha)|\right)_\sigma$ is uniform modulo the log-unit lattice. These hypotheses have already been used in [DPW19, Hyp. 8] or [BR20, H. 4.8], and are backed up by theoretical results in [BDPW20, Th. 3.3].

Drawing random elements modulo a lattice of rank k is done by following a Gaussian distribution of deviation $100 \cdot k$. Concretely, we first choose a random split prime p in the range $[\![2^{97}, 2^{103}]\!]$. Then, for each $\mathfrak{L} \in \mathcal{S} \cap \mathcal{S}_0$, we pick random valuations $v_{\mathfrak{L}}(\alpha)$ modulo the lattice of class relations of rank $\left|\mathcal{S} \cap \mathcal{S}_0\right|$ and random elements $(u_\sigma)_{\sigma \in G_m^+} \in \mathbb{R}^{\varphi(m)/2}$ in the span of the log-unit lattice of rank $\frac{\varphi(m)}{2} - 1$. Finally, we simulate $(\ln|\sigma(\alpha)|)_\sigma$ by adding $\frac{\ln p + \sum_{\mathfrak{L} \in \mathcal{S}} v_{\mathfrak{L}} \ln \mathcal{N}(\mathfrak{L})}{\varphi(m)}$ to each coordinate u_σ, so that their sum is indeed $\frac{\ln|\mathcal{N}(\alpha)|}{2}$. For each field we thereby generate 100 random targets on which to test Tw-PHS on all lattice versions.

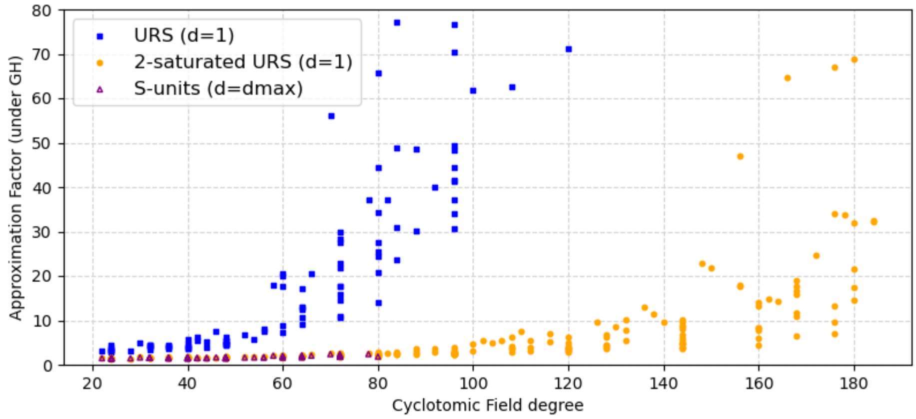

FIG. 5.3 – Approximation factors, with Gaussian Heuristic, reached by Tw-PHS for cyclotomic fields of degree up to 190, on lattices L_{urs}, L_{sat} and L_{su}.

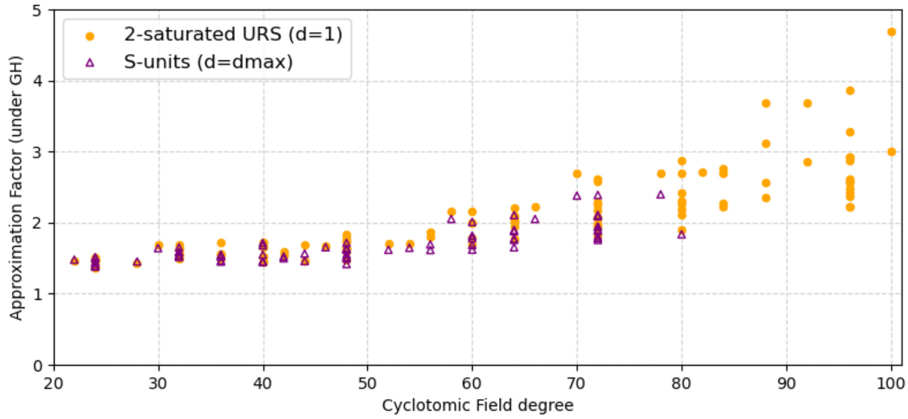

FIG. 5.4 – Approximation factors, with Gaussian Heuristic, reached by Tw-PHS for cyclotomic fields of degree up to 100, on lattices L_{sat} and L_{su}.

Reconstruction of a solution. For each simulated ClDL solution α, given as a random vector $(\{\ln|\sigma(\alpha)|\}_{\sigma\in G_m^+}, \{v_{\mathfrak{L}}(\alpha)\}_{\mathfrak{L}\in\mathcal{S}\cap\mathcal{S}_0})$, it is easy to compute $\varphi(\alpha)$ for any log-$\mathcal{S}$-embedding φ and to derive a target as in [BR20, Eq. (4.7)], including a drift parameterized by some β. Then, considering e.g. $L_{\mathsf{sat}} = \varphi(\mathfrak{F}_{\mathsf{sat}})$, given by the *BKZ*$_{40}$*-reduced* basis $U_{\mathsf{bkz}}\cdot\varphi(\mathfrak{F}_{\mathsf{sat}})$, we find a close vector $v = (y\cdot U_{\mathsf{bkz}})\cdot\varphi(\mathfrak{F}_{\mathsf{sat}})$ to this target using Babai's Nearest Plane algorithm, and from y, U_{bkz} and $\mathfrak{F}_{\mathsf{sat}}$ we easily recover, in compact representation, $s \in \mathcal{O}_{K_m,\mathcal{S}}^{\times}$ st. $v = \varphi(s)$ and also α/s.

The purpose of the drift parameter β is to guarantee $v_{\mathfrak{L}}(\alpha/s) \geq 0$ on all finite places. As mentioned in [BR20], the length of α/s is extremely sensitive to the value of β, so that they searched for an optimal value by dichotomy. However, this positiveness property actually does not seem to be monotonic in β, so we instead applied a crude search strategy, first increasing β until all $v_{\mathfrak{L}}(\alpha/s)$ are positive, then sampling 80 values in $\left[\frac{\beta}{1.4}, \beta\right]$. We output the optimal $\|\alpha/s\|_2$.

Estimator of the approximation factor. Since we do not have access to the shortest element of a challenge ideal, we cannot compute an exact approximation factor as is done in [BR20]. Instead, we estimate the retrieved approximation factor using the inequalities implied by Eq. (2.7). We focus on the Gaussian Heuristic, which seems to give in small dimensions consistent results with the exact approximation factors found in [BR20]. For each cyclotomic field, the plotted points are the means, over the 100 simulated random targets, of the minimal approximation factors obtained using options $\mathsf{iso}/\mathsf{noiso}$ and exp/tw. For each family $\mathfrak{F}$, $\mathfrak{F}_{\mathsf{sat}}$ and $\mathfrak{F}_{\mathsf{su}}$, we maximize the density of resp. L_{urs}, L_{sat} and L_{su}, using only $d = 1$ G_m-orbit for $\mathfrak{F}$, $\mathfrak{F}_{\mathsf{sat}}$, and $d = d_{\max}$ for $\mathfrak{F}_{\mathsf{su}}$. Figure 5.3 shows the approximation factor $\mathrm{af}_{\mathsf{gh}}$ obtained for all lattices L_{urs}, L_{sat} and L_{su} (when applicable) after BKZ_{40} reduction. Figure 5.4 focuses on L_{sat} and L_{su} on small dimensions.

First, we remark that using family $\mathfrak{F}$ from Eq. (3.13) does not seem to be satisfactory, the retrieved approximation factors increasing rapidly. Using the 2-saturated family $\mathfrak{F}_{\mathsf{sat}}$ yields much better results, and looking closely at Fig. 5.4 shows that using a basis $\mathfrak{F}_{\mathsf{su}}$ of the full $\mathcal{S}$-unit group, when available, even improves the picture if $d_{\max} > 1$. For L_{sat}, note that, even for fields of large degree, we obtain small approximation factors similar to the ones observed in [BR20].

However, for four fields of large degree, the values of $\mathrm{af}_{\mathsf{gh}}$ observed in Fig. 5.3 are significantly larger. This variance may be explained by the extreme sensitivity of the drift procedure used in the Cvp step. Indeed, even microscopic differences in the target definition can yield dramatically different outcomes. Improving this step would certainly result in better and narrower approximation factors.

Acknowledgements. The first author is deeply indebted to Radan Kučera for the proof of Lem. 3.14, and for thorough and invaluable discussions about the Stickelberger ideal. Andrea Lesavourey is funded by the Direction Générale de l'Armement (Pôle de Recherche CYBER), with the support of Région Bretagne. This work is supported by the European Union PROMETHEUS project (Horizon 2020 Research and Innovation Program, grant 780701).

References

Bab86. L. Babai: *On Lovász' lattice reduction and the nearest lattice point problem.* Combinatorica, **6**(1), pp. 1–13, 1986.

Bac90. É. Bach: *Explicit bounds for primality testing and related problems.* Math. Comp., **55**(191), pp. 355–380, 1990.

BBV+17. J. Bauch, D. Bernstein, H. de Valence, T. Lange, C. van Vredendaal: *Short generators without quantum computers: the case of multiquadratics.* In *EUROCRYPT (1)*, vol. 10210 of *LNCS*, pp. 27–59, Springer, 2017.

BCP97. W. Bosma, J. Cannon, C. Playoust: *The Magma algebra system. I. The user language.* J. Symbolic Comput., **24**(3-4), pp. 235–265, 1997, computational algebra and number theory (London, 1993).

BDF08. K. Belabas, F. Diaz y Diaz, E. Friedman: *Small generators of the ideal class group.* Math. Comput., **77**(262), pp. 1185–1197, 2008.

BDPW20. K. d. Boer, L. Ducas, A. Pellet-Mary, B. Wesolowski: *Random self-reducibility of Ideal-SVP via Arakelov random walks.* In *CRYPTO (2)*, vol. 12171 of *LNCS*, pp. 243–273, Springer, 2020.

BEF+17. J. Biasse, T. Espitau, P. Fouque, A. Gélin, P. Kirchner: *Computing generator in cyclotomic integer rings.* In *EUROCRYPT (1)*, vol. 10210 of *LNCS*, pp. 60–88, Springer, 2017.

Bel04. K. Belabas: *A relative van Hoeij algorithm over number fields.* J. Symb. Comput., **37**(5), pp. 641–668, 2004.

BFHP21. J. Biasse, C. Fieker, T. Hofmann, A. Page: *Norm relations and computational problems in number fields.* arXiv:2002.12332v3 [math.NT], 2021.

BK21. O. Bernard, R. Kučera: *A short basis of the Stickelberger ideal of a cyclotomic field.* arXiv:2109.13329 [math.NT], 2021.

BLP93. J. Buhler, H. Lenstra, C. Pomerance: *Factoring integers with the number field sieve*, vol. 1554 of *Lecture Notes in Math.* Springer, 1993.

BPR04. J. Buhler, C. Pomerance, L. Robertson: *Heuristics for class numbers of prime-power real cyclotomic fields.* Fields Inst. Commun., **41**, pp. 149–157, 2004.

BR20. O. Bernard, A. Roux-Langlois: *Twisted-PHS: Using the product formula to solve Approx-SVP in ideal lattices.* In *ASIACRYPT*, vol. 12492 of *LNCS*, pp. 349–380, Springer, 2020.

BS16. J.-F. Biasse, F. Song: *Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields.* In *SODA*, pp. 893–902, SIAM, 2016.

BV18. J. Biasse, C. van Vredendaal: *Fast multiquadratic S-unit computation and application to the calculation of class groups.* In *ANTS-XIII*, vol. 2 of *The Open Book Series*, pp. 103–118, Mathematical Sciences Publisher, 2018.

CDPR16. R. Cramer, L. Ducas, C. Peikert, O. Regev: *Recovering short generators of principal ideals in cyclotomic rings.* In *EUROCRYPT (2)*, vol. 9666 of *LNCS*, pp. 559–585, Springer, 2016.

CDW17. R. Cramer, L. Ducas, B. Wesolowski: *Short Stickelberger class relations and application to Ideal-SVP.* In *EUROCRYPT (1)*, vol. 10210 of *LNCS*, pp. 324–348, Springer, 2017.

CDW21. R. Cramer, L. Ducas, B. Wesolowski: *Mildly short vectors in cyclotomic ideal lattices in quantum polynomial time.* J. ACM, **68**(2), 2021.

CGS14. P. Campbell, M. Groves, D. Shepherd: *Soliloquy: A cautionary tale*, 2014, available at `http://docbox.etsi.org/Workshop/2014/201410_CRYPTO/S07_Systems_and_Attacks/S07_Groves_Annex.pdf`.

Che13. Y. Chen: *Réduction de réseau et sécurité concrète du chiffrement complètement homomorphe.* Ph.D. thesis, Paris 7, 2013.

CN11. Y. Chen, P. Q. Nguyen: *BKZ 2.0: Better lattice security estimates.* In *ASIACRYPT*, vol. 7073 of *LNCS*, pp. 1–20, Springer, 2011.

Coh93. H. Cohen: *A course in computational algebraic number theory*, vol. 138 of *Graduate texts in mathematics.* Springer, 1993.

DPW19. L. Ducas, M. Plançon, B. Wesolowski: *On the shortness of vectors to be found by the Ideal-SVP quantum algorithm.* In *CRYPTO (1)*, vol. 11692 of *LNCS*, pp. 322–351, Springer, 2019.

EHKS14. K. Eisenträger, S. Hallgren, A. Y. Kitaev, F. Song: *A quantum algorithm for computing the unit group of an arbitrary degree number field.* In *STOC*, pp. 293–302, ACM, 2014.

FpL16. FpLLL development team: *fplll, a lattice reduction library*, 2016, available at https://github.com/fplll/fplll.
GK89. R. Gold, J. Kim: *Bases for cyclotomic units*. Compos. Math., **71**(1), pp. 13–27, 1989.
GN08. N. Gama, P. Q. Nguyen: *Predicting lattice reduction*. In *EUROCRYPT*, vol. 4965 of *LNCS*, pp. 31–51, Springer, 2008.
Hol17. P. Holzer: *Recovering short generators of principal fractional ideals in cyclotomic fields of conductor $p^\alpha q^\beta$*, 2017, master Thesis, available at http://tuprints.ulb.tu-darmstadt.de/6155/.
Kuč86. R. Kučera: *On a certain subideal of the Stickelberger ideal of a cyclotomic field*. Archivum Mathematicum, **22**(1), pp. 7–19, 1986.
Kuč92. R. Kučera: *On bases of the Stickelberger ideal and of the group of circular units of a cyclotomic field*. J. Number Theory, **40**(3), pp. 284–316, 1992.
Laa16. T. Laarhoven: *Sieving for closest lattice vectors (with preprocessing)*. In *SAC*, vol. 10532 of *LNCS*, pp. 523–542, Springer, 2016.
Les21. A. Lesavourey: *Usability of structured lattices for a post-quantum cryptography: practical computations, and a study of some real Kummer extensions*. Ph.D. thesis, University of Wollongong, 2021.
LLL82. A. K. Lenstra, H. W. Lenstra, L. Lovász: *Factoring polynomials with rational coefficients*. Math. Ann., **261**, pp. 515–534, 1982.
LPR10. V. Lyubashevsky, C. Peikert, O. Regev: *On ideal lattices and learning with errors over rings*. In *EUROCRYPT*, vol. 6110 of *LNCS*, pp. 1–23, Springer, 2010.
LPS20. A. Lesavourey, T. Plantard, W. Susilo: *Short principal ideal problem in multicubic fields*. J. Math. Cryptol., **14**(1), pp. 359–392, 2020.
MG02. D. Micciancio, S. Goldwasser: *Complexity of Lattice Problems*, vol. 671 of *The Kluwer International Series in Engineering and Computer Science*. Springer, 2002.
Mil14. J. C. Miller: *Class numbers of real cyclotomic fields of composite conductor*. LMS J. Comput. Math., **17**, pp. 404–417, 2014.
Nar04. W. Narkiewicz: *Elementary and Analytic Theory of Algebraic Numbers*. Springer Monographs in Mathematics, Springer, 3 edn., 2004.
Neu99. J. Neukirch: *Algebraic Number Theory*, vol. 322 of *Grundlehren des mathematischen Wissenschaften*. Springer, 1999.
PHS19. A. Pellet-Mary, G. Hanrot, D. Stehlé: *Approx-SVP in Ideal lattices with pre-processing*. In *EUROCRYPT (2)*, vol. 11477 of *LNCS*, pp. 685–716, Springer, 2019.
PZ89. M. Pohst, H. Zassenhaus: *Algorithmic Algebraic Number Theory*. Encyclop. Math. Appl., Cambridge University Press, 1989.
Sag20. Sage Developers: *SageMath, the Sage Mathematics Software System (Version 9.0)*, 2020, available at https://www.sagemath.org.
Sch87. C. Schnorr: *A hierarchy of polynomial time lattice basis reduction algorithms*. Theor. Comput. Sci., **53**, pp. 201–224, 1987.
Sch03. R. Schoof: *Class numbers of real cyclotomic fields of prime conductor*. Math. Comput., **72**(242), pp. 913–937, 2003.
Sch08. R. Schoof: *Catalan's Conjecture*. Universitext, Springer, 2008.
Sin78. W. Sinnott: *On the Stickelberger ideal and the circular units of a cyclotomic field*. Ann. Math., **108**(1), pp. 107–134, 1978.
Sin80. W. Sinnott: *On the Stickelberger ideal and the circular units of an abelian field*. Invent. Math., **62**, pp. 181–234, 1980.

SSTX09. D. Stehlé, R. Steinfeld, K. Tanaka, K. Xagawa: *Efficient public key encryption based on ideal lattices*. In *ASIACRYPT*, vol. 5912 of *LNCS*, pp. 617–635, Springer, 2009.

Tho12. E. Thomé: *Square root algorithms for the Number Field Sieve*. In *WAIFI*, vol. 7369 of *LNCS*, pp. 208–224, Springer, 2012.

Was97. L. C. Washington: *Introduction to Cyclotomic Fields*, vol. 83 of *Graduate Texts in Mathematics*. Springer, 2 edn., 1997.

Wes18. B. Wesolowski: *Generating subgroups of ray class groups with small prime ideals*. In *ANTS-XIII*, vol. 2 of *The Open Book Series*, pp. 461–478, Mathematical Sciences Publisher, 2018.

Supplementary materials

A Quantum improvements of the CDW algorithm

In §3.3 a short basis for the Stickelberger lattice has been introduced in Th. 3.7, as well as associated generators defined in Pr. 3.8. We make use of these new elements and see how they can be applied to the approx-Svp algorithm from [CDW17,CDW21]. First, we recall the original algorithms with only aesthetic rearrangement that will reveal useful later on. Then, using explicit Stickelberger elements corresponding to the class group relations of the relatively short generating family W of [CDW21], as well as principal relative norm ideals generators, we replace the last Pip call in the query phase by a class group computation in the preprocessing phase in the maximal real subfield, hence in dimension half of the initial field. Finally, we remove the need of using the random walk mapping challenge ideals into the minus part of the class group, by using the module of *all* real class group relations $C^{+}_{\mathfrak{l}_1,\ldots,\mathfrak{l}_d}$ introduced in §3.4, under the restriction that $h_m^+ \leq O(\sqrt{m})$ (Hyp. A.1).

A.1 Hypothesis on the plus part of the class number

The CDW algorithm from [CDW21] assumes that $h_m^+ \leq \mathrm{poly}(m)$ for any conductor m [CDW21, Ass. 2]. This is needed for their random walk procedure mapping any ideal to Cl_m^- to have a running time in $\mathrm{poly}(m)$. To remove this reduction to Cl_m^- constraint, we use a slightly more restrictive hypothesis.

Hypothesis A.1. We restrict to cyclotomic fields K_m verifying $h_m^+ \leq O(\sqrt{m})$.

This assumption is certainly not true in general. Nevertheless, by the discussion in Section 2.2, it should be valid when m is a power of 2 and asymptotically when m is a prime power. Finally, according to Schoof's table, we note that $h_m^+ \leq \sqrt{m}$ holds for more than 96.6% of all prime conductors $m = p < 10000$. We stress that this restriction only impacts the results of §A.4.

A.2 An equivalent rewriting of the CDW algorithm

The following general proposition will be useful for fully understanding algorithms from [CDW21] as well as the improvements we provide.

As stated in §2.1, given a cyclotomic field K_m, recall we identify $G_m/\langle\tau\rangle$ with G_m^+, and we consider the natural lift of those elements to G_m. For any $\sigma \in G_m^+$, and any $\alpha \in \mathbb{Z}[G_m]$, we write $\Delta_\sigma(\alpha) := \alpha_\sigma - \alpha_{\sigma\tau}$.

Proposition A.2. *Let $\alpha \in \mathbb{Z}[G_m]$. Then for all $\beta \in \mathbb{Z}[G_m]$, we have:*

$$\beta \equiv \alpha \bmod (1+\tau) \iff \forall \sigma \in G_m^+, \quad \Delta_\sigma(\beta) = \Delta_\sigma(\alpha).$$

Moreover, let $\beta \equiv \alpha \bmod (1+\tau)$, then:

1. *For any $\sigma \in G_m^+$:*

– *$\beta_{\sigma\tau} = 0$ if, and only, if $\beta_\sigma = \Delta_\sigma(\alpha)$,*
– *$\beta_\sigma = 0$ if, and only, if $\beta_{\sigma\tau} = -\Delta_\sigma(\alpha)$.*

2. *There is a unique $\beta \equiv \alpha \bmod (1+\tau)$ with nonnegative integer coordinates and minimal ℓ_1-norm, it is defined by:*

$$\forall \sigma \in G_m^+, (\beta_\sigma, \beta_{\sigma\tau}) = \begin{cases} (\Delta_\sigma(\alpha), 0) & \text{if } \Delta_\sigma(\alpha) \geqslant 0 \\ (0, -\Delta_\sigma(\alpha)) & \text{if } \Delta_\sigma(\alpha) < 0. \end{cases} \tag{A.1}$$

Proof. The first assertion is easy since $\beta \equiv \alpha \bmod (1+\tau)$ if, and only if, for all $\sigma \in G_m^+$, $(\beta_\sigma, \beta_{\sigma\tau}) \in (\alpha_\sigma, \alpha_{\sigma\tau}) + (1,1)\cdot\mathbb{Z}$. Thus, locally in the coordinates $\sigma, \sigma\tau$ (with a fixed σ), there is in the class of α modulo $(1+\tau)$ a unique β such that $\beta_{\sigma\tau} = 0$ and a unique β such that $\beta_\sigma = 0$. These are exactly $(\alpha_\sigma - \alpha_{\sigma\tau}, 0)$ and $(0, \alpha_{\sigma\tau} - \alpha_\sigma)$. A coordinate pair $(\beta_\sigma, \beta_{\sigma\tau}) \in \mathbb{Z}^2$ (of $\beta \in \mathbb{Z}[G_m]$) is parametrized as $\Delta_\sigma(\alpha)(1-\lambda, -\lambda)$ for some $\lambda \in \mathbb{R}$. The segment delimited by $(\Delta_\sigma(\alpha), 0)$ and $(0, \Delta_\sigma(\alpha))$ are the points such that $\lambda \in [0,1]$. For any $\lambda > 1$ we have:

$$\|\Delta_\sigma(\alpha)(1-\lambda, -\lambda)\|_1 = |\Delta_\sigma(\alpha)|(2\lambda - 1) > |\Delta_\sigma(\alpha)|,$$

and for $\lambda < 0$ one has:

$$\|\Delta_\sigma(\alpha)(1-\lambda, -\lambda)\|_1 = |\Delta_\sigma(\alpha)|(2|\lambda| + 1) > |\Delta_\sigma(\alpha)|.$$

Last, if $\lambda \in [0,1]$ the norm is $|\Delta_\sigma(\alpha)|$. Finally, in order to find a minimal element in a given class of $\mathbb{Z}[G_m]$ modulo $(1+\tau)$ with nonnegative coefficients only, it is sufficient to find a minimal pair $(\beta_\sigma, \beta_{\sigma\tau})$ with nonnegative coefficients for each $\sigma \in G_m^+$. Fix $\sigma \in G_m^+$ and assume without loss of generality that $\Delta_\sigma(\alpha) \geqslant 0$. Then following the characterisation above, any equivalent pair with minimal norm can be written $\Delta_\sigma(\alpha)(1-\lambda, -\lambda)$ with $\lambda \in [0,1]$. Among them, $(\Delta_\sigma(\alpha), 0)$ is clearly the only pair such that both coefficients are nonnegative. □

We can now recall the main algorithms from [CDW21]. Algorithm A.1 is WalkToCl$^-$ [CDW21, Alg. 5]. This algorithm gives reduces the general case to the case where the input ideal is in the relative class groups, for which the Stickelberger ideal is a natural lattice of class relations.

Algorithm A.1 WalkToCl$^-(\mathfrak{a})$: random walk to Cl_m^-

Input: an ideal $\mathfrak{a} \subset \mathcal{O}_{K_m}$.
Output: an ideal $\mathfrak{b} \subset \mathcal{O}_{K_m}$ s.t. $[\mathfrak{a}\mathfrak{b}] \in \mathrm{Cl}_m^-$ and $\mathcal{N}(\mathfrak{b}) \leq \exp(\tilde{O}(m))$.

$\ell = \tilde{O}(m), B = poly(m)$
repeat
  for $i = 1, \ldots, \ell$ **do**
    Choose $\mathfrak{L}_i$ uniformly at random among prime ideals of norm less than B
    $\mathfrak{b} \leftarrow \prod_{i=1}^{d} \mathfrak{L}_i$
until $\mathcal{N}_{K_m/K_m^+}(\mathfrak{a}\mathfrak{b})$ is principal, using the (quantum) Pip algorithm from [BS16]
return $\mathfrak{b}$

Once this technical requirement is satisfied, the main steps described in [CDW21] are given by the Reduce algorithm in Alg. A.2 which corresponds to [CDW21, Alg. 3]. This algorithm is subsequently used in algorithm $\textsc{Cpm}^-$ described in Alg. A.3 and which corresponds to [CDW21, Alg. 4][8]. Note also that compared to [CDW21, Alg. 4], the end of $\textsc{Cpm}^-$ algorithm is slightly modified to satisfy the convention we use for the ClDl algorithm.

Algorithm A.2 $\textsc{Reduce}(W, \xi)$: finds a reduction of ξ

Input: $\alpha \in \mathbb{Z}[G_m]$ and $W \subset \mathbb{Z}[G_m]$ a generating set of the Stickelberger lattice.
Output: $\beta \in \mathbb{Z}[G_m]$ s.t. $\|\beta\|_1 \leq \frac{1}{4} \cdot \varphi(m)^{3/2}$, and $C^\alpha = C^\beta$ for any $C \in \mathrm{Cl}_m^-$.

$v \leftarrow \textsc{Cvp}(\pi(W), \pi(\alpha))$
$\gamma \leftarrow \pi(\alpha) - v \cdot \pi(W)$
Define $(a_\sigma)_{\sigma \in G_m^+}$ as the integral coordinates of γ in the basis $(\pi(\sigma))_{\sigma \in G_m^+}$ of $\mathbb{Z}[G_m]/(1+\tau)$
$\beta \leftarrow \sum_{\sigma \in G_m^+} a_\sigma \sigma \in \mathbb{Z}[G_m]$
return β

Algorithm A.3 $\textsc{Cpm}^-(W, \mathfrak{L}, \alpha)$: solves the CPM problem for ideal $\mathfrak{L}^\alpha$

Input: A generating set W [CDW21, Lem. 4.4] of the Stickelberger lattice, an ideal $\mathfrak{L}$ such that $[\mathfrak{L}] \in \mathrm{Cl}_{K_m}^-$ and an element $\alpha \in \mathbb{Z}[G_m]$.
Output: an integral ideal $\mathfrak{b} = \mathfrak{L}^\gamma$ s.t. $\mathfrak{L}^\alpha \mathfrak{b}$ is principal and and $\mathcal{N}(\mathfrak{b}) = \mathcal{N}(\mathfrak{L})^{O(\varphi(m)^{3/2})}$.

$\beta \leftarrow \textsc{Reduce}(W, \alpha)$
Write β as $\beta = \sum_{\sigma \in G_m^+} a_\sigma \sigma$
for $\sigma \in G_m^+$ **do**
  $(a_\sigma^+, a_\sigma^-) \leftarrow \begin{cases} (a_\sigma, 0) & a_\sigma \geq 0, \\ (0, -a_\sigma) & \textit{otherwise} \end{cases}$
$\gamma \leftarrow \sum_{\sigma \in G_m^+} (a_\sigma^+ + a_\sigma^- \tau)\sigma$
return $\mathfrak{L}^\gamma$.

Finally, all the previously introduced algorithms are used to define the algorithm CDW [CDW21, Alg. 7] solving Approx-Svp for ideal lattice algorithm[9]. For this last algorithm, it will be useful for us to use an equivalent rewriting of it in a preprocessing phase (Alg. A.4) and a query phase (Alg. A.5). We also recall there exists an algorithm ShortGenerator [CDW21, Alg. 1] whose property is described in Th. A.3.

In order to be coherent with future algorithms that will be described with a preprocessing phase and a query phase, we argue that the (randomized) ClDl step of [CDW21, lines 4-8 Alg. 6] can be rewritten as follows. Essentially, instead of testing whether the ClDl algorithm succeeds within the algorithm, we fix a

[8] This algorithm was originally called $\textsc{ClosePrincipalMultiple}^-$ in [CDW21].
[9] This algorithm was originally called IdealSVP in [CDW21].

number of orbits d during the preprocessing phase (Alg. A.4) before moving to the query phase (Alg. A.5). If the ClDL step of the query phase fails then we go back to the preprocessing phase with a higher d. Also, for any of such d, we choose the bound $B = poly(m)$ so that $\mathfrak{M} = \{\mathfrak{L} \mid \mathcal{N}(\mathfrak{L}) \leq B, [\mathfrak{L}] \in \mathrm{Cl}_m^-\}$ has at least d elements allowing us to pick the d ideals of smallest norm within $\mathfrak{M}$, as in step 3 of Alg. A.4. After a small number of query we expect to find a sufficiently big d such that the ideals $\mathfrak{L}_1, \ldots, \mathfrak{L}_d$ generates Cl_m^-.

Algorithm A.4 $\mathrm{CDW}_{\text{pre-proc}}$: find a generating family of Cl_m^-

Input: a cyclotomic field K_m of conductor m and an integer d
Output: a family $\mathfrak{B}$ of prime ideals (expected to generate Cl_m^-)
1: $B = poly(m)$
2: $\mathfrak{M} \leftarrow \{\mathfrak{L} \mid \mathcal{N}(\mathfrak{L}) \leq B, [\mathfrak{L}] \in \mathrm{Cl}_m^-\}$
3: Choose $\mathfrak{L}_1, \ldots, \mathfrak{L}_d$ with smallest norm in $\mathfrak{M}$
4: $\mathfrak{B} \leftarrow \{\mathfrak{L}_i^\sigma \mid \sigma \in G_m, i = 1, \ldots, d\}$
5: **return** $\mathfrak{B}$

Algorithm A.5 $\mathrm{CDW}_{\text{query}}(\mathfrak{a})$: finding mildly short vectors in the ideal $\mathfrak{a}$

Input: an ideal $\mathfrak{a} \in \mathcal{O}_{K_m}$, a family $\mathfrak{B} \leftarrow \{\mathfrak{L}_i^\sigma \mid \sigma \in G_m, i = 1, \ldots, d\}$
Output: an element $h \in \mathfrak{a}$ of norm $\|h\|_2 \leq \exp(\tilde{O}(\sqrt{m})) \cdot \mathcal{N}(\mathfrak{a})^{1/\varphi(m)}$
1: $\mathfrak{b}' \leftarrow \mathrm{WalkToCl}^-(\mathfrak{a})$
2: $(y_{i,\sigma})_{\sigma \in G_m, i=1,\ldots,d} \leftarrow \mathrm{ClDL}_{\mathfrak{B}}(\mathfrak{a}\mathfrak{b}')$ ▷ $\mathfrak{a}\mathfrak{b}' \prod_{i,\sigma} (\mathfrak{L}_i^\sigma)^{y_{i,\sigma}} \sim 1$
3: **for** $i = 1, \ldots, d$ **do**
4: $\xi_i \leftarrow \sum_{\sigma \in G_m} y_{i,\sigma} \sigma \in \mathbb{Z}[G_m]$
5: $\mathfrak{b}_i' \leftarrow \mathrm{CPM}^-(W, \mathfrak{L}_i, \xi_i)$
6: $\mathfrak{b} \leftarrow \mathfrak{b}' \prod_{i=1}^d \mathfrak{b}_i'$
7: $g \leftarrow \mathrm{PIP}(\mathfrak{a}\mathfrak{b})$
8: $h \leftarrow \mathrm{ShortGenerator}(\mathrm{g})$
9: **return** h

Theorem A.3 ([CDW21, Th. 3.6]). *There is a randomized algorithm* ShortGenerator *that for any $g \in \mathcal{O}_{K_m}$ (in compact representation), finds an element $h \in \mathcal{O}_{K_m}$ (in compact representation) such that $g \cdot \mathcal{O}_{K_m} = h \cdot \mathcal{O}_{K_m}$ and $\|h\|_2 = \exp\left(O(\sqrt{m \log m})\right) \cdot \mathcal{N}(g)^{1/\varphi(m)}$, and runs in polynomial time in the size of the input.*

Now that we have introduced algorithms used in [CDW21], we first look into steps 2–5 of Alg. A.3. Essentially, these steps guarantee that the exponent $\gamma \in \mathbb{Z}[G_m]$ has only nonnegative coordinates in the basis $((\sigma)_{\sigma \in G_m^+}, (\sigma\tau)_{\sigma \in G_m^+})$, using the property $\mathfrak{L}^{-1} \sim \mathfrak{L}^\tau$ that was ensured by the restriction to the relative class group. However, it is also important that the resulting γ has small norm $\|\gamma\|_1$. In Pr. A.4, we show that steps 2–5 of Alg. A.3 guarantee that the returned

Algorithm A.6 PositiveOptim(α): returns an element in the class of α modulo $(1+\tau)\mathbb{Z}[G_m^+]$ whose coordinates in basis $((\sigma)_{\sigma\in G_m^+}, (\sigma\tau)_{\sigma\in G_m^+})$ are nonnegative integers and which is minimal for ℓ_1-norm inside the equivalence class.

Input: an element $\alpha \in \mathbb{Z}[G_m]$

Output: an element $\tilde{\alpha} \equiv \alpha$ of minimal ℓ_1-norm and whose coordinates in basis $((\sigma)_{\sigma\in G_m^+}, (\sigma\tau)_{\sigma\in G_m^+})$ are nonnegative integers.

```
Write α as ((a_σ)_{σ∈G_m^+}, (a_στ)_{σ∈G_m^+}) on the basis ((σ)_{σ∈G_m^+}, (στ)_{σ∈G_m^+}) of Z[G_m]
α̃ ← α
for σ ∈ G_m^+ do                                ▷ Dealing with negative coordinates
    if a_σ ≤ a_στ then
        α̃ ← α̃ − a_σ(1 + τ)σ
    else if a_στ ≤ a_σ then
        α̃ ← α̃ − a_στ(1 + τ)σ
return α̃.
```

exponent γ is actually minimal in a certain sense. Before that, we introduce the subroutine PositiveOptim in Alg. A.6 that generalizes steps 2–5 of Alg. A.3. This algorithm also applies to elements whose "right part" of coordinates are not all zero and explicitely shows that the modification are done using elements of $(1+\tau)\cdot\mathbb{Z}[G_m^+]$.

Proposition A.4. *In Alg. A.3, it is possible de replace steps 2–5 by subroutine* PositiveOptim. *Moreover, this shows the resulting γ has minimal ℓ_1-norm given $\beta \leftarrow$ Reduce(W,α) as in step 1 of Alg. A.3.*

Proof. We identify $\alpha \in \mathbb{Z}[G_m]$ with its coordinates $((a_\sigma)_{\sigma\in G_m^+}, (a_{\sigma\tau})_{\sigma\in G_m^+})$ in the basis $\left((\sigma)_{\sigma\in G_m^+}, (\sigma\tau)_{\sigma\in G_m^+}\right)$. Then, PositiveOptim, act the following way. For any $\sigma \in G_m^+$, $\alpha := (\ldots, a_\sigma, \ldots, a_{\sigma\tau}, \ldots)$ is mapped to $(\ldots, \Delta_\sigma(a), \ldots, 0, \ldots)$ if $\Delta_\sigma(a) \geq 0$, and if $\Delta_\sigma(a) < 0$, it is mapped to $(\ldots, 0, \ldots, -\Delta_\sigma(a), \ldots)$. This is precisely what steps 2–5 returns in the particular case where for all $\sigma \in G_m^+$, $a_{\sigma\tau} = 0$. Note that by Pr. A.2, those images are precisely of minimal norm (inside a fixed equivalence class). All in all, we conclude that the transformation $\beta \mapsto \gamma$ of Alg. A.3 remains inside the equivalence class of β and that it returns the element of minimal ℓ_1-norm inside this class. □

In Pr. A.4, we proved that given a particular class modulo $(1+\tau)$, algorithm PositiveOptim returns an element (with nonnegative coordinates) of the class whose ℓ_1-norm is minimal among all elements of the class. Nevertheless, among all the coset $\alpha + S_m$ how can we find the class whose associated minimal value is the smallest value among all the possible lower bounds? In previous works such as [CDW17,DPW19,CDW21] the question is raised when discussing whether to use a Cvp solver on $\pi(S_m)$ and then lifting it back, or directly on the extended Stickelberger lattice $S_m + (1+\tau)\mathbb{Z}[G_m]$[10]. The following proposition proves that, given an exact Cvp solver, the construction using $\pi(S_m)$ is optimal.

[10] Both modules being used as a replacement for S_m not being full-rank.

Proposition A.5. *Let $\alpha \in \mathbb{Z}[G_m]$, W_{bk} the short basis of the Stickelberger ideal S_m as introduced in Th. 3.7 and note* Cvp *an exact close vector problem solver on $\pi(W_{bk})$, for ℓ_1 norm. Define $\gamma(v) := \textsc{PositiveOptim}(\alpha - v \cdot W_{bk})$, as a function of $v \in \mathbb{Z}^{\varphi(m)/2}$, then: $\mathrm{argmin}_{v\in\mathbb{Z}^{\varphi(m)/2}} \|\gamma(v)\|_1 = \textsc{Cvp}(\pi(W_{bk}), \pi(\alpha))$.*

Proof. We note $\{w_1, \dots, w_{\varphi(m)/2}\}$ the elements of W_{bk} and we write v as the vector $(v_1, \dots, v_{\varphi(m)/2}) \in \mathbb{Z}^{\varphi(m)/2}$. Then:

$$\begin{aligned}\|\gamma(v)\|_1 &= \sum_{\sigma\in G_m^+} |\varDelta_\sigma(\textsc{PositiveOptim}(\alpha - v \cdot W_{\mathsf{bk}}))| \\ &= \sum_{\sigma\in G_m^+} |\varDelta_\sigma(\alpha - \sum_{i=1}^{\varphi(m)/2} v_i w_i)|\end{aligned}$$

by applying Pr. A.2, since subroutine PositiveOptim does not alter the equivalence class. Now, by definition of the projection π,

$$\begin{aligned}\sum_{\sigma\in G_m^+} |\varDelta_\sigma(\alpha - \sum_{i=1}^{\varphi(m)/2} v_i w_i)| &= \sum_{\sigma\in G_m^+} |\pi(\alpha)_\sigma - \sum_i v_i \pi(w_i)_\sigma| \\ &= \|\pi(\alpha) - v \cdot \pi(W_{\mathsf{bk}})\|_1.\end{aligned}$$

Hence, minimizing $\|\gamma(v)\|_1$ is equivalent to minimizing $\|\pi(\alpha) - v \cdot \pi(W_{\mathsf{bk}})\|_1$, which is achieved by taking $v = \textsc{Cvp}(\pi(W_{\mathsf{bk}}), \pi(\alpha))$. □

A.3 Using explicit Stickelberger generators

Many quantum steps are required in the query phase of the CDW algorithm (Alg. A.5). First, the random walk to reach Cl_m^- requires a polynomial number (in $h_{K_m}^+$) of steps and each of these steps requires a Pip test in the maximal real subfield. Second, a ClDl step is performed in the cyclotomic field to obtain inputs used in the Cpm$^-$ subroutine. Finally, a final Pip is performed in the cyclotomic field in order to recover a short generator.

Our goal in this subsection is to use Th. 3.7, Pr. 3.8 and the subroutine PositiveOptim, to reduce the cost of the last Pip call (inside Alg. A.5). In order to do so, one key ingredient is to replace the generating set W by the short basis W_{bk} of the Stickelberger lattice, introduced in Th. 3.7. This last switch is beneficial for several reasons:

1. In order to solve Cvp, using [CDW21, Cor. 2.2], one does not need anymore to compute a maximal set of linearly independent vectors inside W (in a greedy manner). We also note that this full-rank set of vectors only ensures that the Cvp algorithm is done inside a (full rank) sublattice of the Stickelberger lattice. Whereas, using the complete Stickelberger lattice basis ensures the best result for the Cvp algorithm, regarding the approximation factor.

2. The second advantage is that, using Pr. 3.8, we can use the explicit Stickelberger generators (associated to the principal ideals resulting from the action of W_{bk}). Exhibiting such Stickelberger generators is (in general) not possible for elements of the generating set W. This point will be of importance for replacing the last Pip call in dimension n (which is done for any challenge) in the CDW algorithm, by the computation of the real class group. Note that this last part also required the introduction of PositiveOptim (Alg. A.6).

Concretely, we define $(\textsc{Cpm}^-)'$ as Alg. A.7 and $\mathrm{CDW}^{\mathsf{explicit}}$ as the successive combinaison of algorithms Alg. A.8 and A.9, defining a preprocessing phase and a query phase.

Algorithm A.7 $\left(\textsc{Cpm}^-\right)'(W_{\mathsf{bk}}, \mathfrak{L}, \alpha)$: solves the CPM problem for ideal $\mathfrak{L}^\alpha$

Input: W_{bk} the basis of the Stickelberger lattice defined in §3.3, an ideal $\mathfrak{L}$ such that $[\mathfrak{L}] \in \mathrm{Cl}^-_{K_m}$ and an element $\alpha \in \mathbb{Z}[G_m]$.

Output: an integral ideal $\mathfrak{b} = \mathfrak{L}^\gamma$ s.t. $\mathfrak{L}^\alpha \mathfrak{b}$ is principal and and $\mathcal{N}(\mathfrak{b}) = \mathcal{N}(\mathfrak{L})^{O(\varphi(m)^{3/2})}$.

$v \leftarrow \textsc{Cvp}(\pi(W_{\mathsf{bk}}), \pi(\alpha))$

$\beta \leftarrow \alpha - v \cdot W_{\mathsf{bk}}$

$\gamma \leftarrow \textsc{PositiveOptim}(\beta)$

return $\mathfrak{L}^\gamma$.

Algorithm A.8 $\mathrm{CDW}^{\mathsf{explicit}}_{\text{pre-proc}}$: finding a generating family for the relative class group and generators for certain principal ideals

---

Input: a cyclotomic field K_m of conductor m and an integer d

Output: a family $\mathfrak{B} \leftarrow \{\mathfrak{L}_i^\sigma \mid \sigma \in G_m, i = 1, \ldots, d\}$ generating Cl^-_m and generators of the principal ideals $\{\mathfrak{L}_i^{\alpha_m(b)}\}_{i,b}$ ($\alpha_m(b) \in W_{\mathsf{bk}}$) and $\{\mathfrak{L}_i^{1+\tau}\}_i$

$d = \mathit{polylog}(m), B = \mathit{poly}(m)$

$\mathfrak{M} \leftarrow \{\mathfrak{L} \mid \mathcal{N}(\mathfrak{L}) \le B, [\mathfrak{L}] \in \mathrm{Cl}^-_m\}$

Choose $\mathfrak{L}_1, \ldots, \mathfrak{L}_d$ with smallest norm in $\mathfrak{M}$

$\mathfrak{B} \leftarrow \{\mathfrak{L}_i^\sigma \mid \sigma \in G_m, i = 1, \ldots, d\}$

Compute generators $\{\gamma^-_{\mathfrak{L}_i,b}\}_b$ st. $\mathfrak{L}_i^{\alpha_m(b)} = \langle \gamma^-_{\mathfrak{L}_i,b} \rangle$ for $\alpha_m(b) \in W_{\mathsf{bk}}$ and $i = 1, \ldots, d$ ▷ See Pr. 3.8

Compute generators $\{\gamma_r^+\}_r$ st. $\langle \gamma_r^+ \rangle = \prod_{i=1}^d \mathfrak{L}_i^{(1+\tau)r_i}$ for $r \in \mathbb{Z}[G_m^+]^d$ ▷ See Eq. (3.13) and Rem. 3.11

return $\mathfrak{B}$, $\{\gamma^-_{\mathfrak{L}_i,b}\}_{\substack{i=1,\ldots,d,\\ b \in M'_m}}$, $\{\gamma^+_{\mathfrak{L}_r}\}_{r \in \mathbb{Z}[G_m^+]}$

We first prove correctness of the new algorithms we introduced. Notably, we prove that prove that $\textsc{Cpm}^-$ returns the same result as $(\textsc{Cpm}^-)'$. Subsequently we deduce the correctness of algorithm $\mathrm{CDW}^{\mathsf{explicit}}$ which is splitted in a preprocessing phase (Alg. A.8) and then a query phase (Alg. A.9).

Algorithm A.9 $\mathrm{CDW}^{\mathsf{explicit}}_{\mathrm{query}}(\mathfrak{a})$: finding mildly short vectors in the ideal $\mathfrak{a}$

Input: an ideal $\mathfrak{a} \in \mathcal{O}_{K_m}$, a family $\mathfrak{B} \leftarrow \{\mathfrak{L}_i^\sigma \mid \sigma \in G_m, i = 1, \dots, d\}$ generating Cl_m^- and generators $\{\gamma^-_{\mathfrak{L}_i,b}\}_{\substack{i=1,\dots,d,\\ b \in M'_m}}$, $\{\gamma^+_{\mathfrak{L}_r}\}_{r \in \mathbb{Z}[G_m^+]}$

Output: an element $h \in \mathfrak{a}$ of norm $\|h\|_2 \le \exp(\tilde{O}(\sqrt{m})) \cdot \mathcal{N}(\mathfrak{a})^{1/\varphi(m)}$

$\mathfrak{b}' \leftarrow \mathrm{WalkToCl}^-(\mathfrak{a})$

$\xi, (y_{i,\sigma})_{\sigma \in G_m, i=1,\dots,d} \leftarrow \mathrm{ClDL}_{\mathfrak{B}}(\mathfrak{a}\mathfrak{b}')$ $\quad \triangleright\ \langle \xi \rangle \sim \mathfrak{a}\mathfrak{b}' \prod_{i,\sigma} (\mathfrak{L}_i^\sigma)^{y_{i,\sigma}}$

for $i = 1, \dots, d$ **do**

  $\xi_i \leftarrow \sum_{\sigma \in G_m} y_{i,\sigma}\sigma \in \mathbb{Z}[G_m]$

  $\mathfrak{L}_i^{\gamma_i} \leftarrow (\mathrm{CPM}^-)'(W_{\mathsf{bk}}, \mathfrak{L}_i, \xi_i)$

    where $\gamma_i = \xi_i - \sum_b v_{i,b}\alpha_m(b) - (1+\tau)r_i$

    for integers $(v_{i,b})_{b \in M'_m}$ and $r_i \in \mathbb{Z}[G_m^+]$

$g \leftarrow \alpha \Big/ \left(\gamma_r^+ \cdot \prod_{\substack{i=1,\dots,d\\ b \in M'_m}} (\gamma^-_{\mathfrak{L}_i,b})^{v_{i,b}} \right)$ where $r = (r_1, \dots, r_d) \in \mathbb{Z}[G_m^+]$

$h \leftarrow \mathrm{ShortGenerator}(\mathrm{g})$

return h

Corollary A.6. *Algorithm* $(\mathrm{CPM}^-)'$ *and* $\mathrm{CDW}^{\mathsf{explicit}}$ *are correct. Notably, let* $\mathfrak{L}$ *be a an ideal st.* $[\mathfrak{L}] \in \mathrm{Cl}_m^-$ *and* $\alpha \in \mathbb{Z}[G_m]$*, then, algorithms* CPM^- *and* $(\mathrm{CPM}^-)'$ *output the same result on input* $(W_{\mathsf{bk}}, \mathfrak{L}, \alpha)$.

Proof. Correctness of algorithm $(\mathrm{CPM}^-)'$ is a straightforward corollary of Pr. A.4, since this proposition essentially shows that using steps 2–5 of Alg. A.2 or subroutine PositiveOptim (Alg. A.6) returns the same element (and note that we use the same CVP solver in both CPM^- and $(\mathrm{CPM}^-)'$). This result is not dependant on W_{bk} and would have been true for the original generating family W from [CDW21]. For the correctness of $\mathrm{CDW}^{\mathsf{explicit}}$, we first use the fact that CPM^- and $(\mathrm{CPM}^-)'$ output the same result on input $(W_{\mathsf{bk}}, \mathfrak{L}, \alpha)$. Secondly, using results specific to W_{bk}, we note that §3.3 provides us with Stickelberger generators associated to the lattice basis W_{bk}. In other words, for any ideal $\mathfrak{L}_i$ of the basis, there exists elements $\{\gamma^-_{\mathfrak{L}_i,b}\}_b$ st. $\mathfrak{L}_i^{\alpha_m(b)} = \langle \gamma^-_{\mathfrak{L}_i,b} \rangle$ for $b \in M'_m$, using Pr. 3.8. Moreover, the ClDL algorithm from Biasse and Song (used in Alg. A.5) not only recovers the family $(y_{i,\sigma})_{\sigma \in G_m, i=1,\dots,d}$ but also the element $\xi \in \mathcal{O}_{K_m}$ such that:

$$\mathfrak{a}\mathfrak{b}' = \langle \xi \rangle \prod_{\substack{i=1,\dots,d\\ \sigma \in G_m}} (\mathfrak{L}_i^\sigma)^{-y_{i,\sigma}} = \langle \xi \rangle \prod_i \mathfrak{L}_i^{-\xi_i}$$

with the notation $\xi_i := \sum_{\sigma \in G_m} y_{i,\sigma}\sigma$ for $i = 1, \dots, d$. Now, for a fixed ideal $\mathfrak{L}_i$ ($i = 1, \dots, d$), on input $(\mathfrak{L}_i, \xi_i)$, algorithm $(\mathrm{CPM}^-)'$ returns an element $\mathfrak{L}_i^{\gamma_i}$ with $\gamma_i = \xi_i - \sum_{b \in M'_m} v_{i,b}\alpha_m(b) - (1+\tau)r_i$ where $(v_{i,b})_{b \in M'_m}$ is the vector with integral coordinates obtain by the CVP subroutine inside $(\mathrm{CPM}^-)'$, and $r_i \in \mathbb{Z}[G_m^+]$. It follows:

$$\mathfrak{a}\mathfrak{b}' \left(\prod_{i=1,\dots,d} \mathfrak{L}_i^{\gamma_i} \right) = \langle \xi \rangle \prod_{\substack{i=1,\dots,d\\ b \in M'_m}} \mathfrak{L}_i^{-\sum_b v_{i,b}\alpha_m(b)} \mathfrak{L}_i^{-(1+\tau)r_i}.$$

To conclude, recall from Eq. (3.11) and Rem. 3.11 that for $r = (r_1, \ldots, r_d) \in \mathbb{Z}[G_m]^d$, we have $\langle \gamma_r^+ \rangle = \prod_{i=1,\ldots,d} \mathfrak{L}_i^{(1+\tau)r_i}$. $\square$

In terms of calls to quantum algorithms, we replaced the last Pip in dimension n (for each query) by the computation of some generators during the preprocessing phase (step 6, Alg. A.8). Now, these generators can be all obtained by the computation of the real class group. Indeed, following [BS16, Th 1.1 and Alg. 1], we note that the computation of the class group reduces to the calculation of $\mathcal{S}$-units for a particular set $\mathcal{S}$. In particular, this implies that the calculation of the class group also yields, at the same time, the generators associated to those class relations. Finally, from [BS16, Alg. 2], we deduce that the cost of computing $\mathcal{S}$-units is similar to the cost of the Pip algorithm. Concretely, this means that computing the relations during the preprocessing has a quantum cost equivalent to the cost of a single query to the Pip algorithm in dimension $n/2$.

A.4 Avoiding the random walk

In the previous algorithms presented, in the original, as well as the first modification, working on the minus part of the class group is still required. Hence doing the random walk from Alg. A.1 is still required during the query phase. We note this random walk calls for polynomially (in $h^+_{K_m}$) many calls to the Pip algorithm (in dimension $n/2$), in order to test membership to Cl^-_m of candidate ideals by testing principality in $\mathcal{O}^+_{K_m}$ (of the images by the relative norm map $\mathcal{N}_{K_m/K_m^+}$). A possible theoretical solution to bypass those Pip calls is to use relations induced from relations on $\mathrm{Cl}_{K_m^+}$. These relations were introduced in §3.4 as $C^+_{\mathfrak{l}_1,\ldots,\mathfrak{l}_d}$ for ideals $\mathfrak{l}_1, \ldots, \mathfrak{l}_d$ associated to ideals $\mathfrak{L}_1, \ldots, \mathfrak{L}_d$ generating Cl_{K_m} and required the computation of the real class group. Using the same argument made at the end of the previous paragraph means that steps 3–4 of Alg. A.10 can be done using a single call to a $\mathcal{S}$-units computation, whose cost is equivalent to the a single call to Pip in dimension $n/2$.

One technical issue is that using relations coming from real classes does not let us use algorithm PositiveOptim anymore, yet we still need to recover an element $\gamma \in \mathbb{Z}[G_m]$ with nonnegative integer coordinates. We proceed “à la PHS” (or Tw-PHS) by computing a “drifted” Cvp, the added drift being chosen greater than the infinity decoding radius of the Cvp solver used. Like previous CDW and $\mathrm{CDW}^{\mathsf{explicit}}$ algorithms, the $\mathrm{CDW}^{\mathsf{no\text{-}walk}}$ algorithm is splitted in a preprocessing phase (Alg. A.10) followed by a query phase (Alg. A.11).

Proposition A.7. *Algorithm* $\mathrm{CDW}^{\mathsf{no\text{-}walk}}$ *is correct.*

Proof. The drifted Cvp algorithm described in step 3 ensures that g (given in step 4) is in $\mathfrak{a}$. Indeed, fix $i \in \{1, \ldots, d\}$. Note $z = [(v_{i,b})_{i,b}, (v'_r)_r] \cdot B$, by definition of the decoding radius D of the Cvp algorithm, $\|y + (\beta, \ldots, \beta) - z\|_\infty \leq D \leq \beta$. Taking coordinates, it follows that for any $i = 1, \ldots, d$ and $\sigma \in G_m$, $|y_{i,\sigma} + \beta - z_{i,\sigma}| \leq \beta$ and then $0 \leq y_{i,\sigma} - z_{i,\sigma} \leq 2\beta$. Since by definition,

Algorithm A.10 $\mathrm{CDW}^{\textsf{no-walk}}_{\text{pre-proc}}$: finding a generating family for the relative class group and generators for certain principal ideals

Input: a cyclotomic field K_m of conductor m

Output: a family $\mathfrak{B} \leftarrow \{\mathfrak{L}_i^\sigma \mid \sigma \in G_m, i = 1, \ldots, d\}$ generating Cl_{K_m}, the generators of the principal ideals $\{\mathfrak{L}_i^{\alpha_m(b)}\}_{i,b}$ $(\alpha_m(b) \in W_{\mathsf{bk}})$, the real class relations $C^+_{\mathfrak{l}_1,\ldots,\mathfrak{l}_d}$ for $\mathfrak{l}_i = \mathcal{N}_{K_m/K_m^+}(\mathfrak{L}_i)$ $(i = 1, \ldots, d)$ as well as the associated generators

1: Compute $\mathrm{Cl}_{K_m} = \langle \mathfrak{L}_1, \ldots, \mathfrak{L}_d \rangle$ with $d \leq \log(h_{K_m})$
2: Compute generators $\{\gamma^-_{i,b}\}_{i,b}$ st. $\mathfrak{L}_i^{\alpha_m(b)} = \langle \gamma^-_{i,b} \rangle$ for $\alpha_m(b) \in W_{\mathsf{bk}}$ and $i = 1, \ldots, d$ ▷ Using Pr. 3.8
3: Compute the real class relations $C^+_{\mathfrak{l}_1,\ldots,\mathfrak{l}_d}$ associated to ideals $\mathfrak{l}_i = \mathcal{N}_{K_m/K_m^+}(\mathfrak{L}_i)$ $(i = 1, \ldots, d)$ ▷ See §3.4
4: Compute generators $\{\gamma_r^+\}_r$ st. $\langle \gamma_r \rangle = \prod_{i=1}^d \mathfrak{L}_i^{(1+\tau)r_i}$ for $r = (r_1, \ldots, r_d) \in C^+_{\mathfrak{l}_1,\ldots,\mathfrak{l}_d}$
5: **return** $\mathfrak{B}$, $\{\gamma^-_{i,b}\}_{\substack{i=1,\ldots,d,\\ b \in M'_m}}$, $\{\gamma_r^+\}_{r \in C^+_{\mathfrak{l}_1,\ldots,\mathfrak{l}_d}}$

Algorithm A.11 $\mathrm{CDW}^{\textsf{no-walk}}_{\text{query}}(\mathfrak{a})$: finding mildly short vectors in the ideal $\mathfrak{a}$

Input: an ideal $\mathfrak{a}$ in $\mathcal{O}_{K_m}$, a family $\mathfrak{B} \leftarrow \{\mathfrak{L}_i^\sigma \mid \sigma \in G_m, i = 1, \ldots, d\}$ generating Cl_{K_m}, generators $\{\gamma^-_{i,b}\}_{\substack{i=1,\ldots,d,\\ b \in M'_m}}$, $\{\gamma_r^+\}_{r \in C^+_{\mathfrak{l}_1,\ldots,\mathfrak{l}_d}}$ and a drift β greater than the decoding radius of the CVP algorithm

Output: $h \in \mathfrak{a}$ of norm $\|h\|_2 \leq \exp\left(O\left(\max(\sqrt{\varphi(m)}, h^+_{K_m})\sqrt{\log m}\right)\right) \cdot \mathcal{N}(\mathfrak{a})^{1/\varphi(m)}$

1: $\alpha, y \leftarrow \mathrm{ClDL}_{\mathfrak{B}}(\mathfrak{a})$ where $y := (y_{i,\sigma})_{\sigma \in G_m, i=1,\ldots,d}$ ▷ $\langle \xi \rangle \sim \mathfrak{a} \prod_{i,\sigma} (\mathfrak{L}_i^\sigma)^{y_{i,\sigma}}$
2: Let $B = \mathcal{S}_m^d + (1+\tau) C^+_{\mathfrak{l}_1,\ldots,\mathfrak{l}_d}$
3: $v \leftarrow \mathrm{CVP}\big(B, y + (\beta, \ldots, \beta)\big)$, where $v := \left[(v_{i,b})_{1 \leq i \leq d, b \in M'_m}, (v_r)_{r \in C^+_{\mathfrak{l}_1,\ldots,\mathfrak{l}_d}}\right]$
4: $g \leftarrow \alpha \Big/ \left(\prod_{r \in C^+_{\mathfrak{l}_1,\ldots,\mathfrak{l}_d}} (\gamma_r^+)^{v_r} \prod_{1 \leq i \leq d, b \in M'_m} (\gamma^-_{\mathfrak{L}_i,c})^{v_{i,b}}\right)$
5: $h \leftarrow \mathrm{ShortGenerator}(g)$
6: **return** h

$\langle g \rangle = \mathfrak{a} \prod_{i,\sigma} (\mathfrak{L}_i^\sigma)^{y_{i,\sigma} - z_{i,\sigma}}$, the algorithm returns $g \in \mathfrak{a}$. We now use Th. A.3 with a minor adaptation of the proof from [CDW21, Th. 3.6]. In our situation,

$$\max_{w \in [W_{\mathsf{bk}} | C^+_{\mathfrak{l}_1,\ldots,\mathfrak{l}_d}]} \|w\|_2 = \max(\sqrt{\varphi(m)/2}, h^+_{K_m})$$

using Pr. 3.12 and that short elements of the basis W_{bk} have ℓ_2-norm equal to $\sqrt{\varphi(m)/2}$ (see Th. 3.7). It follows that if $h = \mathrm{ShortGenerator}(g)$, then:

$$\|h\|_2 \leq \mathcal{N}(g)^{1/\varphi(m)} \cdot \exp\left(O(\max(\sqrt{\varphi(m)}, h^+_{K_m})\sqrt{\log m}\right).$$

□

The quantum steps used in algorithms CDW, $\mathrm{CDW}^{\textsf{explicit}}$ and $\mathrm{CDW}^{\textsf{no-walk}}$ are summarized in Tab. A.1. We emphasize that the computation of the class group has a cost equivalent to the PIP algorithm (in the same dimension), since they both reduce to a single call to the computation of $\mathcal{S}$-units, for suitable sets $\mathcal{S}$ of prime ideals.

	Preproccessing phase Class group computation (dim. $n/2$)	Query phase		
		Pip (dim. n)	Pip (dim. $n/2$)	ClDl
CDW	0	1	$O(poly(h^+_{K_m}))$	1
CDW$^{\mathsf{explicit}}$	1	0	$O(poly(h^+_{K_m}))$	1
CDW$^{\mathsf{no\text{-}walk}}$	1	0	0	1

Table A.1 – Number of quantum steps used for algorithms CDW, CDW$^{\mathsf{explicit}}$ and CDW$^{\mathsf{no\text{-}walk}}$.

B Additional experimental results

B.1 Geometry of log-$\mathcal{S}$-unit sublattices

In the following, we provide data regarding the geometry of the log-$\mathcal{S}$-unit sublattices L_{urs} and L_{sat} for additional cyclotomic fields.

m	d	set	k	$\mathrm{Vol}^{1/k}$	δ_0 raw	δ_0 LLL	δ_0 bkz$_{40}$	δ raw	δ LLL	δ bkz$_{40}$
159	1	urs	155	11.291	0.998	0.998	0.998	2.177	1.706	1.672
		sat	155	8.989	1.000	1.000	1.000	6.143	1.894	1.905
	2	urs	259	12.576	0.999	0.999	0.999	2.350	1.786	1.732
		sat	259	9.572	1.000	1.000	1.000	6.902	2.024	2.024
	3	urs	363	13.364	0.999	0.999	0.999	2.419	1.809	1.754
		sat	363	9.978	1.000	1.000	1.000	7.602	2.064	2.064
149	1	urs	221	12.192	0.999	0.999	0.999	2.828	2.092	2.028
		sat	221	9.697	1.000	1.000	1.000	12.473	2.307	2.266
	2	urs	369	13.353	0.999	0.999	0.999	3.134	2.234	2.173
		sat	369	10.150	1.000	1.000	1.000	14.472	2.509	2.483
	3	urs	517	13.962	0.999	0.999	0.999	3.269	2.271	2.213
		sat	517	10.410	1.000	1.000	1.000	22.211	2.569	2.552
	4	urs	665	14.415	1.000	1.000	1.000	3.327	2.301	2.244
		sat	665	10.632	1.000	1.000	1.000	20.731	2.606	2.594
516	1	urs	251	11.815	1.000	0.999	0.999	2.535	2.029	2.008
		sat	251	9.395	1.001	1.000	1.000	6.508	2.342	2.354
	2	urs	419	12.921	1.000	0.999	0.999	2.833	2.155	2.128
		sat	419	9.818	1.000	1.000	1.000	8.208	2.549	2.557
	3	urs	587	13.850	1.000	0.999	0.999	2.945	2.202	2.166
		sat	587	10.321	1.000	1.000	1.000	10.348	2.617	2.615
	4	urs	755	14.445	1.000	0.999	0.999	2.998	2.221	2.194
		sat	755	10.650	1.000	1.000	1.000	12.682	2.649	2.650
181	1	urs	269	12.855	1.000	1.000	1.000	2.747	2.308	2.146
		sat	269	10.220	1.001	1.001	1.001	7.486	2.535	2.497
	2	urs	449	14.033	1.000	1.000	1.000	2.958	2.455	2.268
		sat	449	10.661	1.000	1.000	1.000	9.849	2.734	2.705
	3	urs	629	14.823	1.000	1.000	1.000	3.064	2.507	2.312
		sat	629	11.045	1.000	1.000	1.000	12.340	2.799	2.778
	4	urs	809	15.330	1.000	1.000	1.000	3.096	2.529	2.330
		sat	809	11.300	1.000	1.000	1.000	12.307	2.828	2.814
209	1	urs	269	10.796	1.000	0.999	0.999	2.678	2.237	2.226
		sat	269	8.583	1.001	1.000	1.000	8.273	2.601	2.600
	2	urs	449	12.651	1.000	0.999	0.999	2.921	2.317	2.317
		sat	449	9.612	1.000	1.000	1.000	14.860	2.731	2.723

m	d	set	k	$\mathrm{Vol}^{1/k}$	δ_0 raw	δ_0 LLL	δ_0 bkz$_{40}$	δ raw	δ LLL	δ bkz$_{40}$
217	1	urs	269	12.110	1.000	0.998	0.998	2.608	2.133	2.131
		sat	269	9.629	1.001	0.999	0.999	6.814	2.423	2.425
	2	urs	449	13.741	1.000	0.999	0.999	2.857	2.265	2.264
		sat	449	10.440	1.000	0.999	0.999	10.474	2.632	2.633
	3	urs	629	14.646	1.000	0.999	0.999	2.941	2.315	2.326
		sat	629	10.913	1.000	0.999	0.999	11.667	2.699	2.704
279	1	urs	269	12.059	1.000	1.000	0.999	2.573	2.077	2.071
		sat	269	9.588	1.001	1.001	1.000	11.575	2.392	2.397
	2	urs	449	13.528	1.000	1.000	0.999	2.836	2.213	2.197
		sat	449	10.278	1.000	1.000	1.000	12.899	2.606	2.605
	3	urs	629	14.378	1.000	1.000	0.999	2.965	2.267	2.247
		sat	629	10.713	1.000	1.000	1.000	16.966	2.680	2.683
	4	urs	809	14.971	1.000	1.000	1.000	3.010	2.285	2.260
		sat	809	11.036	1.000	1.000	1.000	17.733	2.712	2.709
	5	urs	989	15.396	1.000	1.000	1.000	3.053	2.299	2.278
		sat	989	11.271	1.000	1.000	1.000	18.878	2.731	2.730
297	1	urs	269	12.331	1.000	0.999	0.999	3.169	2.068	2.029
		sat	269	9.804	1.001	1.000	1.000	21.668	2.309	2.323
	2	urs	449	13.513	1.000	0.999	0.999	3.676	2.236	2.150
		sat	449	10.266	1.000	1.000	1.000	36.211	2.542	2.549
	3	urs	629	14.165	1.000	0.999	0.999	3.895	2.310	2.205
		sat	629	10.555	1.000	1.000	1.000	37.241	2.648	2.645
	4	urs	809	14.674	1.000	0.999	0.999	4.007	2.339	2.229
		sat	809	10.816	1.000	1.000	1.000	40.952	2.690	2.684
235	1	urs	275	11.873	1.000	0.998	0.998	2.631	2.187	2.141
		sat	275	9.439	1.001	0.999	0.999	7.618	2.476	2.475
	2	urs	459	13.287	1.000	0.998	0.998	2.936	2.348	2.285
		sat	459	10.094	1.000	0.999	0.999	12.645	2.705	2.701
	3	urs	643	14.178	1.000	0.999	0.999	3.061	2.404	2.319
		sat	643	10.563	1.000	0.999	0.999	13.258	2.779	2.769
	4	urs	827	14.743	1.000	0.999	0.999	3.099	2.427	2.342
		sat	827	10.867	1.000	0.999	0.999	13.861	2.811	2.803
564	1	urs	275	12.264	1.000	0.999	0.999	2.551	2.035	2.085
		sat	275	9.750	1.001	1.000	1.000	14.624	2.387	2.384
	2	urs	459	13.384	1.000	0.999	0.999	2.831	2.193	2.248
		sat	459	10.168	1.000	1.000	1.000	15.707	2.656	2.643
	3	urs	643	14.393	1.000	0.999	0.999	2.984	2.236	2.291
		sat	643	10.724	1.000	1.000	1.000	17.342	2.728	2.714
	4	urs	827	15.032	1.000	0.999	0.999	3.029	2.253	2.313
		sat	827	11.080	1.000	1.000	1.000	18.829	2.759	2.743

Table B.1 – Geometric characteristics of L_{urs} and L_{sat} for some cyclotomic fields with log-$\mathcal{S}$-embedding of type noiso/exp.

m	d	φ_{tw}-type	k	$\mathrm{Vol}^{1/k}$	δ_0 raw	δ_0 LLL	δ_0 bkz_{40}	δ raw	δ LLL	δ bkz_{40}
159	1	iso/exp	155	8.989	1.000	1.000	1.000	6.143	1.898	1.921
		iso/tw	155	10.088	1.001	1.001	1.001	7.533	2.117	2.143
		noiso/exp	155	8.989	1.000	1.000	1.000	6.143	1.894	1.905
		noiso/tw	155	10.088	1.001	1.001	1.001	7.533	2.119	2.139
	2	iso/exp	259	9.572	1.000	1.000	1.000	6.902	2.028	2.036
		iso/tw	259	10.258	1.001	1.001	1.001	8.805	2.313	2.337
		noiso/exp	259	9.572	1.000	1.000	1.000	6.902	2.024	2.024
		noiso/tw	259	10.258	1.001	1.001	1.001	8.805	2.317	2.334
	3	iso/exp	363	9.978	1.000	1.000	1.000	7.602	2.066	2.066
		iso/tw	363	10.484	1.000	1.000	1.000	9.857	2.373	2.397
		noiso/exp	363	9.978	1.000	1.000	1.000	7.602	2.064	2.064
		noiso/tw	363	10.484	1.000	1.000	1.000	9.857	2.376	2.392
149	1	iso/exp	221	9.697	1.000	1.000	1.000	12.473	2.305	2.244
		iso/tw	221	10.883	1.001	1.001	1.001	15.626	2.672	2.602
		noiso/exp	221	9.697	1.000	1.000	1.000	12.473	2.307	2.266
		noiso/tw	221	10.883	1.001	1.001	1.001	15.626	2.668	2.612
	2	iso/exp	369	10.150	1.000	1.000	1.000	14.472	2.507	2.467
		iso/tw	369	10.878	1.001	1.001	1.001	18.958	2.982	2.936
		noiso/exp	369	10.150	1.000	1.000	1.000	14.472	2.509	2.483
		noiso/tw	369	10.878	1.001	1.001	1.001	18.958	2.982	2.949
	3	iso/exp	517	10.410	1.000	1.000	1.000	22.211	2.569	2.531
		iso/tw	517	10.938	1.001	1.001	1.001	29.658	3.084	3.050
		noiso/exp	517	10.410	1.000	1.000	1.000	22.211	2.569	2.552
		noiso/tw	517	10.938	1.001	1.001	1.001	29.658	3.085	3.058
	4	iso/exp	665	10.632	1.000	1.000	1.000	20.731	2.606	2.576
		iso/tw	665	11.050	1.000	1.000	1.000	27.968	3.149	3.117
		noiso/exp	665	10.632	1.000	1.000	1.000	20.731	2.606	2.594
		noiso/tw	665	11.050	1.000	1.000	1.000	27.968	3.149	3.128
516	1	iso/exp	251	9.395	1.001	1.000	1.000	6.508	2.341	2.359
		iso/tw	251	10.544	1.002	1.001	1.001	8.112	2.739	2.733
		noiso/exp	251	9.395	1.001	1.000	1.000	6.508	2.342	2.354
		noiso/tw	251	10.544	1.002	1.001	1.001	8.112	2.730	2.739
	2	iso/exp	419	9.818	1.000	1.000	1.000	8.208	2.550	2.565
		iso/tw	419	10.522	1.001	1.000	1.000	10.682	3.059	3.062
		noiso/exp	419	9.818	1.000	1.000	1.000	8.208	2.549	2.557
		noiso/tw	419	10.522	1.001	1.000	1.000	10.682	3.055	3.064
	3	iso/exp	587	10.321	1.000	1.000	1.000	10.348	2.620	2.623
		iso/tw	587	10.845	1.001	1.000	1.000	13.713	3.168	3.167
		noiso/exp	587	10.321	1.000	1.000	1.000	10.348	2.617	2.615
		noiso/tw	587	10.845	1.001	1.000	1.000	13.713	3.169	3.167
	4	iso/exp	755	10.650	1.000	1.000	1.000	12.682	2.652	2.652
		iso/tw	755	11.068	1.000	1.000	1.000	16.973	3.221	3.219
		noiso/exp	755	10.650	1.000	1.000	1.000	12.682	2.649	2.650
		noiso/tw	755	11.068	1.000	1.000	1.000	16.973	3.221	3.220

TABLE B.2 – Geometric characteristics of L_{sat} for some cyclotomic fields. Comparison between choices iso/noiso and exp/tw.

B.2 Gram-Schmidt norms

Here, we provide figures showing the Gram-Schmidt log norms for other cyclotomic fields and number of orbits, comparing values before and after reduction.

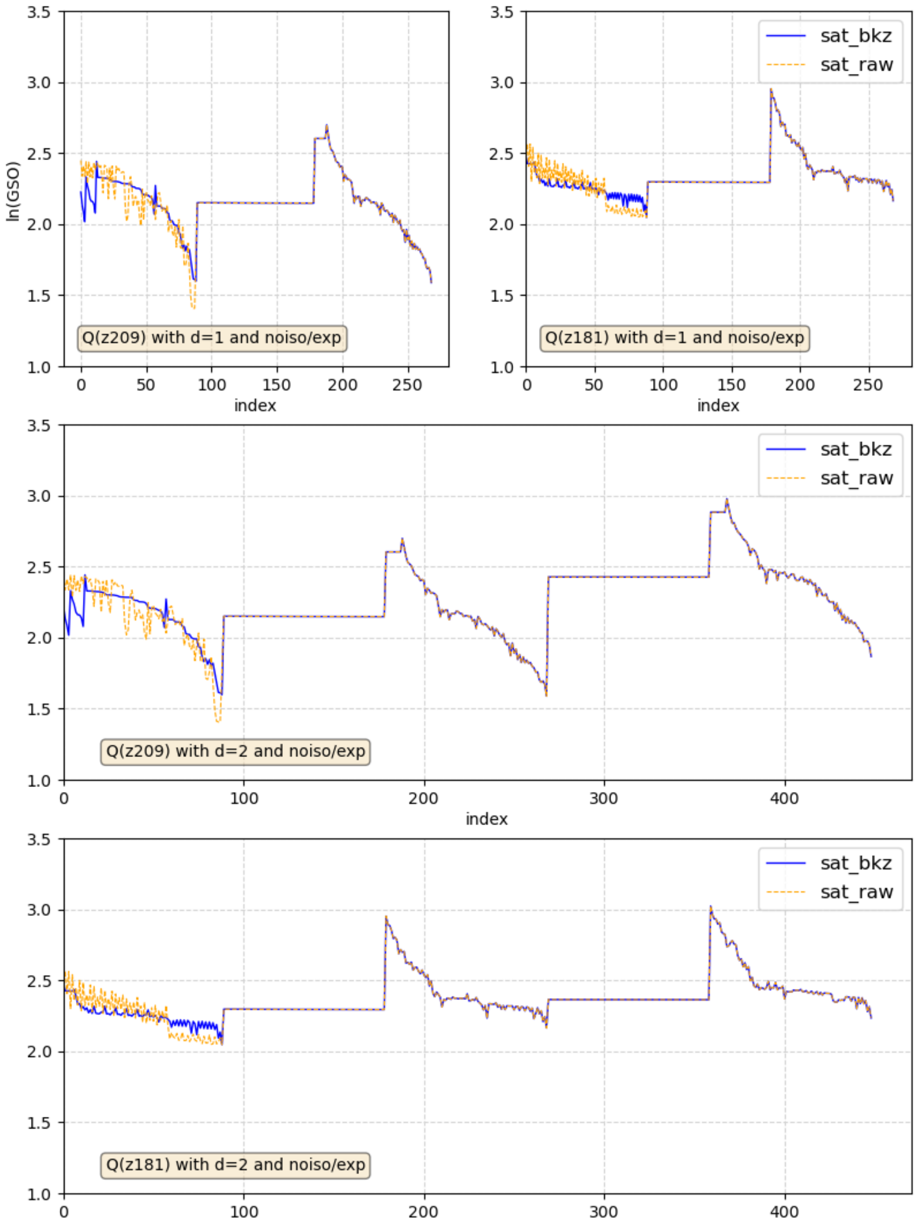

FIG. B.1 – L_{sat} lattices for $\mathbb{Q}(z_{209})$ and $\mathbb{Q}(z_{181})$: Gram-Schmidt log norms before and after reduction by BKZ$_{40}$, for $d = 1$ and $d = 2$ G_m-orbits.

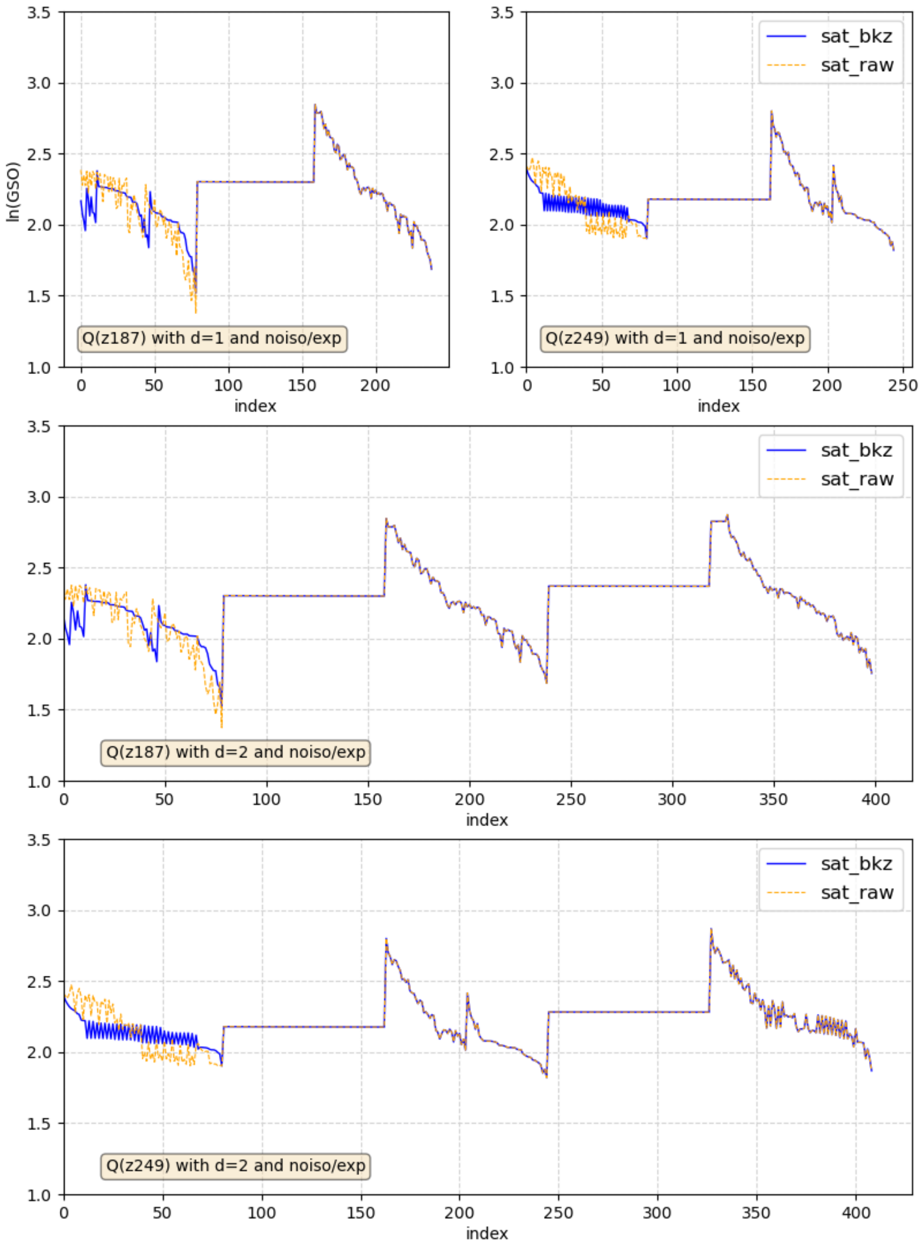

FIG. B.2 – L_{sat} lattices for $\mathbb{Q}(z_{187})$ and $\mathbb{Q}(z_{249})$: Gram-Schmidt log norms before and after reduction by BKZ_{40}, for $d = 1$ and $d = 2$ G_m-orbits.

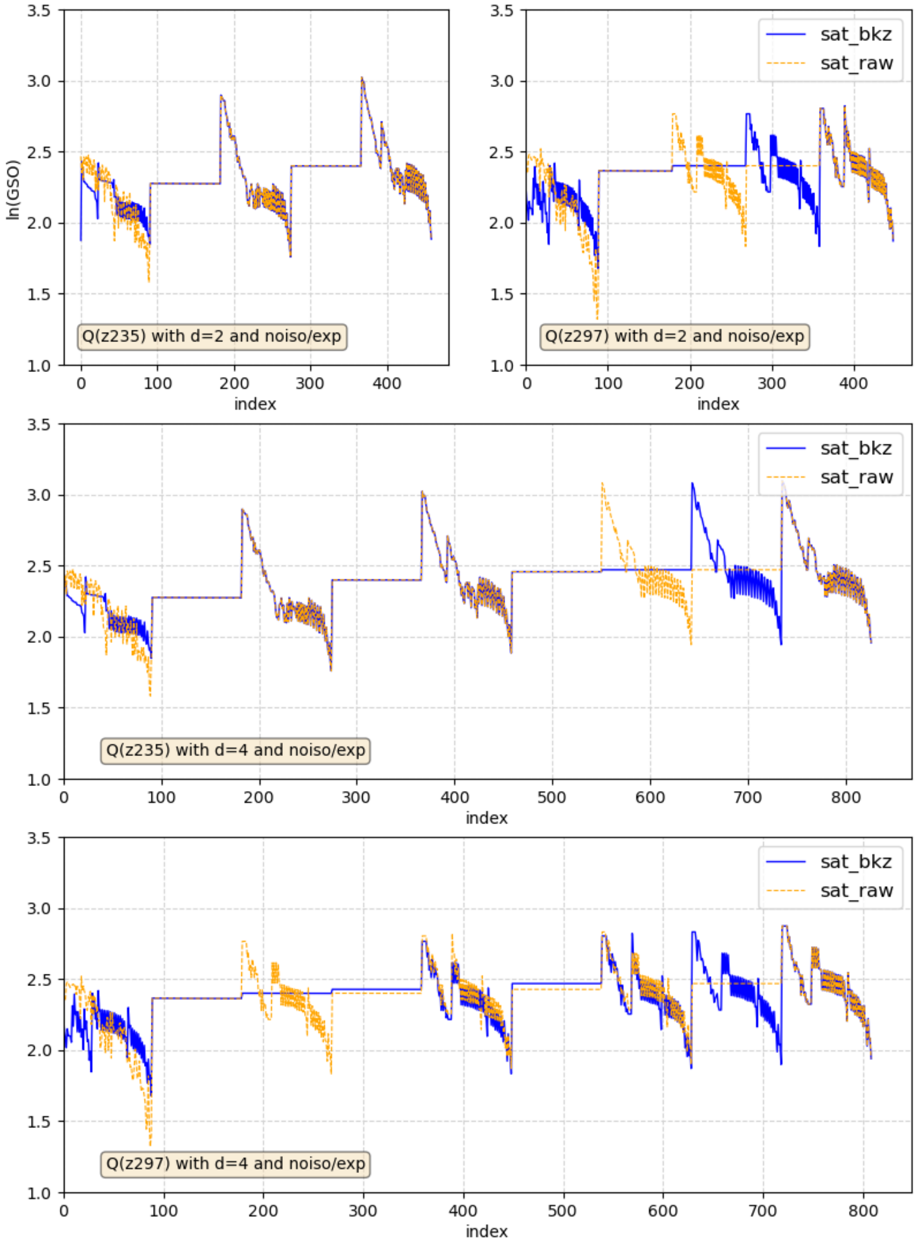

FIG. B.3 – L_{sat} lattices for $\mathbb{Q}(z_{235})$ and $\mathbb{Q}(z_{297})$: Gram-Schmidt log norms before and after reduction by BKZ_{40}, for $d = 2$ and $d = 4$ G_m-orbits.