On Algebraic Embedding for Unstructured Lattices

Madalina Bolboceanu * Zvika Brakerski † Devika Sharma †

Abstract

Efficient lattice-based cryptography usually relies on the intractability of problems on lattices with algebraic structure such as ideal-lattices or module-lattices. It is an important open question to evaluate the hardness of such lattice problems, and their relation to the hardness of problems on unstructured lattices.

It is a known fact that an unstructured lattice can be cast as an ideal-lattice in some *order* of a number field (and thus, in a rather trivial sense, that ideals in orders are as general as unstructured lattices). However, it is not known whether this connection can be used to imply useful hardness results for structured lattices, or alternatively new algorithmic techniques for unstructured lattices.

In this work we show that the Order-LWE problem (a generalization of the well known Ring-LWE problem) on certain orders is at least as hard as the (unstructured) LWE problem. So in general one should not hope to solve Order-LWE more efficiently than LWE. However, we only show that this connection holds in orders that are very "skewed" and in particular irrelevant for cryptographic applications. We then discuss the ability to embed unstructured lattices in "friendlier" orders, which requires devising an algorithm for computing the conductor of relevant orders. One of our technical tools is an improved hardness result for Order-LWE, closing a gap left in prior work.

*Bitdefender, Romania, mbolboceanu@bitdefender.com.

†Weizmann Institute of Science, Israel, {zvika.brakerski,devika.sharma}@weizmann.ac.il. Supported by the Binational Science Foundation (Grant No. 2016726), and by the European Union Horizon 2020 Research and Innovation Program via ERC Project REACT (Grant 756482) and via Project PROMETHEUS (Grant 780701).

Contents

1 Introduction

The Learning with Errors (LWE) problem, as defined by Regev [Reg05], is a convenient way to construct numerous cryptographic primitives such that their security is based on the hardness of solving worst-case lattice problems on integer lattices.[1] See [Pei16] for an exposition. The worst-case to average-case hardness reduction and the conjectured post-quantum security are the two appealing characteristics of the LWE problem.

However, there is a drawback of basing cryptographic primitives on LWE in practice. It induces relatively high computational complexity and large instance size; an LWE-based encryption scheme, for instance, has long keys and ciphertexts, along with high encryption complexity.

It was known since the introduction of the NTRU cryptosystems [HPS98] and more rigorously by the results in [LM06, PR06] that the efficiency of the lattice-based cryptosystems could be significantly improved by instead using lattices stemming from algebraic number theory. In [SSTX09], and then in [LPR10, LPR13], the authors defined the first known algebraic number theoretic analogs of LWE; Polynomial-LWE (PLWE) and Ring-LWE (RLWE), respectively. Roughly, they replaced the abelian group $\mathbb{Z}_q^n$ appearing in LWE by abelian groups that have an additional ring structure. For PLWE, it is the ring of polynomials $\mathbb{Z}[x]/(f(x))$, and for RLWE, it is the ring of integers $\mathcal{O}_K$ in a number field K. We will explain the properties of these algebraic objects below when needed. Similar to Regev's original result, the authors showed that each of these problems, PLWE and RLWE, is as hard as solving worst-case lattice problems on their respective *ideal* lattices, a special class of lattices that stems from embedding the number field into a Euclidean space, so that any ideal (and in fact any discrete subgroup) corresponds to a lattice.

Naturally, fixing a ring R, not all lattices can be expressed as ideals of R and therefore ideal lattices constitute a subset of the class of all lattices. Furthermore, these lattices have an additional algebraic structure which makes ideal-lattice problems potentially easier to solve than their counterparts on general lattices. Indeed, recently it has been shown that on some parameter regimes, state of the art quantum algorithms for ideal lattices asymptotically significantly outperform the best known (classical or quantum) algorithms for general lattices [CGS14, CDPR16, CDW17, DPW19, PHS19, BRL20].

Since the introduction of RLWE, various algebraically structured variants of the LWE problem have been defined, each with their own worst-case to average-case reduction: Module-LWE [LS12], Middle-Product LWE [RSSS17], and Order-LWE [BBPS19]. The Order-LWE problem, which will be of interest in this work, is a generalization of the Ring-LWE problem which is obtained by replacing the ring of integers in RLWE by one of its full-rank subrings, i.e., an order. Improving and extending the results from [RSW18], the authors in [PP19] proved that all the above mentioned variants are at least as hard as Ring-LWE (with some order-dependent penalty in the parameters). On the other hand, by merely forgetting the ring (or module) structure on these structured LWE problems, one obtains (multiple) LWE samples, thereby proving that all the algebraically structured LWE problems are not harder than the (unstructured) LWE. In this paper, we prove that every number field has certain orders such that their corresponding Order-LWE problem is equivalent to the unstructured LWE problem. Therefore, in a sense, Order-LWE can be viewed as a generalization of Regev's LWE, and thus encompasses all variants of LWE. The result emphasizes how devious certain algebraic structures can be, and that it would be naïve to assume that algebraic versions

[1] We prefer to keep the discussion at a high level at this point and not specify the exact lattice problem. In this context, relevant problems include Discrete Gaussian Problem (DGS), Shortest Independent Vectors Problem (SIVP) and Bounded distance decoding (BDD). See the supplementary material for definitions.

of unstructured problems are necessarily simpler. We note that, as expected, the orders in which Order-LWE is as hard as LWE do not seem to be useful for improving efficiency in cryptographic contexts. This is exactly the reason that allows us to prove this equivalence. Namely, the added noise which is needed for cryptographic applications (i.e. the "error" of LWE) "smudges" the algebraic structure of the order almost entirely.

There are various algebraic variants of LWE, with respective worst-case hardness reductions. However, the full set of integer lattices is not captured by the known reductions. To approach this gap, we would like to better understand the hardness of solving lattice problem on ideal lattices (where these hardness results apply) and integer lattices.[2] To this end, we embed integer lattices into number fields as ideals in their ring of multipliers and show that solving lattice problems on these ideal lattices is at most as hard as Order-LWE (regardless of whether they are invertible or not, contrary to prior works), the order being their respective ring of multipliers. We further exploit this embedding to analyze the quality of the algebraic structure induced on a (any) fixed integer lattice. We describe an algorithm to compute the conductor of the ring of multipliers, and consider an embedding optimal if the conductor is trivial, i.e., equals the ring of integers. We describe our work in more detail now.

1.1 This Work: General Lattices as Ideals

Making a lattice into an ideal lattice can be done as follows. Given a number field K over $\mathbb{Q}$ of degree n, the elements in K can be considered as formal polynomials of degree $(n-1)$ with rational coefficients. This induces a correspondence between (rational) n-dimensional vectors and field elements known as the *coefficient embedding* (from the field K into $\mathbb{Q}^n \subseteq \mathbb{R}^n$). Once a number field K is chosen and fixed, this correspondence allows to present any (rational) lattice as an additive *subgroup* of K, but not necessarily as an ideal in the aforementioned ring-of-integers. However, it is known that any such (discrete) subgroup $\mathcal{L}$ that corresponds to a full-rank lattice L in $\mathbb{Q}^n$ constitutes an ideal in some *full-rank subring* of the ring of integers. Such subrings are known as orders, and the maximal order in which the group $\mathcal{L}$ is an ideal is called its ring of multipliers, denoted as $\mathcal{O}_{\mathcal{L}}$.

The coefficient embedding is a way to map between (rational) lattices and elements of the number field and vice versa. However, in most algorithms and hardness reductions (all except [LM06, SSTX09]), ideals are mapped into lattices in $\mathbb{R}^n$ using a different embedding known as the canonical embedding (or Minkowski embedding). The canonical embedding allows for a cleaner transition between elements in number fields and vectors in the Euclidean space. However, it appears to be less suitable for our goal of mapping *arbitrary lattices* into ideals. The reason is that the canonical embedding does not map elements in the number field to rational vectors (i.e., the image of the number field is not contained in $\mathbb{Q}^n$). Therefore, we are forced to consider both embeddings: we map lattices into ideals using the (inverse) coefficient embedding, and then consider (for the sake of algorithms and hardness) the lattice that is induced by applying the canonical embedding on the ideal. This incompatibility of embeddings creates a distortion between the lattice on which we want to solve the problem (the coefficient embedding of the ideal) and the lattice on which we actually attempt to solve it (the canonical embedding of the ideal). This distortion, which depends on the number field, can be quantified and bounded.[3] We study this

[2] Indeed, we show above that in some cases it is possible to relate Order-LWE to LWE directly but the question about the relation between ideal lattices and general integer lattices remains relevant nonetheless.

[3] We note that in some special cases this distortion (up to scaling) does not exist. Most notably in power-of-two

introduction of the algebraic structure and alteration of the geometric structure on L, in fair detail in Section 3.

Recall that [BBPS19] showed a connection between solving the Order-LWE problem and solving lattice problems on ideals of that order. We could therefore hope that the above embedding would imply that for any lattice (respectively distribution over lattices) there exists an order (respectively distribution over orders) for which Order-LWE is at least as hard as solving short vector problems on this lattice (or distribution). Alas, [BBPS19] only relates the hardness of Order-LWE with the hardness of *invertible* ideal lattices in the order. We recall that an ideal in the ring is invertible if it has an inverse which is also a (possibly fractional) ideal in the ring. While all ideals of the ring of integers are invertible, this is not necessarily the case for ideals of orders. Although a naive sounding restriction, it left the infinite set of non-invertible ideals uncaptured by an important average-case problem. In particular, the lattice $\mathcal{L}$ is not necessarily invertible in its ring of multipliers and therefore prior to this work the above derivation could not be made.

In Section 4, we improve the existing hardness result for Order-LWE to show that this problem is as hard as solving lattice problems on all ideal lattices of the order, under a regularity condition on the Order-LWE modulus. The approximation factor obtained is identical to the one in [BBPS19]. The novelty of this improvement is our generalization of the so-called cancellation lemma that is in the heart of ideal lattice hardness results such as [LPR10, PRSD17, BBPS19].

The cancellation lemma provides a way to map a lattice point into its coefficient vector with respect to a basis of another, fixed and perhaps denser, lattice. The coefficient vector will constitute the LWE secret s. In order to preserve the algebraic structure, this needs to be done via multiplication by a field element. Prior results used the invertibility of the ideal to show that this is possible. In order to obtain a similar result for non-invertible ideals, we first observe that any non-invertible ideal $\mathcal{L}$ can be viewed as a sublattice of an invertible ideal $\mathfrak{p}$. We can thus apply the cancellation lemma using $\mathfrak{p}$ and map between elements of $\mathcal{L}$ and elements of $\mathfrak{p}$ using the inclusion relation. This relation is of course not an isomorphism, however in the context of Order-LWE reduction, what we need is an isomorphism between the modulo q versions of these ideals (where q is the LWE modulus). Indeed we show that under a regularity condition (specifically, $(q, [\mathcal{O}_K : \mathcal{O}_\mathcal{L}]) = 1$, i.e., q is coprime to the index of the order inside the ring of integers), the inclusion relation between the ideals implies an isomorphism modulo q. This suffices to allow the proof to go through. Using similar techniques we can also show (under the same condition) an equivalence between two variants of Order-LWE that were defined in [BBPS19] (a primal and dual variant).

Lastly, in Section 4, we also extend the Ring-LWE hardness result. The strengthened result now includes solving lattice problems (DGS) for lattices that are not necessarily ideals in the ring of integers, but rather ideals in orders whose index is coprime with the Ring-LWE modulus. This comes at a cost on the approximation factor (for DGS) if the lattice is not an $\mathcal{O}_K$-ideal. The cost is directly related to the conductor of the ring of multipliers of the lattice.[4] This result generalizes the Order-LWE to RLWE reduction proved in [BBPS19, Cor 5.2]. The above results hold for any number field K. See Section 4 for full statements and proofs.

In Section 5, we show that every number field has chain(s) of orders beginning from $\mathcal{O}_K$ such that their corresponding Order-LWE problems become (not necessarily strictly) harder. We prove that this gradient of hardness terminates at special 'skewed' orders. That is, we show that Order-

cyclotomic number fields.

[4]The conductor of an order is the maximal ideal which is shared between the order and the ring of integers. Properties of the conductor are often used to relate the order and the ring of integers.

LWE corresponding to these orders is equivalent to the unstructured LWE problem. More precisely, we show that for "reasonable" Gaussian noise, from say D_α, the noise in the Order-LWE sample drowns the last $n-1$ coordinates of the Order-LWE instance. Thus only one coefficient survives, which is distributed like a (standard) LWE sample with a related noise parameter. We call such orders α-drowning and describe a recipe to construct them.

In Section 6, we move on to consider the case of p-ary lattices. Such lattices are important since it is known that general lattice problems reduce to p-ary lattice problems (e.g. LWE). See [Ajt96, Reg09]. We specifically consider the case where p is prime and zoom-in on the embedding of such lattices in a number field. Recall that our results from Section 4 imply that order-ideal lattice problems can be solved using RLWE oracle, but with some loss in the approximation factor. This loss is related to the conductor of the ring of multipliers and can roughly be related to the index $[\mathcal{O}_K : \mathcal{O}]$. We expect this loss to be too great for most p-ary lattices, however it is possible that for some class of p-ary lattices the loss will be small enough so that relating their hardness to RLWE is meaningful. To this end we develop an algorithm that, given a p-ary lattice as input, computes the conductor of its ring of multipliers efficiently (as a product of prime ideals). Such an algorithm may find other uses in the context of computational aspects of algebraic number theory. Our algorithm and analysis are specific to so-called monogenic number fields, but we explain its consequences in the non-monogenic setting as well. Lastly, we show that, as expected, in the case of a power-of-two cyclotomic field, most p-ary lattices will not have a "favorable" conductor in terms of the effect on the approximation factor.

1.2 Technical Overview

In this section we provide a somewhat more technical outline of our results in Sections 4, 5, 6. To keep this overview simple, we present all the algebraic results for the case of a power-of-two cyclotomic field, i.e., $K = \mathbb{Q}[x]/(x^n+1)$, where n is a power of two. We will specify when the result holds in more generality, and urge the enthusiastic reader to seek details in the relevant section.

We begin with a brief description of the LWE problem: a secret vector $\mathbf{s}$ is sampled from $\mathbb{Z}_q^n$, for a modulus q and an adversary gets access to an oracle that outputs pairs of the form $(\mathbf{a}, b = \frac{1}{q}\langle \mathbf{a}, \mathbf{s}\rangle + \mathbf{e} \mod \mathbb{Z})$, for a uniform $\mathbf{a} \in \mathbb{Z}_q^n$ and a small 'noise' $\mathbf{e} \in \mathbb{R}/\mathbb{Z}$, that typically follows a Gaussian distribution. The goal of the adversary is to distinguish this oracle from the one that outputs $(\mathbf{a}, b)$, with b uniform over $\mathbb{R}/\mathbb{Z}$. The Ring-LWE setup is described in a more algebraic environment, where the sample spaces are algebraic objects isomorphic to $\mathbb{Z}_q^n$. It is well-known that the *ring of integers* of K is the ring of integer polynomials $\mathcal{O}_K := \mathbb{Z}[x]/(x^n+1)$. Observe that $\mathcal{O}_K$ is a $\mathbb{Z}$-module of rank n, much like an integer lattice. Further, one can also define the dual $\mathcal{O}_K^\vee$ of $\mathcal{O}_K$, exactly like the dual of a lattice.[5] There is a canonical way of embedding the field K into $\mathbb{R}^n$ (more accurately, a copy of $\mathbb{R}^n$ that lies inside $\mathbb{C}^n$), with the so called Minkowski embedding of K. The $\mathbb{R}$-vector space generated by the image of K is denoted by $K_\mathbb{R}$. Under this embedding one can view ideals in K as lattices in $K_\mathbb{R}$. For a modulus q, the Ring-LWE problem is defined as follows: for a secret polynomial $s \in \frac{\mathcal{O}_K^\vee}{q\mathcal{O}_K^\vee}$, the adversary gets access to an oracle that outputs pairs of the

[5] Formally this is done by replacing the Euclidean inner product by its number-theoretic analog, the bilinear Trace map $Tr : K \times K \to \mathbb{Q}$. The trace coincides with the Hermitian inner product on the Minkowski space $K_\mathbb{R}$, as $\langle \sigma(x), \overline{\sigma(y)} \rangle := Tr(xy)$, where $\sigma(x)$, $\sigma(y)$ are the images of x, y in $K_\mathbb{R}$, respectively, and $\overline{\sigma(y)}$ is the complex conjugate of $\sigma(y)$.

form

$$(a, \frac{1}{q} \cdot a \cdot s + e) \in \frac{\mathcal{O}_K}{q\mathcal{O}_K} \times \frac{K_{\mathbb{R}}}{\mathcal{O}_K^\vee}$$

where a is drawn uniformly over $\frac{\mathcal{O}_K}{q\mathcal{O}_K}$, and e is drawn from a small Gaussian over $K_{\mathbb{R}}$. Intuitively, in this case, e can be thought of as a polynomial with very small coefficients. The goal of the adversary here is to distinguish between the output of this oracle and the output of an oracle that gives uniform pairs over the same domain.

The Order-LWE problem is a genuine generalization of the Ring-LWE problem. For, once $\mathcal{O}_K$ is replaced by an *order*, a full rank sub-ring of $\mathcal{O}_K$, the problem is defined exactly as above. Some simple examples of orders to keep in mind could be the ring $\mathcal{O}_K$ itself, or $\mathbb{Z} + d\mathcal{O}_K$, for any integer d, or the ring of integer polynomials modulo f, $\mathbb{Z}[x]/(f)$, if the field in discussion is defined as $K = \mathbb{Q}[x]/(f)$.

Extended hardness result of Order-LWE (Section 4). The authors in [BBPS19] defined the Order-LWE problem and showed that this problem is as hard as solving lattice problems on the 'invertible' ideal (lattices) of the Order. When specialized to the order $\mathcal{O}_K$, this is the hardness result as proved in [LPR10, PRSD17], where there is no mention of invertibility of the ideal lattices considered, since all $\mathcal{O}_K$-ideals are invertible. This distinction only arises when working with ideals of a proper order $\mathcal{O}$ ($\neq \mathcal{O}_K$). As the proof of the $\mathcal{O}$-LWE hardness result given in [BBPS19] followed the exact same blueprint described for the hardness of Ring-LWE, it needed to convert BDD (Bounded Distance Decoding) samples on $\mathcal{O}$-ideals to LWE samples. Prior to this work, this conversion was accomplished by using the so-called Cancellation lemma, which necessarily required the ideal to be invertible. That was the only reason the $\mathcal{O}$-LWE hardness result needed to be restricted to this sub-class of $\mathcal{O}$-ideals. In this work, we show that the conclusion of the cancellation lemma holds even if the ideal is not invertible, as long as we choose the modulus q to be coprime to the index $[\mathcal{O}_K : \mathcal{O}]$. We use the generalization of ideal factorization, known as Jordan-Hölder filtration for a non-invertible ideal $\mathcal{I} \subseteq \mathcal{O}$, to show that there exists an invertible ideal $\mathfrak{p}$ such that $\mathcal{I} \subseteq \mathfrak{p} \subseteq \mathcal{O}$ and the index $[\mathfrak{p} : \mathcal{I}]$ is coprime to q. The coprimality condition implies an isomorphism $\mathcal{I}/q\mathcal{I} \simeq \mathfrak{p}/q\mathfrak{p}$. Composing this isomorphism with the cancellation lemma, for $\mathfrak{p}$ now is invertible in $\mathcal{O}$, we get that $\mathcal{I}/q\mathcal{I} \simeq \mathcal{O}/q\mathcal{O}$.[6] This is exactly what was missing in the hardness proof in [BBPS19], as the rest of the argument is exactly as it is there. Under the coprimality condition, $(q, [\mathcal{O}_K : \mathcal{O}]) = 1$, we also show that the dual and the primal $\mathcal{O}$-LWE problems are equivalent, thereby further strengthening the hardness result for the dual $\mathcal{O}$-LWE problem, as well.

In this section, we also extend the Ring-LWE hardness result. We described the details of the strengthened results previously. See the introduction above.

Equivalence of Order-LWE and (unstructured) LWE (Section 5). Let K be the power-of-two cyclotomic and let p be a prime such that $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_n$, where $\mathfrak{p}_i$'s are prime ideals in $\mathcal{O}_K$. Then, the following chain of orders exists

$$\mathcal{O}_K \supseteq \mathbb{Z} + \mathfrak{p}_1 \supseteq \mathbb{Z} + \mathfrak{p}_1\mathfrak{p}_2 \supseteq \dots \supseteq \mathbb{Z} + \mathfrak{p}_1 \cdots \mathfrak{p}_{n-1} \supseteq \mathbb{Z} + p\mathcal{O}_K$$

[6] A concurrent work, namely an updated version of [PP19], showed that Cancellation Lemma also holds for non-invertible ideals, but requires instead *invertibility modulo an ideal* $\mathcal{J}$. In our case, this ideal $\mathcal{J}$ is $q\mathcal{O}$ and they remark that all fractional ideals are invertible modulo $q\mathcal{O}$, due to the coprimality condition, $(q, [\mathcal{O}_K : \mathcal{O}] = 1)$. Therefore, this lemma provides an isomorphism $\mathcal{O}/q\mathcal{O} \simeq \mathcal{I}/q\mathcal{I}$, for all fractional ideals $\mathcal{I}$ and thus, an alternative proof to ours.

As proven in [PP19, Thm. 4.3], for orders $\mathcal{O}' \subseteq \mathcal{O}$, there is an error preserving reduction from $\mathcal{O}$-LWE to $\mathcal{O}'$-LWE, as long as the modulus q is coprime to $[\mathcal{O} : \mathcal{O}']$. Therefore we can derive the following chain of error preserving reductions, as long as $(p, q) = 1$,

$$\mathcal{O}_K\text{-LWE} \to \mathbb{Z} + \mathfrak{p}_1\text{-LWE} \to \ldots \to \mathbb{Z} + \mathfrak{p}_1 \cdots \mathfrak{p}_{n-1}\text{-LWE} \to (\mathbb{Z} + p\mathcal{O}_K)\text{-LWE}$$

Observe that the $\mathbb{Z}$-basis of the order $\mathbb{Z} + p\mathcal{O}_K$ is given by the set $\{1, p\zeta, \ldots p\zeta^{n-1}\}$, as $\mathcal{O}_K = \mathbb{Z}[\zeta]$, with ζ a primitive root of unity. For a large p, one of these basis elements is much shorter than the rest. It is in this sense that we call this order 'skewed'. We show that this skewed order is α-drowning. That is, for $p \geq \frac{1}{\alpha}$, the error sampled from a spherical Gaussian distribution D_α over $K_\mathbb{R}$ drowns the last $n-1$ coordinates of $K_\mathbb{R}/\mathcal{O}^\vee$ and it is only the coefficient corresponding to the basis element 1 that survives, in this Order-LWE sample, and looks like the second coordinate of an LWE sample. This implies that the Order-LWE problem corresponding to $\mathbb{Z}+p\mathcal{O}_K$ is equivalent to the unstructured LWE problem. To get an intuitive idea of the proof that $\mathbb{Z} + p\mathcal{O}_K$ is α-drowning, observe that the set $(\mathbb{Z} + p\mathcal{O}_K)^\vee$, in this special case, looks like

$$(\mathbb{Z} + p\zeta\mathbb{Z} + \ldots + p\zeta^{n-1}\mathbb{Z})^\vee = \frac{1}{n}\mathbb{Z} + \frac{1}{pn}\zeta\mathbb{Z} + \ldots + \frac{1}{pn}\zeta^{n-1}\mathbb{Z}$$

Consider a noise term e drawn from a spherical (in $K_\mathbb{R}$) Gaussian D_α.[7] Its coefficients in this basis are Gaussian with a diagonal covariance matrix whose diagonal entries are $(\alpha^2 n, \alpha^2 p^2 n, \ldots, \alpha^2 p^2 n)$. In the specified choice of parameters, $\alpha p\sqrt{n}$ is greater than the smoothing parameter of $\mathbb{Z}$, thereby proving that the last $n-1$ coefficients of e are indistinguishable from uniform elements in $\mathbb{R}/\mathbb{Z}$. Whereas the first coefficient looks like a part of a LWE-sample with error from $D_{\alpha\sqrt{n}}$. In Section 5, we describe α-drowning orders in any number field K and show that Order-LWE corresponding to them is equivalent to LWE. The proof, in this general case, requires a more involved analysis since the covariance matrix of the Gaussian over the basis of the order is not in general diagonal which makes it much more difficult to analyze.

Finding the conductor of rings of multipliers for p-ary lattices (Section 6). We embed p-ary integer lattices into number fields to analyze the hardness and the possibility of solving short vector problems on it. An integer lattice L is said to be p-ary if it is periodic mod p, where p is a rational integer. Common examples are the lattices that are induced by the LWE [Reg05] or SIS [Ajt96] problems. We consider the specific case where p is prime. The aforementioned results show that solving lattice problems on p-ary lattices implies that they can be solved on arbitrary lattices, and therefore it is still useful to consider this seemingly restricted class of lattices.

We show that $\mathcal{L}$, the embedding of a p-ary lattice L, is always an ideal of the order $\mathbb{Z} + p\mathcal{O}_K$. Recall that, in the power of two cyclotomic, the Order-LWE problem for $\mathbb{Z} + p\mathcal{O}_K$ is as hard as the LWE problem, so solving lattice problems on $\mathcal{L}$ is still as hard as solving the unstructured LWE. Therefore, so far, the additional algebraic structure does not improve the chances of solving lattice problems on L. But this order, $\mathbb{Z} + p\mathcal{O}_K$, might not be the full ring of multipliers for $\mathcal{L}$. Let $\mathcal{O}_\mathcal{L}$ denote the ring of multipliers and let $\mathcal{C}_\mathcal{L}$ be its conductor ideal: it is the set of all elements in $\mathcal{O}_\mathcal{L}$ such that multiplying $\mathcal{O}_K$ by them embeds $\mathcal{O}_K$ into $\mathcal{O}_\mathcal{L}$. We use the fact that the conductor is the largest $\mathcal{O}_K$-ideal contained in $\mathcal{O}_\mathcal{L}$ to conclude that $\mathcal{C}_\mathcal{L} \mid p\mathcal{O}_K$. This is the starting point

[7] The Order-LWE problem is often considered with noise that is sampled from an elliptical Gaussian, or even a family of elliptical Gaussians, but we can simply consider the largest spherical Gaussian that is contained in that distribution.

for the algorithm described in Section 6, that on input the HNF basis for L, outputs the prime decomposition $\mathcal{C}_{\mathcal{L}}$ into prime ideals sitting over $p\mathcal{O}_K$ in K. The correctness of the algorithm relies on the interplay between ideal decomposition in $\mathcal{O}_K$ and factorization of the polynomial $x^n + 1$ in $\mathbb{F}_p[x]$. The algorithm also reveals information about the conductor in non-monogenic fields, under a coprimality condition. See the discussion before Subsection 6.1 for details.

Preservation of the geometry when (coefficient) embedding p-ary integer lattices into the power of two cyclotomic extension was lucrative enough a reason for us to measure the proportion of the subset of p-ary lattices whose conductor equals $p\mathcal{O}_K$, to the full set of p-ary lattices. In Subsection 6.2, we fix an integer $k \leq n$ and count the number of p-ary lattices, L of determinant equal to p^k such that $\mathcal{C}_{\mathcal{L}} = p\mathcal{O}_K$. We find that this set is significantly large in size.

2 Preliminaries

We describe the well-known results and the standard notations. Given a distribution D, when writing $x \leftarrow D$, we mean an element x sampled from this distribution. Given a set X, we denote by $U(X)$, the uniform distribution over this set. For a vector $\mathbf{x} \in \mathbb{C}^n$, we let $\|\mathbf{x}\|$ be its Euclidean norm, defined as $\|\mathbf{x}\| = (\sum_{i=1} |x_i|^2)^{1/2}$. We denote by $(\mathbf{e}_i)_{1 \leq i \leq n}$ the canonical basis of $\mathbb{R}^n$, where $\mathbf{e}_i$ is the vector with 1 on the i-th entry and zeros elsewhere. For a prime integer p, we denote by $\mathbb{F}_p$, the finite field with p elements, which is identified with the ring of residue classes modulo p, $\mathbb{Z}_p$. We use the standard big-O notation for classifying the growth of functions and say $f(n) = \widetilde{O}(g(n))$ if $f(n) = O(g(n) \cdot \log^c n)$, for a constant factor c. We also let $f(n) = poly(n)$, for $f(n) = O(n^c)$ and a constant c.

2.1 The Space H

To be able to speak about the geometric properties of a number field K, we embed it into the following space,

$$H = \{\mathbf{x} \in \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2} | x_{s_1+s_2+j} = \overline{x_{s_1+j}}, \text{ for any } 1 \leq j \leq s_2\}.$$

H is an n-dimensional vector space over $\mathbb{R}$, equipped with the inner product induced on $\mathbb{C}^n$, and hence isomorphic to (a copy of) $\mathbb{R}^n$. It has a special orthonormal basis $(\mathbf{h}_i)_{1 \leq i \leq n}$ given by the columns of the following matrix:

$$B = \begin{pmatrix} \mathrm{Id}_{s_1 \times s_1} & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}}\mathrm{Id}_{s_2 \times s_2} & \frac{i}{\sqrt{2}}\mathrm{Id}_{s_2 \times s_2} \\ 0 & \frac{1}{\sqrt{2}}\mathrm{Id}_{s_2 \times s_2} & \frac{-i}{\sqrt{2}}\mathrm{Id}_{s_2 \times s_2} \end{pmatrix}$$

This is the space $K_{\mathbb{R}}$, up to an isomorphism, mentioned in the introduction.

2.2 Lattices

Given a finite dimensional vector space V over $\mathbb{R}$ (e.g. $\mathbb{R}^n$ or $H \subseteq \mathbb{C}^n$) a $\mathbb{Z}$-lattice $\mathcal{L}$ is an (discrete) additive group generated by a set (basis) $B = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\} \subseteq V$ of elements that are linearly independent over $\mathbb{R}$. In other words,

$$\mathcal{L} := \{\sum_{i=1}^{k} a_i \mathbf{v}_i : a_i \in \mathbb{Z}, \mathbf{v}_i \in B\}$$

The integer k is called the rank of the lattice $\mathcal{L}$ and when $k = \dim_{\mathbb{R}} V$, the lattice L is said to be of full rank. The *determinant* of the lattice, $\det(\mathcal{L}) := \sqrt{\det(\langle \mathbf{v}_i, \mathbf{v}_j \rangle)_{i,j}}$, and is independent of the choice of the basis. Under the inner product of V, the dual lattice $\mathcal{L}^*$, is of the same rank as $\mathcal{L}$, and is defined as

$$\mathcal{L}^* := \{\mathbf{v} \in V : \langle \mathbf{v}, \mathbf{x} \rangle, \in \mathbb{Z} \ \ \forall \mathbf{x} \in \mathcal{L}\}$$

Let $B(0, r)$ denote the closed Euclidean ball of radius r around 0. The successive minimum of the lattice $\mathcal{L}$ is defined as

$$\lambda_i(\mathcal{L}) := \inf\{r > 0 : \mathrm{rank}_{\mathbb{Z}}(\mathrm{span}_{\mathbb{Z}}(\mathcal{L} \cap B(0, r))) > i\}$$

Lemma 2.1 ([Ban93]). $1 \leq \lambda_1(\mathcal{L}) \cdot \lambda_n(\mathcal{L}^*) \leq n$.

2.2.1 Gaussians and Smoothing Parameter facts

Let V be a real inner product space of dimension n with an orthonormal basis $(\mathbf{v}_i)_{1 \leq i \leq n}$, e.g., $\mathbb{R}^n$ with the canonical basis or H with the basis B. We identify an element $x \in V$ in a unique way with a vector $\mathbf{x} \in \mathbb{R}^n$, of its coordinates with respect to this basis. Recall that a symmetric matrix $\Sigma \in M_n(\mathbb{R})$ is said to be *(semi) positive definite* if $\mathbf{x}^T \Sigma \mathbf{x} > 0$ (or $\mathbf{x}^T \Sigma \mathbf{x} \geq 0$, resp.), for any non-zero $\mathbf{x} \in \mathbb{R}^n$. This property puts a partial order on the set of symmetric matrices; $\Sigma_1 \geq \Sigma_2$ if $\mathbf{x}^T(\Sigma_1 - \Sigma_2)\mathbf{x} \geq 0$, for any non-zero $\mathbf{x} \in \mathbb{R}^n$.

Definition 2.2. *For a positive definite matrix $\Sigma \in M_n(\mathbb{R})$ and a mean vector $\boldsymbol{c} \in \mathbb{R}^n$, define the Gaussian function $\rho_{\boldsymbol{c},\sqrt{\Sigma}} : V \to (0, 1]$ as $\rho_{\boldsymbol{c},\sqrt{\Sigma}}(x) = e^{-\pi(\boldsymbol{x}-\boldsymbol{c})^T \Sigma^{-1}(\boldsymbol{x}-\boldsymbol{c})}$. We denote by $D_{\boldsymbol{c},\sqrt{\Sigma}}$, the normalized continuous Gaussian distribution over V corresponding to $\rho_{\boldsymbol{c},\sqrt{\Sigma}}$.*

When $\mathbf{c}$ is the zero vector, it is dropped from the subscript. When $\Sigma = \mathrm{diag}(r_i^2)$, for some $\mathbf{r} = (r_1, \ldots, r_n) \in \mathbb{R}^n$, the distribution is called an elliptical Gaussian and is denoted as $\rho_{\mathbf{r}}$ and $D_{\mathbf{r}}$. If all r_i's equal r, it is called a spherical Gaussians and is written as ρ_r and D_r. We will frequently use the fact that if x follows a Gaussian distribution of covariance matrix Σ, i.e., $x \leftarrow D_{\sqrt{\Sigma}}$, then $Tx \leftarrow D_{\sqrt{T\Sigma T^*}}$, where T is a linear transformation on V, and T^* is the conjugate-transpose operator.

Proposition 2.3. *[Was04, Thm 2.44] Let X be a Gaussian vector over $\mathbb{R}^n$ of covariance matrix Σ. Suppose X splits as $X = (X_a, X_b)$ and its covariance matrix is written accordingly as:*

$$\Sigma = \begin{pmatrix} \Sigma_{aa} & \Sigma_{ab} \\ \Sigma_{ba} & \Sigma_{bb} \end{pmatrix}.$$

Then,
i) the marginal distribution of X_a is a Gaussian distribution of covariance matrix Σ_{aa}, and
ii) the conditional distribution of X_b, given the value for X_a as x_a, is a Gaussian distribution of covariance matrix $\Sigma_{bb} - \Sigma_{ba}\Sigma_{aa}^{-1}\Sigma_{ab}$ and mean $\Sigma_{ba}\Sigma_{aa}^{-1}x_a$.

When working with elliptical Gaussians over H, we restrict our parameters to belong to the set $G = \{\mathbf{r} \in (\mathbb{R}^+)^n | \ \mathbf{r}_{s_1+s_2+j} = \mathbf{r}_{s_1+j}, \ 1 \leq j \leq s_2\}$. We say that $\mathbf{r}_1 \geq \mathbf{r}_2$ if $\mathbf{r}_{1i} \geq \mathbf{r}_{2i}$, for all $1 \leq i \leq n$, and by $\mathbf{r} \geq r$ we mean that $\mathbf{r}_i \geq r$, for all $1 \leq i \leq n$. Given a lattice $\mathcal{L}$ in V and a real positive definite matrix Σ, we define the discrete Gaussian distribution $D_{\mathcal{L},\sqrt{\Sigma}}$ on $\mathcal{L}$ as $D_{\mathcal{L},\sqrt{\Sigma}}(x) := \frac{\rho_{\sqrt{\Sigma}}(x)}{\rho_{\sqrt{\Sigma}}(\mathcal{L})}$, for any $x \in \mathcal{L}$.

Definition 2.4 (Smoothing Condition [Pei10, Def 2.2, 2.3]). *For a lattice $\mathcal{L}$ in V of rank n and a parameter $\varepsilon > 0$, we define the smoothing parameter of $\mathcal{L}$, $\eta_\varepsilon(\mathcal{L})$, as the smallest $r > 0$ such that $\rho_{1/r}(\mathcal{L}^* \setminus \{0\}) \leq \varepsilon$. For a positive definite matrix Σ, we say that $\sqrt{\Sigma} \geq \eta_\varepsilon(\mathcal{L})$ if $\rho_{\sqrt{\Sigma^{-1}}}(\mathcal{L}^* \setminus \{0\}) \leq \varepsilon$.*

Lemma 2.5. *If $\mathcal{L}' \subseteq \mathcal{L}$ are two full-rank lattices in V, $\varepsilon \in (0,1)$ and $\sqrt{\Sigma} \geq \eta_\varepsilon(\mathcal{L}')$, then the statistical distance between $D_{\mathcal{L},\sqrt{\Sigma}}$ mod $\mathcal{L}'$ and the uniform distribution over $\mathcal{L}/\mathcal{L}'$ is at most 2ε.*

Proof. Its proof is the same as of [GPV08, Cor. 2.8] but uses [Pei10, Lem. 2.4] instead of [GPV08, Lem 2.7]. □

Lemma 2.6. *Let $\mathcal{L}$ be a full-rank lattice in V. Then the following hold:*

(i) [MR07, Lem 3.2, 3.3] $\eta_\varepsilon(\mathcal{L}) \leq \frac{\sqrt{n}}{\lambda_1(\mathcal{L}^*)}$, for $\varepsilon = 2^{-\Omega(n)}$. Moreover, for any positive $\varepsilon > 0$, $\eta_\varepsilon(\mathcal{L}) \leq \sqrt{\frac{ln(2n(1+1/\varepsilon))}{\pi}} \cdot \lambda_n(\mathcal{L})$.

(ii) [Reg09, Claim 2.13] $\eta_\varepsilon(\mathcal{L}) \geq \sqrt{\frac{ln(1/\varepsilon)}{\pi}} \cdot \frac{1}{\lambda_1(\mathcal{L}^*)}$, for any $\varepsilon \in (0,1)$.

From Lemma 2.6 (i), (ii), we deduce that for $\varepsilon = e^{-n}$, $\eta_\varepsilon(\mathcal{L}) = \frac{\theta(\sqrt{n})}{\lambda_1(\mathcal{L}^*)}$.

2.2.2 Lattice problems

Let $\mathcal{L}$ be a full-rank lattice in a n dimensional real space V. We state in the following the standard lattice problems:

Definition 2.7 (Shortest Independent Vector Problem). *For an approximation factor $\gamma = \gamma(n) \geq 1$ and a family of lattices $\mathfrak{L}$, the $\mathfrak{L}$-$\mathtt{SIVP}_\gamma$ problem is: given a lattice $\mathcal{L} \in \mathfrak{L}$, output n linearly independent lattice vectors of norm at most $\gamma \cdot \lambda_n(\mathcal{L})$.*

Definition 2.8 (Discrete Gaussian Sampling). *For a family of lattices $\mathfrak{L}$ and a function $\gamma : \mathfrak{L} \to G = \{\boldsymbol{r} \in \mathbb{R}^n |\ \boldsymbol{r}_{s_1+s_2+j} = \boldsymbol{r}_{s_1+j},\ 1 \leq j \leq s_2\}$, the $\mathfrak{L}$-$\mathtt{DGS}_\gamma$ problem is: given a lattice $\mathcal{L} \in \mathfrak{L}$ and $\boldsymbol{r} \geq \gamma(\mathcal{L})$, output a sample $x \in \mathcal{L}$ which follows a distribution statistically indistinguishable from $D_{\mathcal{L},\boldsymbol{r}}$.*

Definition 2.9 (Bounded Distance Decoding). *For a family of lattices $\mathfrak{L}$ and a function $\delta : \mathfrak{L} \to \mathbb{R}^+$, the $\mathfrak{L}$-$\mathtt{BDD}_\delta$ problem is: given a lattice $\mathcal{L} \in \mathfrak{L}$, a distance bound $d \leq \delta(\mathcal{L})$ and a coset $e + \mathcal{L}$, where $\|e\| \leq d$ find e.*

Definition 2.10 (Gaussian Decoding Problem [PRSD17]). *For a lattice $\mathcal{L} \subset H$ and a Gaussian parameter $g > 0$, the $\mathcal{L}$-$\mathtt{GDP}_\gamma$ problem is as follows: given as input a coset $e + \mathcal{L}$, where $\boldsymbol{e} \in H$ is drawn from D_g, output $\boldsymbol{e}$.*

We recall here the reduction from $\mathtt{SIVP}$ to $\mathtt{DGS}$ from [Reg05].

Lemma 2.11 ([Reg05, Lem 3.17]). *For $\varepsilon = \varepsilon(n) \leq \frac{1}{10}$ and $\gamma \geq \sqrt{2}\eta_\varepsilon(\mathcal{L})$, there is a reduction from $\mathtt{SIVP}_{2\sqrt{n}/\lambda_n(\mathcal{L})\cdot\gamma}$ to $\mathtt{DGS}_\gamma$.*

2.2.3 p-ary lattices

For an integer p, an integer lattice $L \subset \mathbb{Z}^n$ is said to be a *p-ary integer lattice* of determinant p^k, with $k \leq n$, if $p\mathbb{Z}^n \subseteq L \subseteq \mathbb{Z}^n$, and $[\mathbb{Z}^n : L] = p^k$. For our purpose, we choose p to be a small prime with $O(\log k)$ bits and $n = O(k)$. It is well-known that such a p-ary lattice L can be generated as $A\mathbb{Z}_p^{n-k} + p\mathbb{Z}^n$, for a full-rank matrix $A \in M_{n\times n-k}(\mathbb{F}_p)$, where $\mathbb{F}_p$ (or $\mathbb{Z}_p$) is the finite field with p elements.

Lemma 2.12. *The HNF basis for L is given by the columns of:*

$$\begin{pmatrix} Id_{n-k\times n-k} & 0 \\ A_2A_1^{-1} & pId_{k\times k} \end{pmatrix}$$

where $A^t = (A_1^t|A_2^t)$, with an invertible $A_1 \in M_{n-k}(\mathbb{F}_p)$ and $A_2 \in M_{k\times n-k}(\mathbb{F}_p)$.

Proof. Let $\mathbf{x} \in L$. Then, $\mathbf{x} \equiv A \cdot \mathbf{z} \mod p$, for $\mathbf{z} \in \mathbb{F}_p^{n-k}$. Split $\mathbf{x}$ as $(\mathbf{x}_1|\mathbf{x}_2)$, for $\mathbf{x}_1 \in \mathbb{Z}^{n-k}$ and $\mathbf{x}_2 \in \mathbb{Z}^k$. Then, $\mathbf{x}_1 \equiv A_1 \cdot \mathbf{z} \mod p$ and $\mathbf{x}_2 \equiv A_2 \cdot \mathbf{z} \mod p$. Since A_1 is invertible over $\mathbb{F}_p$, one may write $\mathbf{x}_2 \equiv A_2A_1^{-1}\mathbf{x}_1 \mod p$, thereby showing that any $\mathbf{x} \in L$ can be represented as $(\mathbf{x}_1|A_2A_1^{-1}\mathbf{x}_1 + p \cdot \mathbf{u})$, for some $\mathbf{u} \in \mathbb{Z}^k$. Notice that this basis coincides with the HNF basis of the lattice. □

Owing to the results of [Ajt96, Reg05], it is sufficient to solve lattice problems on p-ary lattices, as solving lattice problems on p-ary lattices is at least as hard as solving lattice problems on general integer lattices.

2.3 Lattices in number fields: Orders and Ideals

A *number field* $K := \mathbb{Q}(\theta)$ of degree n is a $\mathbb{Q}$-vector space obtained by attaching a root θ of a monic, irreducible polynomial $f(x)$ of degree n. It is well-known that each such K has exactly n field embeddings $\sigma_i : K \to \mathbb{C}$, that map θ to each complex root of the minimal polynomial f. Embeddings whose image lies in $\mathbb{R}$ are called *real embedding*, otherwise it is called a *complex embedding*. The *canonical (or Minkowski) embedding* $\sigma : K \to \mathbb{C}^n$ is defined as:

$$\sigma(x) = (\sigma_1(x), \sigma_2(x), \ldots, \sigma_n(x)), \text{ for any } x \in K.$$

The image $\sigma(K)$ generates the n-dimensional real vector space $K_\mathbb{R}$ that is isomorphic to the space H. We use $K_\mathbb{R}$ and H interchangeably. By a lattice in K, we mean the image in $K_\mathbb{R}$, of a $\mathbb{Z}$-module in K. The most extensively studied lattice in K is its ring of integers

$$\mathcal{O}_K := \{\beta \in K : \exists \text{ (monic) } g(x) \in \mathbb{Z}[x] \text{ such that } g(\beta) = 0\}$$

This ring is a full-rank lattice in K, i.e., $rank_\mathbb{Z}\ \mathcal{O}_K = n$. A sub-ring $\mathcal{O}$ of $\mathcal{O}_K$ satisfying $rank_\mathbb{Z}\ \mathcal{O} = n$ is said to be an *Order*. In other words, an order $\mathcal{O}$ equals $\mathbb{Z}g_1 \oplus \ldots \oplus \mathbb{Z}g_n$, for some basis $\{g_1, g_2, \ldots, g_n\} \subseteq \mathcal{O}$ of $K/\mathbb{Q}$. The set of all orders is a partial ordered set with respect to set containment and has $\mathcal{O}_K$ as the unique maximal element.

Lemma 2.13. *Let $\mathcal{O}$ be an order in K. Then, $\mathcal{O}$ has a $\mathbb{Z}$-basis containing* 1.

Proof. Let the notation $A \xrightarrow{\phi} B \xrightarrow{\psi} C$ mean that $\phi(A) \subseteq \ker(\psi) := \{b \in B : \psi(b) = 0\}$. Then, the following is a short exact sequence of $\mathbb{Z}$-modules, where the second map is inclusion and the third map is the projection.

$$0 \to \mathbb{Z} \to \mathcal{O} \to \mathcal{O}/\mathbb{Z} \to 0$$

To prove the claim, it suffices to show that $\mathcal{O}/\mathbb{Z}$ is a torsion free $\mathbb{Z}$-module, and hence a free $\mathbb{Z}$-module, [DF91, Chapter 12.1, Thm 5], as that would imply that the above sequence splits, i.e., $\mathcal{O} = \mathbb{Z} \oplus \mathcal{O}/\mathbb{Z}$. See [Chu, Lem. 2]. Then, a $\mathbb{Z}$-basis for $\mathcal{O}$ is the union of a $\mathbb{Z}$-basis for $\mathcal{O}/\mathbb{Z}$ and 1, a $\mathbb{Z}$-basis for $\mathbb{Z}$.

Finally, in order to see that $\mathcal{O}/\mathbb{Z}$ is torsion free, assume, to the contrary, that there is a non-zero $x \in \mathcal{O}/\mathbb{Z}$, such that $mx = 0 \mod \mathbb{Z}$. Then $x \in \frac{1}{m}\mathbb{Z} \cap \mathcal{O} \subseteq \mathbb{Q} \cap \mathcal{O}_K = \mathbb{Z}$, by definition of the ring of integers $\mathcal{O}_K$. □

Another important class of full-rank lattices in K that we study are ideals in K. An (integral) *ideal* $\mathcal{I}$ in $\mathcal{O}$ is an additive subgroup that is closed under scalar multiplication by $\mathcal{O}$, i.e. $x \cdot a \in \mathcal{I}$ for every $x \in \mathcal{O}$ and $a \in \mathcal{I}$. Every ideal is a $\mathbb{Z}$-module of rank n. Further, ideals in K can be thought of as integers in $\mathbb{Z}$, since they can be added, mutliplied and (sometimes) divided. The *sum* of two ideals $\mathcal{I}, \mathcal{J} \subseteq \mathcal{O}$ is defined by $\mathcal{I} + \mathcal{J} := \{x + y \mid x \in \mathcal{I}, y \in \mathcal{J}\}$, and their *product* is defined by $\mathcal{I} \cdot \mathcal{J} := \{\sum x_i y_i \mid x_i \in \mathcal{I}, y_i \in \mathcal{J}\}$. Their *intersection* is simply their set theoretic intersection, and their *quotient* is defined by $(\mathcal{I} : \mathcal{J}) := \{x \in K \mid x\mathcal{J} \subseteq \mathcal{I}\}$. All of the former sets are ideals in $\mathcal{O}$.

An integral ideal $\mathfrak{p} \subset \mathcal{O}$ is *prime* if for every pair of elements $x, y \in \mathcal{O}$, whenever $xy \in \mathfrak{p}$, then either $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$. Every integral ideal $\mathcal{I}$ of $\mathcal{O}$ contains a product of prime ideals $\mathcal{I} \supseteq \prod \mathfrak{p}_i$. Integral ideals $\mathcal{I}, \mathcal{J}$ of $\mathcal{O}$ are *coprime*, if $\mathcal{I} + \mathcal{J} = \mathcal{O}$ and therefore we also have, $\mathcal{I}\mathcal{J} = \mathcal{I} \cap \mathcal{J}$ and $(\mathcal{I} \cap \mathcal{J})\mathcal{L} = \mathcal{I}\mathcal{L} \cap \mathcal{J}\mathcal{L}$, for any ideal $\mathcal{L}$. For an integral ideal $\mathcal{I} \subseteq \mathcal{O}$, the set of *associated primes* of $\mathcal{I}$ is the set of all prime ideals of $\mathcal{O}$ that contain $\mathcal{I}$. We state the well-known Chinese Remainder Theorem.

Theorem 2.14 (Chinese Remainder Theorem)**.** *Let $\mathcal{I}$ be a fractional ideal over an order $\mathcal{O}$ and $\mathcal{J}_1, \mathcal{J}_2, \ldots, \mathcal{J}_l$ pairwise coprime $\mathcal{O}$-ideals. Then the canonical map of $\mathcal{O}$-modules*

$$\mathcal{I}/\prod_i \mathcal{I}\mathcal{J}_i \to \bigoplus_i \mathcal{I}/\mathcal{I}\mathcal{J}_i$$

is an isomorphism.

The *norm* of an ideal $\mathcal{I} \subset \mathcal{O}$ is its index as a subgroup of $\mathcal{O}$, i.e. $N(\mathcal{I}) := [\mathcal{O} : \mathcal{I}] = |\mathcal{O}/\mathcal{I}|$. For the special case where $\mathcal{O} = \mathcal{O}_K$ is the maximal order, the norm is a multiplicative function, i.e. $N(\mathcal{I}\mathcal{J}) = N(\mathcal{I}) \cdot N(\mathcal{J})$ for any integral $\mathcal{I}, \mathcal{J}$. A *fractional ideal* $\mathcal{I} \subset K$ of $\mathcal{O}$ is a set such that $d\mathcal{I} \subset \mathcal{O}$ for some $d \in \mathcal{O}$. We define its norm to be $N(\mathcal{I}) := N(d\mathcal{I})/|N(d)|$. Note that for any fractional ideals $\mathcal{I}, \mathcal{J}$, their sum, product, quotient and intersection are again fractional ideals.

Given a geometric norm $\|\cdot\|$ on H, such as the Euclidean norm, we can define a norm on field elements by identifying them with their Minkowski embeddings, i.e. $\|x\| = \|\sigma(x)\|$, for any $x \in K$. The next lemma shows a bound on the (Euclidean) norm on short vectors in lattices in a number field K.

Lemma 2.15 ([BBPS19, Lem 2.21])**.** *Let K be a number field of degree n and $\mathcal{I}$ an ideal over an order $\mathcal{O}$. Then*

$$\sqrt{n} \cdot N(\mathcal{I})^{1/n} \leq \lambda_1(\mathcal{I}).$$

Remark 2.16. *Since every order $\mathcal{O}$ contains 1, it follows that $\lambda_1(\mathcal{O}) \leq \sqrt{n}$. On the other hand, the first part in the inequality of Lemma 2.15 tells that $\lambda_1(\mathcal{O}) \geq \sqrt{n}$, since $N(\mathcal{O}) = 1$. This proves that $\lambda_1(\mathcal{O})$ is exactly $\sqrt{n}$.*

A fractional ideal $\mathcal{I}$ is *invertible* if there exists a fractional ideal $\mathcal{J}$ such that $\mathcal{I} \cdot \mathcal{J} = \mathcal{O}$. If there exists such a $\mathcal{J}$, then it is unique and equal to $(\mathcal{O} : \mathcal{I})$, and is denoted by $\mathcal{I}^{-1}$. In general, an ideal in an order may not be invertible. However, in the special case where $\mathcal{O} = \mathcal{O}_K$ is the maximal order, *every* fractional ideal is invertible. Later, we will describe a criterion for an $\mathcal{O}$-ideal to be invertible when we define the conductor ideal below.

The following lemma, popularly known as the Cancellation Lemma, plays a crucial role in the hardness result for algebraic LWE's. Note that it uses the invertibility of the ideal $\mathcal{I}$.

Lemma 2.17 ([BBPS19, Thm 2.35])**.** *Let $\mathcal{I}$ and $\mathcal{J}$ be integral ideals of an order $\mathcal{O}$ and $\mathcal{M}$ a fractional ideal. Assume that $\mathcal{I}$ is an invertible ideal. Then, given the associated primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ of $\mathcal{J}$, and an element $t \in \mathcal{I} \setminus \bigcup_{i=1}^{r} \mathcal{I}\mathfrak{p}_i$, the multiplication by t map θ_t, $\theta_t(x) = t \cdot x$, induces the following isomorphism of $\mathcal{O}$-modules*

$$\frac{\mathcal{M}}{\mathcal{J}\mathcal{M}} \xrightarrow{\sim} \frac{\mathcal{I}\mathcal{M}}{\mathcal{I}\mathcal{J}\mathcal{M}}.$$

This map can be efficiently inverted using $\mathcal{I}$, $\mathcal{J}$, $\mathcal{M}$ and t can be found using $\mathcal{I}$ and $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$.

Remark 2.18. *The above result is proved in [BBPS19, Thm 2.35] under a condition weaker than demanding that $\mathcal{I}$ be an invertible $\mathcal{O}$-ideal. The proof only requires the tuple $(t, \mathcal{I}, \mathcal{J}, \mathcal{M})$ to satisfy $t\mathcal{M} + \mathcal{I}\mathcal{J}\mathcal{M} = \mathcal{I}\mathcal{M}$.*

In the improved hardness result in Section 4.1, we will deal with the scenario of non-invertible ideals. To circumvent this issue, we use the following result, which shows that under a coprimality condition, the inclusion induces an isomorphism.

Lemma 2.19 ([PP19, Lemma 4.1])**.** *Let $\mathcal{L}' \subseteq \mathcal{L}$ be two lattices in a number field K and q an integer coprime with $[\mathcal{L}' : \mathcal{L}]$. Then the natural inclusion $\mathcal{L}' \subseteq \mathcal{L}$ induces a bijection*

$$f : \frac{\mathcal{L}'}{q\mathcal{L}'} \xhookrightarrow{\sim} \frac{\mathcal{L}}{q\mathcal{L}} \quad f(x) = x + q\mathcal{L}.$$

Moreover, this map is efficiently computable given a basis of $\mathcal{L}'$ relative to a basis of $\mathcal{L}$.

We denote by $\xhookrightarrow{\sim}$ the isomorphism induced by the inclusion considered.

2.3.1 Duality

For an element $a \in K$, the trace $Tr(a)$ is the sum $\sum_{i=1}^{n} \sigma_i(a)$, of images of a under all the embeddings of K. In other words, it is the sum of all coordinates of $\sigma(a)$.

Definition 2.20. *The dual of the lattice $\mathcal{L}$ is defined as*

$$\mathcal{L}^\vee = \{x \in K |\ Tr(x \cdot \mathcal{L}) \subseteq \mathbb{Z}\}.$$

Recall that $H \subseteq \mathbb{C}^n$ inherits the usual Hermitian inner product from $\mathbb{C}^n$. As, for $x, y \in K$,

$$Tr(xy) = \sum_{i=1}^{n} \sigma_i(xy) = \sum_{i=1}^{n} \sigma_i(x)\sigma_i(y) = \langle \sigma(x), \overline{\sigma(y)} \rangle$$

we have the following relation between the duals; $\sigma(\mathcal{L}^\vee) = \overline{\sigma(\mathcal{L})^*}$. Given a basis $(b_i)_{1 \le i \le n}$ of $\mathcal{L}$, a basis $(b_i^\vee)_{1 \le i \le n}$ of $\mathcal{L}^\vee$ can be found by considering $Tr(b_i \cdot b_j^\vee) = \delta_{ij}$, for any $1 \le i, j \le n$. When $\mathcal{L}$ is a fractional ideal over an order $\mathcal{O}$, it follows that $\mathcal{L}^\vee$ is also a fractional ideal over $\mathcal{O}$. We recall briefly some properties of duality:

Proposition 2.21 ([Conc, Section 3], [Conb, Section 4])**.** *For any two lattices $\mathcal{I}$ and $\mathcal{J}$ in a number field K:*
i) $(\mathcal{I}^\vee)^\vee = \mathcal{I}$.
ii) if $\mathcal{I} \subset \mathcal{J}$, then $\mathcal{J}^\vee \subset \mathcal{I}^\vee$.
iii) if $\mathcal{I}$ is an $\mathcal{O}$ ideal, then $\mathcal{I} \cdot \mathcal{I}^\vee = \{x \in K | x\mathcal{I} \subseteq \mathcal{I}\}^\vee \subseteq \mathcal{O}^\vee$. If $\mathcal{O} = \mathcal{O}_K$, equality holds.
iv) if $\mathcal{I}, \mathcal{J}$ are ideals over $\mathcal{O}$ and $\mathcal{I}$ is invertible, then $(\mathcal{I}\mathcal{J})^\vee = \mathcal{I}^{-1}\mathcal{J}^\vee$.

Proposition 2.22 ([Conc, Thm 3.7])**.** *If $\mathcal{O} = \mathbb{Z}[x]/(f)$, for a monic polynomial f and some root $\theta \in K$, then $\mathcal{O}^\vee = \frac{1}{f'(\theta)}\mathcal{O}$.*

2.3.2 The Ring of Multipliers

For any lattice $\mathcal{L}$ in a number field K, we define a *multiplier* of $\mathcal{L}$ as an element $x \in K$ such that $x\mathcal{L} \subseteq \mathcal{L}$. It turns out that the set of these multipliers has a ring structure, and moreover, form an order in the field K. For more details, see [Neu99, Chapter 1, Sect.12].

Definition 2.23. *For a lattice $\mathcal{L} \subset K$, we define its ring of multipliers as*

$$\mathcal{O}_\mathcal{L} = \{x \in K |\ x\mathcal{L} \subseteq \mathcal{L}\}.$$

Both $\mathcal{L}$ and $\mathcal{L}^\vee$ are ideals of $\mathcal{O}_\mathcal{L}$. In fact, $\mathcal{O}_\mathcal{L}$ is the largest such order. In particular, if the lattice $\mathcal{L}$ is an order itself, then it is its own ring of multipliers. The following is an interesting and important characterisation of $\mathcal{O}_\mathcal{L}$.

Proposition 2.24 ([Conb, Rem 4.2])**.** *For any lattice $\mathcal{L} \subset K$, $\mathcal{O}_\mathcal{L}^\vee = \mathcal{L}\mathcal{L}^\vee$.*

2.3.3 The Conductor Ideal

The non-maximality of an order $\mathcal{O}$ is reflected in a special ideal of $\mathcal{O}$ called the conductor ideal. We describe how this ideal is also closely related to the invertibility and unique factorization of $\mathcal{O}$-ideals.

Definition 2.25. *The* conductor *of an order $\mathcal{O}$ is defined to be the ideal*

$$\mathcal{C}_\mathcal{O} = (\mathcal{O}_K : \mathcal{O}) := \{x \in K : x \cdot \mathcal{O}_K \subseteq \mathcal{O}\}.$$

It is the maximal $\mathcal{O}_K$-ideal contained in $\mathcal{O}$.

We remark that one may define the conductor ideal in a more general scenario: when two orders $\mathcal{O}_1$ and $\mathcal{O}_2$ may not be ordered with respect to set containment. In this case, the conductor of $\mathcal{O}_1$ with respect to $\mathcal{O}_2$ is the biggest $\mathcal{O}_2$-ideal contained in $\mathcal{O}_1$ and is defined as $\mathcal{C}_{\mathcal{O}_1,\mathcal{O}_2} := \{x \in K |\ x\mathcal{O}_2 \subseteq \mathcal{O}_1\}$. The proof is exactly the same as in the case when $\mathcal{O}_2 = \mathcal{O}_K$. The following lemma describes the relation between the conductor and the duals of the orders. It is a generalization of [BBPS19, Lemma 2.32, Remark 2.33].

Lemma 2.26. *Let $\mathcal{O}_1$ and $\mathcal{O}_2$ be two orders in K and let $\mathcal{C} := \mathcal{C}_{\mathcal{O}_1,\mathcal{O}_2}$ be as defined above. Then, $\mathcal{O}_2 \cdot \mathcal{O}_1^\vee = \mathcal{C}^\vee$. Further, if $\mathcal{C}$ is an invertible $\mathcal{O}_2$-ideal, then*

$$\mathcal{C}\mathcal{O}_1^\vee = \mathcal{O}_2^\vee.$$

Proof. By the definition of the dual of an ideal (Definition 2.20),

$$\begin{aligned}(\mathcal{O}_2 \cdot \mathcal{O}_1^\vee)^\vee &= \{x \in K |\ Tr(x\mathcal{O}_2 \cdot \mathcal{O}_1^\vee) \subseteq \mathbb{Z}\} \\ &= \{x \in K |\ x \cdot \mathcal{O}_2 \subseteq (\mathcal{O}_1^\vee)^\vee = \mathcal{O}_1\} \\ &= \mathcal{C}.\end{aligned}$$

Therefore, $\mathcal{C}^\vee = \mathcal{O}_2\mathcal{O}_1^\vee$. Using invertibility of $\mathcal{C}$ as an $\mathcal{O}_2$-ideal, we get that $\mathcal{C}^\vee = \mathcal{C}^{-1}\mathcal{O}_2^\vee$. Inserting this in the equality above yields the final claim. □

There is a distinction between $\mathcal{O}$-ideals, based on invertibility. This distinction did not exist when dealing with $\mathcal{O}_K$-ideals, since all $\mathcal{O}_K$-ideals are invertible. But the picture is not all that bad.

Theorem 2.27. *[Conb] The nonzero $\mathcal{O}$-ideals coprime to $\mathcal{C}_\mathcal{O}$ are invertible and also have unique factorization into prime ideals over $\mathcal{O}$. Further, they are in a multiplicative bijection with the set of nonzero $\mathcal{O}_K$-ideals coprime to $\mathcal{C}_\mathcal{O}$, via the maps $\mathcal{I} \mapsto \mathcal{I}\mathcal{O}_K$ and $\mathcal{J} \mapsto \mathcal{J} \cap \mathcal{O}$.*

2.3.4 Localization

We only describe the results used in the next section. To understand the concept of localization more thoroughly, we refer the reader to [Neu99, Ch. 1].

Definition 2.28. *Let $\mathfrak{p}$ be a prime ideal of an order $\mathcal{O}$. Localization of $\mathcal{O}$ at $\mathfrak{p}$ is defined as the following set*

$$\mathcal{O}_\mathfrak{p} = \left\{\frac{r}{s} |\ r \in \mathcal{O},\ s \notin \mathfrak{p}\right\}.$$

It is straightforward to check that $\mathcal{O}_\mathfrak{p}$ is a ring. Further, it has a unique maximal ideal, namely $\mathfrak{p}\mathcal{O}_\mathfrak{p}$, and therefore is a *local* ring. The complement of the unique maximal ideal is the group of units, $\mathcal{O}_\mathfrak{p}^* := \left\{\frac{r}{s} |\ r, s \notin \mathfrak{p}\right\}$. The ideals of $\mathcal{O}_\mathfrak{p}$ are the sets $\mathcal{I}\mathcal{O}_\mathfrak{p} = \left\{\frac{r}{s} |\ r \in \mathcal{I},\ s \notin \mathfrak{p}\right\}$, for any ideal $\mathcal{I}$ of $\mathcal{O}$. Notice that for ideals $\mathcal{I}$ such that $\mathcal{I} \nsubseteq \mathfrak{p}$, we have $1 \in \mathcal{I}_\mathfrak{p}$, hence $\mathcal{I}\mathcal{O}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}$. Localization also behaves nicely when performing ideal operations. In particular, for any fractional $\mathcal{O}$-ideals $\mathcal{I}$ and $\mathcal{J}$ and a prime $\mathcal{O}$-ideal $\mathfrak{p}$, $(\mathcal{I}\mathcal{J})_\mathfrak{p} = \mathcal{I}_\mathfrak{p}\mathcal{J}_\mathfrak{p}$ and $(\mathcal{I}/\mathcal{J})_\mathfrak{p} \simeq \mathcal{I}_\mathfrak{p}/\mathcal{J}_\mathfrak{p}$. Moreover, we can extend $\mathcal{O}$-module maps $f : \mathcal{I} \to \mathcal{J}$ to maps $f_\mathfrak{p} : \mathcal{I}_\mathfrak{p} \to \mathcal{J}_\mathfrak{p}$ as $f_\mathfrak{p}(r/s) := f(r)/s$.

We recall that if $\mathfrak{p}$ is an invertible prime ideal, then $\mathcal{O}_\mathfrak{p}$ is a Discrete Valuation Ring, and hence a Unique Factorization Domain, i.e. any proper ideal of it can be written as a unique product of prime ideals. ([Ste08, Prop 5.4], [DF91, Chapter 8.3,Thm 12])

2.3.5 Jordan-Hölder filtrations

It is a well-known fact from algebraic number theory that $\mathcal{O}_K$ is a Dedekind domain, i.e., every ideal in $\mathcal{O}_K$ can be uniquely decomposed into prime ideals in $\mathcal{O}_K$, much like the unique factorization of integers into prime numbers. This property is not true for ideals in a (non-maximal) order. However, the Jordan-Hölder filtrations may be considered as the analog of unique decomposition into prime ideals for $\mathcal{O}$-ideals, when $\mathcal{O}$ is a non-maximal order. Let $m = [\mathcal{O}_K : \mathcal{O}]$ be the index of $\mathcal{O}$ in $\mathcal{O}_K$. As $m\mathcal{O}_K$ is an $\mathcal{O}_K$-ideal contained in $\mathcal{O}$, we have $\mathcal{C}_{\mathcal{O}} | m\mathcal{O}_K$. Define, for an ideal $\mathcal{I}$ of a ring R, $Spec_R(\mathcal{I})$ to be the set of prime ideals in R that contain $\mathcal{I}$. This set coincides with the set of associated primes of $\mathcal{I}$, defined previously in Section 2.3.

Theorem 2.29 ([Cone, Thm 8.9])**.** *Let $\mathcal{O}$ be an order. Then for any integral ideal $\mathcal{I}$ there is a descending chain of ideals*

$$\mathcal{O} = \mathcal{I}_0 \supset \mathcal{I}_1 \supset \ldots \supset \mathcal{I}_l = \mathcal{I}, \tag{2.3.1}$$

where each quotient $\mathcal{I}_i/\mathcal{I}_{i+1}$ is a simple $\mathcal{O}$-module. Moreover, for any $0 \leq i \leq l-1$, $\mathcal{I}_i/\mathcal{I}_{i+1} \sim \mathcal{O}/\mathfrak{p}_i$ for some prime ideal $\mathfrak{p}_i$ of $\mathcal{O}$. These primes are the primes of $\mathcal{O}$ that contain $\mathcal{I}$ and their number is independent on the choice of the series. Furthermore, $[\mathcal{O} : \mathcal{I}] = \prod_{i=0}^{l-1} [\mathcal{O} : \mathfrak{p}_i]$.

Definition 2.30. *A finite chain for an $\mathcal{O}$-ideal $\mathcal{I}$ as in Theorem 2.29 is called a Jordan-Hölder filtration of $\mathcal{I}$.*

Lemma 2.31 (Restatement of [Cone, Theorem 8.6])**.** *Let $\mathfrak{q}$ be a prime ideal in $\mathcal{O}$ that does not lie in $Spec_{\mathcal{O}}(m\mathcal{O})$. Then, $\mathfrak{q}$ is invertible.*

Proof. As $\mathfrak{q} \not\supseteq m\mathcal{O}$, the two ideals are co-maximal, i.e. $\mathfrak{q} + m\mathcal{O} = \mathcal{O}$. Let $\pi + mb = 1$, for some $\pi \in \mathfrak{q}$ and $b \in \mathcal{O}$.

Consider the ideal $\tilde{\mathfrak{q}} := \{y \in K : y\mathfrak{q} \subset \mathcal{O}\}$. By [Cone, Thm 3.2, Section 8], $\mathcal{O} \subsetneq \tilde{\mathfrak{q}}$. Choose $x \in \tilde{\mathfrak{q}} \setminus \mathcal{O}$. Then, $\mathfrak{q} \subseteq \mathfrak{q} + x\mathfrak{q} \subseteq \mathcal{O}$. As $\mathfrak{q}$ is a maximal ideal, we have the following two cases.
Case 1: $\mathfrak{q} + x\mathfrak{q} = \mathcal{O}$. Then, $\mathfrak{q}(\mathcal{O} + x\mathcal{O}) = \mathcal{O}$ and $\mathfrak{q}$ is invertible.
Case 2: $\mathfrak{q} + x\mathfrak{q} = \mathfrak{q}$. This implies that $x\mathfrak{q} \subset \mathfrak{q}$. Since $\mathfrak{q}$ is a finitely generated $\mathbb{Z}$-lattice, we get that $x \in \mathcal{O}_K$. Then,

$$x = x \cdot 1 = x \cdot (\pi + mb) \in x\mathfrak{q} + m\mathcal{O}_K \subset \mathfrak{q} + \mathcal{O} = \mathcal{O}$$

This contradicts the fact that $x \notin \mathcal{O}$. □

Remark 2.32. *Observe that if $\mathfrak{q}$ is a non-invertible prime, then by Lemma 2.31, $\mathfrak{q} \supseteq m\mathcal{O}$, and the index $[\mathcal{O} : \mathfrak{q}] \mid [\mathcal{O} : m\mathcal{O}] = m^n$. Therefore, $Spec_{\mathbb{Z}}([\mathcal{O} : \mathfrak{q}]) \subseteq Spec_{\mathbb{Z}}(m)$.*

Lemma 2.33. *Let $\mathcal{I}$ be an integral $\mathcal{O}$-ideal. Then, there exists an invertible ideal $\mathfrak{q}$ such that $\mathcal{I} \subseteq \mathfrak{q} \subseteq \mathcal{O}$ and $Spec_{\mathbb{Z}}([\mathfrak{q} : \mathcal{I}]) \subseteq Spec_{\mathbb{Z}}(m)$, where $[\mathfrak{q} : \mathcal{I}]$ denotes the index of $\mathcal{I}$ in $\mathfrak{q}$.*

Proof. Without loss of generality, we assume that $\mathcal{I}$ is a non-invertible $\mathcal{O}$-ideal and $Spec_{\mathbb{Z}}([\mathcal{O} : \mathcal{I}]) \not\subseteq Spec_{\mathbb{Z}}(m)$. For if $([\mathcal{O} : \mathcal{I}], m) = 1$, then $\mathcal{I}$ is an invertible $\mathcal{O}$-ideal. Further, if $Spec_{\mathbb{Z}}([\mathcal{O} : \mathcal{I}]) \subseteq Spec_{\mathbb{Z}}(m)$, we may choose $\mathfrak{q} = \mathcal{O}$. By [Cone, Thm 8.9], every integral $\mathcal{O}$-ideal $\mathcal{I}$ has a Jordan-Hölder filteration, i.e, there exist $\mathcal{O}$-ideals $\mathcal{I}_0, \mathcal{I}_1, \ldots, \mathcal{I}_l$ such that

$$\mathcal{O} = \mathcal{I}_0 \supset \mathcal{I}_1 \supset \mathcal{I}_2 \cdots \supset \mathcal{I}_l = \mathcal{I}$$

where each quotient $\mathcal{I}_i/\mathcal{I}_{i+1}$ is a simple $\mathcal{O}$-module and hence isomorphic to $\mathcal{O}/\mathfrak{p}_i$, for some prime ideal $\mathfrak{p}_i$ of $\mathcal{O}$. Further $[\mathcal{O}:\mathcal{I}] = \prod_{i=0}^{l-1}[\mathcal{O}:\mathfrak{p}_i]$.

Let $\mathfrak{p}$ be an invertible ideal that appears as a Jordan-Hölder factor of $\mathcal{I}$, with multiplicity $m_\mathfrak{p}$. We claim that $\mathcal{I} \subset \mathfrak{p}^{m_\mathfrak{p}}$.

Consider the localization of $\mathcal{O}$ at $\mathfrak{p}$, $\mathcal{O}_\mathfrak{p}$, and the following chain:

$$\mathcal{O}_\mathfrak{p} = \mathcal{I}_0\mathcal{O}_\mathfrak{p} \supset \mathcal{I}_1\mathcal{O}_\mathfrak{p} \supset \mathcal{I}_2\mathcal{O}_\mathfrak{p} \cdots \supset \mathcal{I}_l\mathcal{O}_\mathfrak{p} = \mathcal{I}\mathcal{O}_\mathfrak{p} \qquad (*)$$

If $\mathcal{I}_i/\mathcal{I}_{i+1} \simeq \mathcal{O}/\mathfrak{q}$, for $\mathfrak{q} \neq \mathfrak{p}$, then $\mathcal{I}_i\mathcal{O}_\mathfrak{p} = \mathcal{I}_{i+1}\mathcal{O}_\mathfrak{p}$. This is true, as

$$\begin{aligned} \mathcal{I}_i/\mathcal{I}_{i+1} \simeq \mathcal{O}/\mathfrak{q} \quad &\implies \quad \mathcal{I}_i \supseteq \mathcal{I}_{i+1} \supseteq \mathfrak{q}\mathcal{I}_i \\ &\implies \quad \mathcal{I}_i\mathcal{O}_\mathfrak{p} \supseteq \mathcal{I}_{i+1}\mathcal{O}_\mathfrak{p} \supseteq \mathfrak{q}\mathcal{O}_\mathfrak{p}\mathcal{I}_i\mathcal{O}_\mathfrak{p} = \mathcal{I}_i\mathcal{O}_\mathfrak{p}, \end{aligned}$$

where the last equality follows from the fact that $\mathfrak{q} \neq \mathfrak{p}$. If $\mathcal{I}_i/\mathcal{I}_{i+1} \simeq \mathcal{O}/\mathfrak{p}$, then $\mathcal{I}_i\mathcal{O}_\mathfrak{p}/\mathcal{I}_{i+1}\mathcal{O}_\mathfrak{p} \simeq \mathcal{O}_\mathfrak{p}/\mathfrak{p}\mathcal{O}_\mathfrak{p} = \mathcal{O}/\mathfrak{p}$, as localization behaves nicely with respect to isomorphisms. (Section 2.3.4) Therefore, the series $(*)$ is the Jordan-Hölder filteration of $\mathcal{I}\mathcal{O}_\mathfrak{p}$ as an $\mathcal{O}_\mathfrak{p}$-ideal. Recall that $\mathfrak{p}$ is invertible and therefore, the local ring $\mathcal{O}_\mathfrak{p}$ is a Discrete Valuation Ring (DVR) ([Ste08, Prop 5.4]), and hence a Unique Factorization Domain (UFD). ([DF91, Chapter 8, Thm 12]). By uniqueness of the Jordan-Hölder filteration, we get that $\mathcal{I}\mathcal{O}_\mathfrak{p} = (\mathfrak{p}\mathcal{O}_\mathfrak{p})^{m_\mathfrak{p}}$. This shows that $\mathcal{I} \subset \mathcal{I}\mathcal{O}_\mathfrak{p} \cap \mathcal{O} = (\mathfrak{p}\mathcal{O}_\mathfrak{p})^{m_\mathfrak{p}} \cap \mathcal{O} = \mathfrak{p}^{m_\mathfrak{p}}$. Let $\mathfrak{p}_i$ (resp, $\mathfrak{p}'_j$) the invertible (resp, non-invertible) ideals that appear as Jordan-Hölder factors of $\mathcal{I}$, with multiplicity m_i (resp, m'_j). We claim that $\mathcal{I} \subseteq \mathfrak{q} := \prod_i \mathfrak{p}_i^{m_i}$.

Recall that, for each invertible factor $\mathfrak{p}_i$, the ideal $\mathcal{I} \subset \mathfrak{p}_i^{m_i}$. As the factors $\mathfrak{p}_i^{m_i}$'s are pairwise prime, we get

$$\mathcal{I} = \mathcal{I}(\mathfrak{p}_1^{m_1} + \mathfrak{p}_2^{m_2}) \subseteq \mathfrak{p}_1^{m_1}\mathfrak{p}_2^{m_2}$$

Continuing similarly, we get that $\mathcal{I} \subseteq \mathfrak{q}$.

Finally, for the index discussion, observe that

$$\begin{aligned} [\mathfrak{q}:\mathcal{I}] &= \frac{[\mathcal{O}:\mathcal{I}]}{[\mathcal{O}:\mathfrak{q}]} \\ &= \frac{\prod_i [\mathcal{O}:\mathfrak{p}_i]^{m_i} \times \prod_j [\mathcal{O}:\mathfrak{p}'_j]^{m'_j}}{\prod_i [\mathcal{O}:\mathfrak{p}_i^{m_i}]} \\ &= \prod_j [\mathcal{O}:\mathfrak{p}'_j]^{m'_j} \end{aligned}$$

Since $\mathfrak{q} := \prod_i \mathfrak{p}_i^{m_i}$, it follows from the Chinese remainder theorem (Theorem 2.14) that $[\mathcal{O}:\mathfrak{q}] = \prod_i [\mathcal{O}:\mathfrak{p}_i^{m_i}]$. Moreover, since each $\mathfrak{p}_i$ is invertible, the quotients $\mathfrak{p}_i^n/\mathfrak{p}_i^{n+1}$ and $\mathcal{O}/\mathfrak{p}_i$ are isomorphic (Lemma 2.17) and hence $[\mathcal{O}:\mathfrak{p}_i^{m_i}] = [\mathcal{O}:\mathfrak{p}_i] \cdot [\mathfrak{p}_i:\mathfrak{p}_i^2] \cdot \ldots \cdot [\mathfrak{p}_i^{m_i-1}:\mathfrak{p}_i^{m_i}] = [\mathcal{O}:\mathfrak{p}_i]^{m_i}$. Moreover, the non-invertible Jordan-Hölder factors contain $m\mathcal{O}$, by Lemma 2.31. By Remark 2.32, $Spec_\mathbb{Z}([\mathfrak{q}:\mathcal{I}]) \subseteq Spec_\mathbb{Z}(m)$. □

2.3.6 The Order LWE problem

There is a line of work in studying algebraic versions of LWE: Ring-LWE [LPR10], Polynomial-LWE [SSTX09], Order-LWE [BBPS19] and $\mathcal{L}$-LWE [PP19]. In this paper we will focus on Order-LWE. For setting the stage, let K be a number field, $\mathcal{O}$ an order in it, $\mathcal{Q}$ an integral ideal of $\mathcal{O}$ and $u \in (\mathcal{O} : \mathcal{Q}) = \{x \in K |\ x\mathcal{O} \subseteq \mathcal{Q}\}$. For fractional $\mathcal{O}$-ideals $\mathcal{I}$ and $\mathcal{J}$, we denote by $\mathcal{I}_{\mathcal{J}} := \mathcal{I}/\mathcal{J}\mathcal{I}$. We consider $\mathbb{T}_{\mathcal{O}^\vee} := K_{\mathbb{R}}/\mathcal{O}^\vee$. The Order-LWE distribution and problem are stated as follows:

Definition 2.34 ($\mathcal{O}$-LWE distribution)**.** *For $s \in \mathcal{O}_{\mathcal{Q}}^\vee$ and ψ an error distribution over $\mathbb{T}_{\mathcal{O}^\vee}$, we define a sample of the distribution $\mathcal{O}_{s,\psi,u}$ over $\mathcal{O}_{\mathcal{Q}} \times \mathbb{T}_{\mathcal{O}^\vee}$ by generating $a \leftarrow U(\mathcal{O}_{\mathcal{Q}})$, $e \leftarrow \psi$ and by outputting the pair $(a, b = u \cdot a \cdot s + e \bmod \mathcal{O}^\vee)$.*

Definition 2.35 ($\mathcal{O}$-LWE, Average-Case Decision problem)**.** *Let φ be a distribution over $\mathcal{O}_{\mathcal{Q}}^\vee$ and Υ a family of error distributions over $K_{\mathbb{R}}$. The average case decision $\mathcal{O}$-LWE problem, denoted as $\mathcal{O} - \mathrm{LWE}_{(\mathcal{Q},u),\varphi,\Upsilon}$, requires to distinguish independent samples from the distribution $\mathcal{O}_{s,\psi,u}$, where $s \leftarrow \varphi$ and $\psi \leftarrow \Upsilon$ and the same number of samples from the uniform distribution over $\mathcal{O}_{\mathcal{Q}} \times \mathbb{T}_{\mathcal{O}^\vee}$.*

If φ is the uniform distribution over $\mathcal{O}_{\mathcal{Q}}^\vee$, we drop it from the subscript. We recall that when $\mathcal{O} = \mathcal{O}_K$, $\mathcal{Q} = q\mathcal{O}_K$ and $u = 1/q$, the Order-LWE problem becomes the Ring-LWE problem.

The proof of the hardness results for algebraic LWE (Ring-LWE [LPR10, PRSD17], Polynomial-LWE [SSTX09], Module-LWE [LS12], Order-LWE [BBPS19]) follow the same blueprint. For a detailed proof, we refer the reader to [BBPS19]. Briefly, it iterates the following quantum step: given discrete Gaussian samples and an oracle for algebraic LWE, the quantum algorithm outputs narrower discrete Gaussian samples. To do this, it first, transforms an $\mathcal{O}$-LWE oracle, using polynomially many discrete Gaussian samples, into a BDD solver, and then uses the BDD solver to output discrete Gaussian samples of narrower parameter. A sufficient condition required to make BDD-samples on a dual lattice $\mathcal{L}^\vee$, along with discrete Gaussian samples over $\mathcal{L}$, into $\mathcal{O}$-LWE samples is that there must exist ($\mathcal{O}$-module) isomorphisms $f : \mathcal{L}/\mathcal{Q}\mathcal{L} \xrightarrow{\sim} \mathcal{O}/q\mathcal{O}$, and $g : \mathcal{O}^\vee/\mathcal{Q}\mathcal{O}^\vee \xrightarrow{\sim} \mathcal{L}^\vee/\mathcal{Q}\mathcal{L}^\vee$, that satisfy the compatibility condition $u \cdot z \cdot x = u \cdot f(z) \cdot g^{-1}(x) \bmod \mathcal{O}^\vee$, for all $z \in \mathcal{L}/\mathcal{Q}\mathcal{L}$, $x \in \mathcal{L}^\vee/\mathcal{Q}\mathcal{L}^\vee$ with $u \in (\mathcal{O} : \mathcal{Q})$. For efficiency reasons, we require the isomorphisms f and g to be both efficiently computable and invertible. The compatibility condition yields well-defined LWE samples. Formally,

Theorem 2.36. *Let K be an arbitrary number field of degree n and let $\mathcal{O} \subset K$ an order. Let $\mathcal{Q}$ be an integral $\mathcal{O}$-ideal, $u \in (\mathcal{O} : \mathcal{Q})$ and let $\alpha \in (0, 1)$ be such that $\alpha/\|u\|_\infty \geq 2 \cdot \omega(1)$. Let $\mathcal{S}$ be a subset of $\mathcal{O}$-ideal lattices such that, for any $\mathcal{L} \in \mathcal{S}$, there exist ($\mathcal{O}$-module) isomorphisms $f : \mathcal{L}/\mathcal{Q}\mathcal{L} \xrightarrow{\sim} \mathcal{O}/\mathcal{Q}\mathcal{O}$ and $g : \mathcal{O}^\vee/\mathcal{Q}\mathcal{O}^\vee \xrightarrow{\sim} \mathcal{L}^\vee/\mathcal{Q}\mathcal{L}^\vee$, both efficiently computable and invertible, such that $u \cdot z \cdot x = u \cdot f(z) \cdot g^{-1}(x) \bmod \mathcal{O}^\vee$ for any $z \in \mathcal{L}^\vee/\mathcal{Q}\mathcal{L}^\vee$ and $x \in \mathcal{L}/\mathcal{Q}\mathcal{L}$. Then, there is a polynomial-time quantum reduction from $\mathcal{S}$-DGS$_\gamma$ to $\mathcal{O}$-LWE$_{(\mathcal{Q},u),\Upsilon_{u,\alpha}}$, where*

$$\gamma = max\left\{\eta(\mathcal{L}) \cdot \sqrt{2}/\alpha \cdot \omega(1), \frac{\sqrt{2n}}{\lambda_1(\mathcal{L}^\vee)}.\right\}$$

Proof. (Overview) We first prove that the compatibility condition yields well-defined Order-LWE samples. Recall that the isomorphism f maps the discrete Gaussian sample z to the a part of the LWE sample, whereas the isomorphism g^{-1} maps the BDD-secret x to the LWE secret s. Then the compatibility condition yields $u \cdot z \cdot x = u \cdot a \cdot s \bmod \mathcal{O}^\vee$. Under well chosen parameters, as in Lemma [BBPS19, Lem 3.16], the discrete Gaussian distribution over $\mathcal{L}$ mod $\mathcal{Q}\mathcal{L}$ is almost the

uniform distribution over $\mathcal{L}/\mathcal{QL}$ (Lemma 2.5) and since f is an isomorphism, a is almost uniform over $\mathcal{O}/\mathcal{QO}$. Let $y = x + e$ be the BDD coset and e', an additional error term. Then the LWE samples are defined as,

$$\begin{aligned}(a, b) =& (f(z), u \cdot z \cdot y + e' \mod \mathcal{O}^\vee) \\ =& (f(z), u \cdot z \cdot x + \tilde{e} \mod \mathcal{O}^\vee) \\ =& (f(z), u \cdot a \cdot s + \tilde{e} \mod \mathcal{O}^\vee).\end{aligned}$$

For a detailed analysis of the error term, we refer the reader to the proof of [BBPS19, Lem 2.36]. This shows that the compatibility condition implies the well-defined LWE samples and hence the algorithm in Lemma [BBPS19, Lem 3.16].

As described earlier, the hardness proof relies on applying Lemma [BBPS19, Lem 3.15] iteratively for transforming discrete Gaussian samples into discrete Gaussian samples of a narrower parameter. This iterative step uses Lemma [BBPS19, Lem 3.16] and Lemma [PRSD17, Lem 6.7]. As a starting point for the iteration, samples from a discrete Gaussian distribution of a large enough parameter are efficiently generated using [Reg05, Lem 3.2]. □

Hardness results for Ring-LWE [LPR10] [PRSD17], Polynomial-LWE [SSTX09] and Order-LWE [BBPS19] use invertibility of the ideal lattices considered, to derive the compatible maps f and g.

Remark 2.37. *Although Theorem 2.36 presents the hardness result for Order-LWE, a similar proof also derives the hardness result for the dual setting of Order-LWE, as defined in [BBPS19, Def 3.3], where $a \in \mathcal{O}^\vee/\mathcal{QO}^\vee$ and $s \in \mathcal{O}/\mathcal{QO}$. The only difference consists in switching the maps f and g in the* BDD*-to-$\mathcal{O}^\vee$-*LWE *reduction.*

2.3.7 Gaussian distributions over $K_\mathbb{R}$ and $K_\mathbb{R}/\mathcal{O}^\vee$

The proofs of the following results follow from basic properties of the Gaussian vector distributions. However, we include the proof of lemma 2.39 here.

Lemma 2.38. *Let $K = \mathbb{Q}(\theta)$ be a number field of degree n. If $e = e_0 + e_1\theta + \ldots + e_{n-1}\theta^{n-1}$ drawn from D_α over $K_\mathbb{R}$ then $(e_0, e_1, \ldots, e_{n-1})$ satisfies the distribution $D_{\alpha\sqrt{(Vf^*Vf)^{-1}}}$ over $\mathbb{R}^n$, where V_f is the Vandermonde corresponding to the roots of θ. In the special case, when K is the power-of-two cyclotomic extension, the error distribution simplifies to $D_{\alpha\sqrt{(Vf^*Vf)^{-1}}} = D_{\alpha/\sqrt{n}}$.*

Let $Tr = Tr_{K_\mathbb{R}/\mathbb{R}}$ and by $\overline{x}$ the complex conjugation of an element $x \in K_\mathbb{R}$. For an order $\mathcal{O} \subseteq K$, let $P_\mathcal{O} = (Tr(p_i \cdot \overline{p_j}))_{1 \le i,j, \le n}$, such that $\{p_i\}_{1 \le i \le n}$ is the $\mathbb{Z}$-basis of $\mathcal{O}$. Fix an orthonormal $\mathbb{R}$ basis of $K_\mathbb{R}$, $\vec{b} = (b_i)_{1 \le i \le n}$, i.e. $Tr(b_i \cdot \overline{b}_j) = \delta_{ij}$. Notice that for $x \in K_\mathbb{R}$, $x = \sum_{i=1}^{n} Tr(x \cdot \overline{b_i}) b_i = \sum_{i=1}^{n} Tr(x \cdot b_i)\overline{b_i}$. Consider the matrix $P_{\mathcal{O},\vec{b}} = (Tr(b_i \cdot p_j))_{1 \le i,j \le n}$. Observe that $P^t_{\mathcal{O},\vec{b}} \cdot P_{\mathcal{O},\vec{b}} = P_\mathcal{O}$, since

$$(P_\mathcal{O})_{ij} = Tr(p_i \cdot \overline{\sum_{k=1}^{n} Tr(p_j \cdot b_k)\overline{b_k}}) = \sum_{k=1}^{n} Tr(p_i \cdot b_k) \cdot Tr(b_k \cdot p_j) = (P_{\mathcal{O},\vec{b}})^t_i \cdot (P_{\mathcal{O},\vec{b}})_j$$

We used in the above equation the fact that Tr takes real values and it is $\mathbb{R}$ linear.

Lemma 2.39 ([PP19, Sect 5.3.]). *Let e be drawn according to a Gaussian distribution D_α over $K_\mathbb{R}$. Then the coefficients of e with respect to a $\mathbb{Z}$-basis of $\mathcal{O}^\vee$ satisfy a Gaussian distribution over $\mathbb{R}^n$ of covariance matrix $\alpha^2 \cdot P_\mathcal{O}$. In particular, $e \mod \mathcal{O}^\vee$ follows a Gaussian distribution over $\mathbb{R}^n \mod \mathbb{Z}^n$ of the same covariance matrix.*

Proof. First, notice that the coefficients of the error with respect to the $\mathbb{Z}$-basis of $\mathcal{O}^\vee$, $p^\vee$, can be seen from the following vector $Tr(e \cdot \vec{p}) = (Tr(e \cdot p_i))_{1 \leq i \leq n}$. Indeed, let us write e in terms of the $\mathbb{Z}$-basis elements of $\mathcal{O}^\vee$ as $e = e_1 p_1^\vee + \ldots + e_n p_n^\vee$. By using the linearity of the trace over $\mathbb{R}$, we get that $Tr(e \cdot p_i) = \sum_{j=1}^{n} e_i Tr(p_j^\vee \cdot p_i) = e_i$.

Recall from Section 2.2.1 that given an orthonormal $\mathbb{R}$ basis $\vec{b} = (b_i)_{1 \leq i \leq n}$ of $K_\mathbb{R}$, sampling e according to the Gaussian distribution D_α over $K_\mathbb{R}$ means sampling a vector of coefficients, $\overline{e}$, with respect to this $\vec{b}$ according to the same distribution over $\mathbb{R}^n$. So $e = \vec{b}^t \cdot \overline{e}$, where $\overline{e}$ follows the distribution D_α. Therefore, by using again the linearity of the trace over $\mathbb{R}$, we get the following:

$$Tr(\vec{p} \cdot e) = Tr(\vec{p} \cdot \vec{b}^t \cdot \overline{e}) = Tr(\vec{p} \cdot \vec{b}^t) \cdot \overline{e} = P_{\mathcal{O},\vec{b}}^t \cdot \overline{e}.$$

Since $\overline{e}$ satisfies the Gaussian distribution of covariance matrix $\alpha^2 \cdot Id_{n \times n}$, it implies that $Tr(\vec{p} \cdot e)$ follows the Gaussian distribution of covariance matrix $\alpha^2 \cdot P_{\mathcal{O},b}^t \cdot P_{\mathcal{O},b} = \alpha^2 \cdot P_\mathcal{O}$. This completes the proof.

□

3 Embedding integer lattices in number fields

In this section, we embed (unstructured) integer lattices into a number field and discuss the properties this algebraic structure yields. These efforts are an attempt to analyze the hardness and the possibility of solving short vector problems on integer lattices.

Fix a number field $K := \mathbb{Q}(\theta)$ of degree n. We describe the (inverse of the) well-known coefficient embedding. Let $\vec{\theta} = (1, \theta, \theta^2, \ldots, \theta^{n-1})$. Let

$$L = \mathbb{Z}\mathbf{a}_1 + \mathbb{Z}\mathbf{a}_2 + \cdots + \mathbb{Z}\mathbf{a}_n \subseteq \mathbb{Z}^n,$$

be an integer lattice generated by n linearly independent elements $\mathbf{a}_1, \ldots, \mathbf{a}_n \in \mathbb{Z}^n$, with $\mathbf{a}_i = (a_{1i}, a_{2i}, \ldots a_{ni})^t$. Embed $\mathbf{a}_i$ in K as $a_i = \langle \mathbf{a}_i, \vec{\theta} \rangle = a_{1i} + a_{2i}\theta + \ldots + a_{ni}\theta^{n-1}$. It follows from the definition of the Trace function on K that a_i's are $\mathbb{Z}$-linearly independent and hence form an n-dimensional lattice in K. Denote by

$$\mathcal{L} = \mathbb{Z}a_1 + \mathbb{Z}a_2 + \cdots \mathbb{Z}a_n \subseteq \mathbb{Z}[\theta],$$

the embedding of L in K via this coefficient embedding.

Let $\{\sigma_i\}_{i=1}^n$ be the set of real and complex embeddings of K. Define the Minkowski embedding; $\sigma : K \longrightarrow \mathbb{C}^n$ as $\sigma(a) = (\sigma_1(a), \sigma_2(a) \ldots \sigma_n(a))$. The $\mathbb{R}$-vector space generated by $\sigma(K)$ is known as the Minkowski space $K_\mathbb{R}$. Let $V_f = (\sigma_i(\theta^{j-1}))_{1 \leq i,j \leq n}$ denote the Vandermonde matrix corresponding to f. Then, the coefficient and the Minkowski embedding are related as follows; for any $a \in K$, the image $\sigma(a) = V_f \cdot \text{coef}(a)$, where $\text{coef}(a) \in \mathbb{Q}^n$ are the coefficients of a with respect to the power basis $\vec{\theta}$ and V_f is the Vandermonde matrix of f, the minimal polynomial for $\theta \in K$. In other words, the image of $\mathcal{L}$, under the Minkowski map, equals the image of L, under the $\mathbb{C}$-linear transformation defined by V_f: $\sigma(\mathcal{L}) = V_f \cdot L$. We would like to clarify that we consider $\sigma(\mathcal{L})$ as a lattice in $K_\mathbb{R}$, which is isomorphic to $\mathbb{R}^n$. Therefore, these lattices can be viewed as lattices in $\mathbb{R}^n$.

3.1 Geometric properties: Relating lattice parameters of L and $\mathcal{L}$

To discuss the geometric properties, we identify $\mathcal{L}$ with $\sigma(\mathcal{L})$. Let $s_n(V_f) \leq \ldots \leq s_1(V_f)$ be the singular values of V_f. Recall that the spectral norm of V_f is given by the maximum singular value, $s_1(V_f)$, whereas the spectral norm of V_f^{-1} is given by the inverse of the smallest singular value, $s_n(V_f)$. The following result describes how the embedding distorts the Euclidean norm and volume.

Lemma 3.1. *Let $\mathcal{L}$ be the image of L in K, under the coefficient embedding, with respect to $\vec{\theta}$. Then,*

(i) $s_n(V_f) \cdot \|coef(a)\| \leq \|\sigma(a)\| \leq s_1(V_f) \cdot \|coef(a)\|$, *for any* $a \in K$,

(ii) $s_n(V_f) \cdot \lambda_1(L) \leq \lambda_1(\mathcal{L}) \leq s_1(V_f) \cdot \lambda_1(L)$, *and*

(iii) $det(\mathcal{L}) = det(\mathbb{Z}[\theta]) \cdot det(L)$.

Proof. The proofs follow from the definition of the singular values, the successive minima and the Minkowski embedding.
(i) Since $\sigma(a) = V_f \cdot \mathrm{coef}(a)$, the norm

$$\|a\| := \|\sigma(a)\| = \|V_f \cdot \mathrm{coef}(a)\| \leq \|V_f\| \cdot \|\mathrm{coef}(a)\| = s_1(V_f) \cdot \|\mathrm{coef}(a)\|.$$

The converse follows similarly, using $\mathrm{coef}(a) = V_f^{-1} \cdot \sigma(a)$ and $\|V_f^{-1}\| = 1/s_n(V_f)$.
(ii) By definition of the coefficient embedding, $x \in \mathcal{L}$ if and only if $\mathbf{x} := \mathrm{coef}(x) \in L$. If $\|x\| = \lambda_1(\mathcal{L})$, then by (i),

$$\lambda_1(L) \leq \|\mathbf{x}\| \leq \|x\|/s_n(V_f) = \lambda_1(\mathcal{L})/s_n(V_f).$$

Conversely, let $\mathbf{y} \in L$ and let $y \in \mathcal{L}$ be such that $\mathbf{y} = \mathrm{coef}(y)$. If $\|\mathbf{y}\| = \lambda_1(L)$, then

$$\lambda_1(\mathcal{L}) \leq \|y\| \leq s_1(V_f) \cdot \|\mathbf{y}\| = s_1(V_f) \cdot \lambda_1(L).$$

(iii) Recall that $\vec{\theta}$ forms a $\mathbb{Z}$-basis for the lattice $\mathbb{Z}[\theta]$. Let $\sigma_1, \sigma_2, \ldots, \sigma_n$ denote the n embeddings of the number field K. Since σ_i's are $\mathbb{Q}$-linear maps,

$$\begin{aligned}
\det(\mathcal{L}) &:= \det \begin{pmatrix} \sigma_1(a_1) & \ldots & \sigma_1(a_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(a_1) & \ldots & \sigma_n(a_n) \end{pmatrix} \\
&= \det \begin{pmatrix} \sigma_1(1) & \sigma_1(\theta) & \ldots & \sigma_1(\theta^{n-1}) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(1) & \sigma_n(\theta) & \ldots & \sigma_n(\theta^{n-1}) \end{pmatrix} \cdot \det \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix} \\
&= \det(\mathbb{Z}[\theta]) \cdot \det(L).
\end{aligned}$$

□

Remark 3.2. *As $\mathcal{L} \subseteq \mathbb{Z}[\theta]$, the index $[\mathbb{Z}[\theta] : \mathcal{L}] = det(\mathcal{L})/det(\mathbb{Z}[\theta]) = det(L)$. In particular, in a monogenic number field K, i.e. $\mathcal{O}_K = \mathbb{Z}[\theta]$, we have $[\mathcal{O}_K : \mathcal{L}] = det(L) := [\mathbb{Z}^n : L]$. In fact, the quotient groups $\frac{\mathcal{O}_K}{\mathcal{L}}$ and $\frac{\mathbb{Z}^n}{L}$ are isomorphic. This follows from the definition of the coefficient embedding and the fact that $\mathcal{O}_K$ and $\mathcal{L}$ are the images of $\mathbb{Z}^n$ and L, respectively, under this embedding.*

Since the LWE hardness results solve DGS on (relevant) lattices, we analyze how the coefficient embedding alters DGS on $\mathcal{L}$ from DGS on L. The proof follows from basic properties of the Gaussian vector distribution.

Proposition 3.3. *$\mathcal{L}$-DGS$_\alpha$ is equivalent to L-DGS$_{\alpha\cdot\sqrt{(V_f^* V_f)^{-1}}}$.*

Proof. Let $x = x_0 + x_1\theta + \ldots + x_{n-1}\theta^{n-1}$ be sampled from the Gaussian D_α over $K_\mathbb{R}$. Then, by Lemma 2.38, the coefficients, $\mathbf{x} := (x_0, x_1, \ldots, x_{n-1}) \leftarrow D_{\alpha\cdot\sqrt{(V_f^* V_f)^{-1}}}$ over $\mathbb{R}^n$. The definition of the coefficient and the Minkowski embedding implies that $D_\alpha(x) = D_\alpha(V_f \cdot \mathbf{x}) = D_{\alpha\sqrt{(V_f^* V_f)^{-1}}}(\mathbf{x})$, for all $x \in \mathcal{L}$. It further implies that $\sum_{x\in\mathcal{L}} \rho_\alpha(x) = \sum_{\mathbf{x}\in L} \rho_{\alpha\sqrt{(V_f^* V_f)^{-1}}}(\mathbf{x})$. Therefore, the two discrete Gaussians coincide:

$$D_{\mathcal{L},\alpha} \equiv D_{L,\alpha\sqrt{(V_f^* V_f)^{-1}}}.$$

This observation lies at the heart of the equivalence stated in the proposition. The reduction from $\mathcal{L}$-DGS$_\alpha$ to L-DGS$_{\alpha\cdot\sqrt{V_f^{-1}(V_f^{-1})^*}}$ is described by an algorithm that takes as input a lattice $\mathcal{L} \subset K$ and outputs discrete Gaussian samples over $\mathcal{L}$, by using a DGS sampler for the lattice $L = V_f^{-1}\cdot\sigma(\mathcal{L})$ in $\mathbb{Z}^n$, as follows. Let $\mathbf{x} \leftarrow D_{L,\alpha\sqrt{(V_f^* V_f)^{-1}}}$, then $x := \langle \mathbf{x}, \vec{\theta}\rangle \in \mathcal{L}$ follows the distribution $D_{\mathcal{L},\alpha}$. The converse reduction is realized by a similar argument. □

The next result describes how the basis of the dual of the integer lattice L changes, under the (inverse) coefficient embedding. The proof essentially follows from the definition of the coefficient and the Minkowski embedding.

Proposition 3.4. *Let $L \subset \mathbb{Z}^n$ be a integer lattice whose basis is given by the columns of a matrix B. Consider $\mathcal{L}$, its coefficient embedding in a number field K of defining polynomial f. Then, the field elements whose coefficient representations are the columns of $(V_f{}^t V_f)^{-1} \cdot (B^t)^{-1}$ form a basis for $\mathcal{L}^\vee$.*

Proof. Since $\sigma(\mathcal{L}) = V_f \cdot L$, the columns of $V_f \cdot B$ form a basis for $\sigma(\mathcal{L})$. Therefore, its dual, $\sigma(\mathcal{L})^*$ in H endowed with the scalar product on $\mathbb{C}^n$, has as a basis, the columns of $((\overline{V_f}\cdot\overline{B})^t)^{-1} = (\overline{V_f}^t)^{-1}\cdot(B^t)^{-1}$. Further, as $\sigma(\mathcal{L}^\vee) = \overline{\sigma(\mathcal{L})^*}$, we use the relation between the coefficient and the Minkowski embedding, to conclude that field elements in K formed by taking inner products of the columns of the matrix $V_f^{-1}\cdot(V_f{}^t)^{-1}\cdot(B^t)^{-1} = (V_f{}^t V_f)^{-1}\cdot(B^t)^{-1}$ with the power basis $\vec{\theta}$ form a basis for $\mathcal{L}^\vee$. □

Remark 3.5. *By the definition of the Vandermonde matrix V_f (see the discussion at the beginning of Section 3), the (i,j)-th entry of $V_f^t V_f$ is $\sum_{k=1}^n \sigma_k(\theta^{i+j-2}) = Tr(\theta^{i+j-2})$. In the special case of a power of two cyclotomic field,*

$$Tr(\theta^{i+j-2}) = \begin{cases} n & \text{if } i+j-2 = 0 \\ -n & \text{if } i+j-2 \neq 0 \text{ and } i+j-2 = 0 \mod n \\ 0 & \text{otherwise} \end{cases}$$

See [LPR13, Lem. 2.15]. Therefore, in this case, $V_f^t V_f = n\cdot\begin{pmatrix}\boldsymbol{e}_1 & -\boldsymbol{e}_n & \ldots & -\boldsymbol{e}_2\end{pmatrix}$, where $\boldsymbol{e}_i$ is the canonical basis vector with 1 in the i-th place and 0's elsewhere. By Proposition 3.4, a basis of the dual $\mathcal{L}^\vee$ can be found by taking inner products of the columns of the matrix $\frac{1}{n}\cdot\begin{pmatrix}\boldsymbol{e}_1 & -\boldsymbol{e}_n & \ldots & -\boldsymbol{e}_2\end{pmatrix}\cdot (B^t)^{-1}$ with the power basis.

3.2 Algebraic properties: studying the ideal structure of $\mathcal{L}$

The coefficient embedding of $\mathbb{Q}^n$ into K with respect to $\vec{\theta}$ maps $\mathbb{Z}^n$ to $\mathbb{Z}[\theta] \subseteq \mathcal{O}_K$. When the field is monogenic, we choose $\theta \in \mathcal{O}_K$ such that $\mathcal{O}_K$ equals $\mathbb{Z}[\theta]$. In this section, we assume that K is any number field. However, we stress that some of the results look specifically appealing when K is monogenic.

Lemma 3.6. *Let $\mathcal{O}$ be an order in K and let $\mathcal{I}$ be an integral $\mathcal{O}$-ideal. Then, the set $\mathbb{Z} + \mathcal{I}$, contained in $\mathcal{O}$, is an order in K.*

Proof. Since $\mathcal{I}$ is an ideal and hence, in particular, an additive group of rank n, the set $\mathbb{Z}+\mathcal{I}$ is an additive group of rank n. It is also clear that it is a subgroup of $\mathcal{O}$ and contains 1. To see that it is a ring, let $z_1 + i_1$ and $z_2 + i_2$ be two elements in $\mathbb{Z}+\mathcal{I}$. Then,

$$(z_1 + i_1)(z_2 + i_2) = z_1 z_2 + [i_1(z_2 + i_2) + z_1 i_2] \in \mathbb{Z} + \mathcal{I},$$

as $\mathcal{I}$ is closed under scalar multiplication by elements $(z_2 + i_2)$, $z_1 \in \mathcal{O}$. □

The next result proves that given a lattice $\mathcal{L}$ in K, one can always construct an order such that $\mathcal{L}$ is an ideal in it. Recall that the exponent e of a group G is the smallest positive integer such that $e \cdot g = 0$, for all $g \in G$.

Lemma 3.7. *Let $\mathcal{O}$ be an order in K, and let $\mathcal{L} \subseteq \mathcal{O}$ be an additive subgroup of $\mathcal{O}$. Then, $\mathcal{L}$ is an ideal of the order $\mathbb{Z} + m\mathcal{O}$, where m is the exponent of the (additive) quotient group $\mathcal{O}/\mathcal{L}$.*

Proof. As $m\mathcal{O}$ is an integral ideal of $\mathcal{O}$, by Lemma 3.6, the set $\mathbb{Z} + m\mathcal{O}$ is an order. We show that $\mathcal{L}$ is closed under scalar multiplication by elements in $\mathbb{Z} + m\mathcal{O}$, or equivalently, by elements in $m\mathcal{O}$. Using the fact that $m\mathcal{O} \subseteq \mathcal{L}$ and that $\mathcal{L} \subseteq \mathcal{O}$, we get that

$$m\mathcal{O} \cdot \mathcal{L} \subseteq m\mathcal{O} \cdot \mathcal{O} \subseteq m\mathcal{O} \subseteq \mathcal{L}$$

□

Applying Lemma 3.7 to the lattice $\mathcal{L} \subseteq \mathbb{Z}[\theta] \subseteq \mathcal{O}_K$, we get

Corollary 3.8. *Let m_K and m_θ be exponents of the quotient groups $\mathcal{O}_K/\mathcal{L}$ and $\mathbb{Z}[\theta]/\mathcal{L}$, respectively. Then $\mathcal{L}$ is an ideal in (both) the orders $\mathbb{Z}+m_K\mathcal{O}_K$ and $\mathbb{Z}+m_\theta\mathbb{Z}[\theta]$. Further, if the index $[\mathcal{O}_K : \mathbb{Z}[\theta]]$ is coprime to m_θ, then $\mathbb{Z} + m_K\mathcal{O}_K \subseteq \mathbb{Z} + m_\theta\mathbb{Z}[\theta]$.*

Proof. The first claim in the statement follows from Lemma 3.7. For the second, consider the following short exact sequence induced by inclusion,

$$0 \longrightarrow \frac{\mathbb{Z}[\theta]}{\mathcal{L}} \longrightarrow \frac{\mathcal{O}_K}{\mathcal{L}} \longrightarrow \frac{\mathcal{O}_K}{\mathbb{Z}[\theta]} \longrightarrow 0$$

Since the cardinality of the groups, $\mathbb{Z}[\theta]/\mathcal{L}$ and $\mathcal{O}_K/\mathbb{Z}[\theta]$ are coprime, by the Schur-Zassenhaus theorem, the above sequence yields $\frac{\mathcal{O}_K}{\mathcal{L}} = \frac{\mathbb{Z}[\theta]}{\mathcal{L}} \oplus \frac{\mathcal{O}_K}{\mathbb{Z}[\theta]}$. Let e denote the exponent of $\mathcal{O}_K/\mathbb{Z}[\theta]$, then the direct sum and the coprimality condition imply $m_K = m_\theta \cdot e$. Therefore

$$\mathbb{Z} + m_K\mathcal{O}_K \subseteq \mathbb{Z} + m_\theta \cdot e\mathcal{O}_K \subseteq \mathbb{Z} + m_\theta\mathbb{Z}[\theta].$$

□

Let $\mathcal{O}_{\mathcal{L}}$ denote the ring of multipliers of $\mathcal{L}$ in K, i.e., it is the largest order in K such that $\mathcal{L}$ is an ideal of it. By Corollary 3.8,

$$\mathbb{Z} + m_K\mathcal{O}_K \subseteq \mathcal{O}_{\mathcal{L}} \quad \text{and} \quad \mathbb{Z} + m_\theta\mathbb{Z}[\theta] \subseteq \mathcal{O}_{\mathcal{L}} \tag{3.2.1}$$

Recall that $\mathcal{C}_{\mathcal{L}} := \{x \in K : x\mathcal{O}_K \subseteq \mathcal{O}_{\mathcal{L}}\}$, and $\mathcal{C}_\theta := \{x \in K : x\mathbb{Z}[\theta] \subseteq \mathcal{O}_{\mathcal{L}}\}$ are conductors of $\mathcal{O}_{\mathcal{L}}$ with respect to the orders $\mathcal{O}_K$ and $\mathbb{Z}[\theta]$, respectively. Then, $\mathcal{C}_{\mathcal{L}}$ is the largest $\mathcal{O}_K$-ideal in $\mathcal{O}_{\mathcal{L}}$, and $\mathcal{C}_\theta$ is the largest $\mathbb{Z}[\theta]$-ideal in $\mathcal{O}_{\mathcal{L}}$. Further, by Equation (3.2.1),

$$m_K\mathcal{O}_K \subseteq \mathcal{C}_{\mathcal{L}} \quad \text{and} \quad m_\theta\mathbb{Z}[\theta] \subseteq \mathcal{C}_\theta. \tag{3.2.2}$$

Note that both $\mathcal{C}_{\mathcal{L}}$ and $\mathcal{C}_\theta$ are also $\mathcal{O}_{\mathcal{L}}$-ideals. We stress that these well known results hold, and their proofs remain unchanged, even in our general scenario where $\mathbb{Z}[\theta]$ and $\mathcal{O}_{\mathcal{L}}$ may not necessarily share an order relation with respect to set containment. See Section 2.3.3 for more details. Recall that under the assumption that m_θ is coprime to $[\mathcal{O}_K : \mathbb{Z}[\theta]]$, Corollary 3.8 yields a chain of orders, $\mathbb{Z} + m_K\mathcal{O}_K \subseteq \mathbb{Z} + m_\theta\mathbb{Z}[\theta] \subseteq \mathbb{Z}[\theta] \subseteq \mathcal{O}_K$. The assumption that m_θ is coprime to $[\mathcal{O}_K : \mathbb{Z}[\theta]]$ has the following effect on the conductor $\mathcal{C}_\theta$.

Lemma 3.9. *If $(m_\theta, [\mathcal{O}_K : \mathbb{Z}[\theta]]) = 1$, then $\mathcal{C}_\theta$ is an invertible $\mathbb{Z}[\theta]$-ideal.*

Proof. It follows from Equation (3.2.2) that $\mathcal{C}_\theta \mid m_\theta\mathbb{Z}[\theta]$. Since m_θ is coprime to the index $[\mathcal{O}_K : \mathbb{Z}[\theta]]$, the conductor $\mathcal{C}_\theta$ is coprime to the conductor of $\mathbb{Z}[\theta]$ in $\mathcal{O}_K$. This is a sufficient condition for invertiblity as a $\mathbb{Z}[\theta]$-ideal. See Theorem 2.27. □

4 New Hardness Results for $\mathcal{O}$-LWE

In this section, we extend and enhance the hardness results for Order-LWE from [BBPS19] as follows:

- We prove extended versions of worst-case hardness results for both $\mathcal{O}$-LWE and $\mathcal{O}^\vee$-LWE that follow for all $\mathcal{O}$-ideals, with same approximation factors as in the previous hardness statements for Order-LWE and Ring-LWE.
- We extend the worst-case hardness result for Ring-LWE that follows not only for $\mathcal{O}_K$-ideals, but also for $\mathcal{O}$-ideals, for any order $\mathcal{O}$ of index coprime to the Ring-LWE modulus q. However, it incurs a penalty in the approximation factor, which depends on the conductor of the order. This result is complementary to [BBPS19, Thm 3.8 & Cor. 5.2].

4.1 Worst-Case Hardness for All $\mathcal{O}$-ideals

We begin this section with a non-maximal order $\mathcal{O}$ in the number field K. Let $m = [\mathcal{O}_K : \mathcal{O}]$ be the index of $\mathcal{O}$ in $\mathcal{O}_K$. Recall that for an ideal $\mathcal{I}$ of a ring R, $Spec_R(\mathcal{I})$ is the set of all prime ideals in R that contain $\mathcal{I}$. We denote by $\mathrm{Id}(\mathcal{O})$ the set of all fractional $\mathcal{O}$-ideals and further remark that $\mathrm{Id}(\mathcal{O}_K) \subsetneq \mathrm{Id}(\mathcal{O})$. For simplicity of the notation, we denote by $\mathcal{O}\text{-LWE}_{q,\Upsilon}$ the Order-LWE problem with modulus ideal $q\mathcal{O}$, $u = 1/q$, and a distribution Υ over a family of error distributions over $K_{\mathbb{R}}$. Our improved hardness results for $\mathcal{O}$-LWE and $\mathcal{O}^\vee$-LWE are as follows. The definition of $\mathcal{O}^\vee$-LWE is as in [BBPS19, Def 3.3].

Theorem 4.1. *Let K be an arbitrary number field of degree n. Let $\alpha \in (0,1)$ such that $\alpha \cdot q \geq 2 \cdot \omega(1)$. Choose an integer modulus q, coprime to the index $[\mathcal{O}_K : \mathcal{O}]$. Then there are polynomial time quantum reductions*

$$Id(\mathcal{O})\text{-}\mathtt{DGS}_\gamma \longrightarrow \mathcal{O}\text{-LWE}_{q,\Upsilon_\alpha} \tag{4.1.1}$$

$$Id(\mathcal{O})\text{-}\mathtt{DGS}_\gamma \longrightarrow \mathcal{O}^\vee\text{-LWE}_{q,\Upsilon_\alpha} \tag{4.1.2}$$

where $\gamma = max\left\{\eta(\mathcal{L}) \cdot \sqrt{2}/\alpha \cdot \omega(1), \frac{\sqrt{2n}}{\lambda_1(\mathcal{L}^\vee)}\right\}$.

As mentioned in the introduction, the hardness result for Order-LWE, as proved in [BBPS19], showed that $\mathcal{O}$-LWE is at least as hard as lattice problems on lattices that are *invertible* $\mathcal{O}$-ideals. The theorem above extends the result to include non-invertible $\mathcal{O}$-ideals as well, thereby closing the gap. We, however, restrict to the modulus being coprime to the index $[\mathcal{O}_K : \mathcal{O}]$. No such assumption was made on the modulus in [BBPS19, Thm 3.8].

Note that both the hardness results compare the LWE problems with lattice problems on the same set of number field lattices, the $\mathcal{O}$-ideals. This is because the $\mathcal{O}$-LWE and $\mathcal{O}^\vee$-LWE problems are equivalent as long as the modulus q is coprime to the index $[\mathcal{O}_K : \mathcal{O}]$. This equivalence was also studied in [BBPS19, Rem. 3.5], but under a stronger assumption of $\mathcal{O}^\vee$ being an invertible $\mathcal{O}$-ideal.

Proposition 4.2. *Let K be an arbitrary number field of degree n and $\mathcal{O}$ be an order. Choose an integer modulus q, coprime to the index $[\mathcal{O}_K : \mathcal{O}]$, and Υ a distribution over a family of error distributions over $K_\mathbb{R}$. Then, the $\mathcal{O}$-LWE$_{q,\Upsilon}$ and the $\mathcal{O}^\vee$-LWE$_{q,\Upsilon}$ problems are equivalent.*

Proof. Define a map $f : \frac{\mathcal{O}}{q\mathcal{O}} \longrightarrow \frac{\mathcal{O}^\vee}{q\mathcal{O}^\vee}$ as a composition of the following three isomorphsims

$$\begin{array}{ccccccc} \dfrac{\mathcal{O}}{q\mathcal{O}} & \overset{\sim}{\hookrightarrow} & \dfrac{\mathcal{O}_K}{q\mathcal{O}_K} & \overset{\sim}{\longrightarrow} & \dfrac{\mathcal{O}_K^\vee}{q\mathcal{O}_K^\vee} & \overset{\sim}{\hookrightarrow} & \dfrac{\mathcal{O}^\vee}{q\mathcal{O}^\vee} \\ a & \to & a + q\mathcal{O}_K & \to & ta + q\mathcal{O}_K^\vee & \to & ta + q\mathcal{O}^\vee := f(a) \end{array}$$

The first and the last isomorphisms follow from Lemma 2.19, under the coprimality condition on q, as q is coprime to the indices $[\mathcal{O}_K : \mathcal{O}]$ and $[\mathcal{O}^\vee : \mathcal{O}_K^\vee]$, respectively. The middle map is an application of the Cancellation Lemma 2.17 and we let $t \in \mathcal{O}_K^\vee$ be the element, multiplication by which, yields the isomorphism. Then, for $a \in \mathcal{O}/q\mathcal{O}$ and $s \in \mathcal{O}^\vee/q\mathcal{O}^\vee$, the cosets $a \cdot s + q\mathcal{O}^\vee$ and $f(a) \cdot f^{-1}(s) + q\mathcal{O}^\vee$ are equal. To see this, let $s' = f^{-1}(s) \in \mathcal{O}/q\mathcal{O}$. Then,

$$\begin{aligned} a \cdot s + q\mathcal{O}^\vee &= a \cdot f(s') + q\mathcal{O}^\vee \\ &= a \cdot (ts' + q\mathcal{O}^\vee) + q\mathcal{O}^\vee \\ &= tas' + q\mathcal{O}^\vee && \text{as } q \cdot a\mathcal{O}^\vee \subseteq q\mathcal{O}^\vee \\ &= (ta + q\mathcal{O}^\vee) \cdot s' + q\mathcal{O}^\vee && \text{as } q \cdot s'\mathcal{O}^\vee \subseteq q\mathcal{O}^\vee \\ &= f(a) \cdot f^{-1}(s) + q\mathcal{O}^\vee \end{aligned}$$

Therefore, the $\mathcal{O}$-LWE samples $(a, b := \frac{1}{q} \cdot a \cdot s + e \mod \mathcal{O}^\vee)$, where $e \leftarrow \varphi$ for some $\varphi \leftarrow \Upsilon$, can be transformed to $\mathcal{O}^\vee$-LWE samples by considering $(f(a), b := \frac{1}{q} \cdot f(a) \cdot f^{-1}(s) + e \mod \mathcal{O}^\vee)$, where $f(a) \in \mathcal{O}^\vee/q\mathcal{O}^\vee$ and $f^{-1}(s) \in \mathcal{O}/q\mathcal{O}$. Conversely, the $\mathcal{O}^\vee$-LWE samples $(a', b' := \frac{1}{q} \cdot a' \cdot s' + e' \mod \mathcal{O}^\vee)$, where $e' \leftarrow \varphi$ for some $\varphi \leftarrow \Upsilon$, can be made into $\mathcal{O}$-LWE samples by taking $(f^{-1}(a'), b := \frac{1}{q} \cdot f^{-1}(a') \cdot f(s') + e' \mod \mathcal{O}^\vee)$, where $f^{-1}(a') \in \mathcal{O}/q\mathcal{O}$ and $f(s') \in \mathcal{O}^\vee/q\mathcal{O}^\vee$. □

Theorem 4.1 coupled with the reduction from SIVP to DGS (see Lemma 2.11) yields the following generalization of [LPR10, Thm 3.6], [PRSD17, Corollary 6.3].

Corollary 4.3. *Let K be an arbitrary number field of degree n. Let $\alpha \in (0,1)$ satisfy $\alpha q \geq 2\omega(1)$ and q be coprime to $[\mathcal{O}_K : \mathcal{O}]$. Then there is a polynomial time quantum reduction from*

$$Id(\mathcal{O}) - SIVP_{\gamma'} \longrightarrow \mathcal{O} - \mathrm{LWE}_{q,\Upsilon_\alpha},$$

where $\gamma' = \omega(\frac{1}{\alpha})$.

In order to prove Theorem 4.1, we need the following lemma.

Lemma 4.4. *Let q be an integer coprime to $m := [\mathcal{O}_K : \mathcal{O}]$. Let $\mathcal{I}$ be an integral $\mathcal{O}$-ideal. Then, there exist $\mathcal{O}$-module isomorphisms,*

$$f : \frac{\mathcal{I}}{q\mathcal{I}} \xrightarrow{\sim} \frac{\mathcal{O}}{q\mathcal{O}} \quad \text{and} \quad g : \frac{\mathcal{O}^\vee}{q\mathcal{O}^\vee} \xrightarrow{\sim} \frac{\mathcal{I}^\vee}{q\mathcal{I}^\vee}$$

Further, if $a \in \mathcal{O}/q\mathcal{O}$ is the image of $z \in \mathcal{I}/q\mathcal{I}$ and $s \in \mathcal{O}^\vee/q\mathcal{O}^\vee$ is the image of $x \in \mathcal{I}^\vee/q\mathcal{I}^\vee$, then

$$z \cdot x = a \cdot s \mod q\mathcal{O}^\vee.$$

Proof. Let $\mathfrak{p}$ be the invertible ideal that contains $\mathcal{I}$ as described in Lemma 2.33. Then, the integer q is coprime to the index $[\mathfrak{p} : \mathcal{I}]$, as $Spec_{\mathbb{Z}}([\mathfrak{p} : \mathcal{I}]) \subseteq Spec_{\mathbb{Z}}(m)$. By Lemma 2.19, this yields the following isomorphisms induced by inclusion,

$$\begin{aligned} f_1 : \frac{\mathcal{I}}{q\mathcal{I}} &\xhookrightarrow{\sim} \frac{\mathfrak{p}}{q\mathfrak{p}} \qquad \text{and} \qquad g_1 : \frac{\mathfrak{p}^\vee}{q\mathfrak{p}^\vee} \xhookrightarrow{\sim} \frac{\mathcal{I}^\vee}{q\mathcal{I}^\vee} \\ z &\mapsto f_1(z) = \tilde{z} \qquad\qquad \tilde{x} \mapsto g_1(\tilde{x}) = x \\ z + q\mathfrak{p} &= \tilde{z} + q\mathfrak{p} \qquad\qquad \tilde{x} + q\mathcal{I}^\vee = x + q\mathcal{I}^\vee \end{aligned}$$

Invertibility of $\mathfrak{p}$ and the Cancellation Lemma (Lemma 2.17), yield a $t \in \mathfrak{p}$ such that multiplication by t^{-1} induces the following isomorphisms:

$$\begin{aligned} f_2 : \frac{\mathfrak{p}}{q\mathfrak{p}} &\xrightarrow{\sim} \frac{\mathcal{O}}{q\mathcal{O}} \qquad \text{and} \qquad g_2 : \frac{\mathcal{O}^\vee}{q\mathcal{O}^\vee} \xrightarrow{\sim} \frac{\mathfrak{p}^\vee}{q\mathfrak{p}^\vee} \\ \tilde{z} \mapsto f_2(\tilde{z}) = t^{-1}\tilde{z} &:= a \qquad\qquad s \mapsto g_2(s) = t^{-1}s := \tilde{x} \\ t^{-1}\tilde{z} + q\mathcal{O} &= a + q\mathcal{O} \qquad\qquad t^{-1}s + q\mathfrak{p}^\vee = \tilde{x} + q\mathfrak{p}^\vee \end{aligned}$$

The above map uses the fact that $\mathfrak{p}^\vee = \mathfrak{p}^{-1}\mathcal{O}^\vee$. See Proposition 2.21$(iv)$. Define $f = f_2 \circ f_1 : \mathcal{I}/q\mathcal{I} \to \mathcal{O}/q\mathcal{O}$ and $g = g_1 \circ g_2 : \mathcal{O}^\vee/q\mathcal{O}^\vee \to \mathcal{I}^\vee/q\mathcal{I}^\vee$. Since all the maps involved are $\mathcal{O}$-module isomorphisms, so are f and g.

Finally, we prove that f and g are compatible, i.e., for all $z \in \mathcal{I}/q\mathcal{I}$ and $x \in \mathcal{I}^\vee/q\mathcal{I}^\vee$, $z \cdot x = a \cdot s \mod q\mathcal{O}^\vee$, whenever $f(z) = a$ and $g(s) = x$. Consider the coset,

$$\begin{aligned} z \cdot x + q\mathcal{O}^\vee &= z \cdot (x + q\mathcal{I}^\vee) + q\mathcal{O}^\vee && \text{as } z \cdot q\mathcal{I}^\vee \subset q\mathcal{I}\mathcal{I}^\vee \subseteq q\mathcal{O}^\vee \\ &= z \cdot (\tilde{x} + q\mathcal{I}^\vee) + q\mathcal{O}^\vee \\ &= z \cdot \tilde{x} + q\mathcal{O}^\vee \\ &= (z + q\mathfrak{p}) \cdot \tilde{x} + q\mathcal{O}^\vee && \text{as } q\mathfrak{p} \cdot \tilde{x} \subset q\mathfrak{p}\mathfrak{p}^\vee \subseteq q\mathcal{O}^\vee \\ &= (\tilde{z} + q\mathfrak{p}) \cdot \tilde{x} + q\mathcal{O}^\vee \\ &= \tilde{z} \cdot \tilde{x} + q\mathcal{O}^\vee \end{aligned}$$

Therefore, $z \cdot x = \tilde{z} \cdot \tilde{x} \bmod q\mathcal{O}^\vee$. According to the notations, $a = f_2(\tilde{z})$ and $s = g_2^{-1}(\tilde{x})$. Using the definitions of f_2 and g_2,

$$\begin{aligned} \tilde{z} \cdot \tilde{x} + q\mathcal{O}^\vee &= t^{-1}(\tilde{z} + q\mathfrak{p}) \cdot t(\tilde{x} + q\mathfrak{p}^\vee) + q\mathcal{O}^\vee \\ &= (a + q\mathcal{O}) \cdot (s + q\mathcal{O}^\vee) + q\mathcal{O}^\vee \\ &= a \cdot s + q\mathcal{O}^\vee, \end{aligned}$$

therefore $a \cdot s = \tilde{z} \cdot \tilde{x} \bmod q\mathcal{O}^\vee$. This concludes the proof. □

Proof of Theorem 4.1. We use Theorem 2.36 to prove these hardness results. We show that in this case the set $\mathcal{S}$, as described in Theorem 2.36, equals the set of all $\mathcal{O}$-ideals for both $\mathcal{O}$-LWE and $\mathcal{O}^\vee$-LWE. The novelty of this generalization is in the fact that we convert BDD samples on non-invertible $\mathcal{O}$-ideals into LWE samples. Previously, as in the proof of [BBPS19, Theorem 3.7 & 3.8], this step used the Cancellation Lemma (Lemma 2.17) which unavoidably required the ideal for the BDD problem (or the dual ideal, which ever is relevant), to be invertible. We overcome this by the following two-step argument. Let $\mathcal{I}$ be a non-invertible $\mathcal{O}$-ideal. Recall that without loss of generality, we may assume that $\mathcal{I} \subset \mathcal{O}$. By Lemma 2.33, there exists an invertible $\mathcal{O}$-ideal $\mathfrak{p}$ such that $\mathcal{I} \subseteq \mathfrak{p} \subseteq \mathcal{O}$ and all the prime divisors of the index $[\mathfrak{p} : \mathcal{I}]$ divide $[\mathcal{O}_K : \mathcal{O}]$. Then, for all moduli q coprime to $[\mathcal{O}_K : \mathcal{O}]$, we obtain the isomophism $\mathcal{I}/q\mathcal{I} \xrightarrow{\sim} \mathcal{O}/q\mathcal{O}$ by composing the maps obtained from Lemma 2.19 & 2.17 for the pairs $\{\mathcal{I}, \mathfrak{p}\}$ and $\{\mathfrak{p}, \mathcal{O}\}$, respectively. An isomorphism $\mathcal{O}^\vee/q\mathcal{O}^\vee \xrightarrow{\sim} \mathcal{L}^\vee/q\mathcal{L}^\vee$ is obtained in a similar manner. Further, Lemma 4.4 shows that these maps are compatible with respect to the condition mentioned in Theorem 2.36.

Now, let $\mathcal{I}$ be an integral $\mathcal{O}$-ideal. Given a BDD sample $y = x + e$ on $\mathcal{I}^\vee$ and a discrete Gaussian sample z from $\mathcal{I}$, we define $(a, b) \in \mathcal{O}/q\mathcal{O} \times K_\mathbb{R}/\mathcal{O}^\vee$ as $a = f(z)$ and $b = u \cdot z \cdot y + e' \bmod \mathcal{O}^\vee$, for a small error e'. The compatibility of the maps f and g implies that the tuple (a, b) is a well-defined $\mathcal{O}$-LWE sample, i.e. $b = u \cdot f(z) \cdot g^{-1}(x) + \tilde{e} \bmod \mathcal{O}^\vee$, for an error $\tilde{e}$ depending on e and e'. Eq. (4.1.1) follows from Theorem 2.36 with $\mathcal{Q} = q\mathcal{O}$ and $u = 1/q$. Eq. (4.1.2) then follows from the equivalence of $\mathcal{O}$-LWE and $\mathcal{O}^\vee$-LWE, Proposition 4.2. □

4.2 Ring-LWE Hardness for Some Non $\mathcal{O}_K$-ideal Lattices

The authors in [LPR10, PRSD17] showed that solving Ring-LWE is at least as hard as solving short vector problems on the set of all ideals of the ring of integers $\mathcal{O}_K$. We extend this result to include lattice problems on lattices that are not necessarily ideals of $\mathcal{O}_K$. Although, in our reduction, we extend the set of lattices to a strict superset of $\mathcal{O}_K$-ideal lattices, a lattice $\mathcal{L}$ that is not an $\mathcal{O}_K$-ideal incurs a cost of an $\mathcal{O}_\mathcal{L}$-dependent factor in the approximation factor γ. We prove our generalized hardness result for Ring-LWE, often denoted as $\mathcal{O}_K$-LWE, by giving a polynomial time reduction from $\mathcal{O}$-LWE to $\mathcal{O}_K$-LWE and pre-composing it with our hardness result, Theorem 4.1, for $\mathcal{O}$-LWE. In our $\mathcal{O}$-LWE to $\mathcal{O}_K$-LWE reduction, the error parameter gets inflated by the conductor $\mathcal{C}_\mathcal{O}$ of $\mathcal{O}$ in $\mathcal{O}_K$, similar to the error inflation in [BBPS19, Cor 5.2].

Fix a modulus q. Let $\mathcal{O}$ be an order such that $(q, [\mathcal{O}_K : \mathcal{O}]) = 1$. Then, $q\mathcal{O}$ is an integral $\mathcal{O}$-ideal coprime to the conductor $\mathcal{C}_\mathcal{O}$, and therefore by Theorem 2.27 admits a unique factorization into a product of prime ideals over $\mathcal{O}$. Let $Spec_\mathcal{O}(q\mathcal{O}) := \{\mathfrak{q}_1, \ldots, \mathfrak{q}_r\}$.

Proposition 4.5. *Let K be a number field and $\mathcal{O} \subset \mathcal{O}_K$, an order. Let q be an integer coprime to $[\mathcal{O}_K : \mathcal{O}]$, let Υ be a distribution over a family of error distribution over $K_\mathbb{R}/q\mathcal{O}^\vee$, and let $t \in \mathcal{C}_\mathcal{O} \setminus \bigcup_i \mathfrak{q}_i\mathcal{C}_\mathcal{O}$. Then there is a polynomial time reduction from $\mathcal{O}$-LWE$_{q,\Upsilon}$ to Ring-LWE$_{q,t\cdot\Upsilon}$.*

Notice that the reduction increases the noise by a factor of t. We remark that the error parameter of the $\mathcal{O}_K$-LWE problem in Theorem 4.6 would be the least when t is the shortest lattice vector in $\mathcal{C}_{\mathcal{O}} \setminus \bigcup_i \mathcal{C}_{\mathcal{O}}\mathfrak{q}_i$. The existence of such a short multiplier can be proven either by using the combinatorial argument from [BBPS19, Lem 2.36] or by sampling according to a Gaussian distribution over the conductor ideal with a wide parameter, as in [RSW18, Thm 3.1], [BBPS19, Prop 4.7]. We would like to clarify that the statements in these previous works require that the ideal we sample t from be invertible. Their proofs, however, hold true for the conductor ideal.

Proof of Prop. 4.5. Define the following maps,

$$f : \frac{\mathcal{O}}{q\mathcal{O}} \to \frac{\mathcal{O}_K}{q\mathcal{O}_K}, \qquad f^\vee : \frac{\mathcal{O}^\vee}{q\mathcal{O}^\vee} \xrightarrow{\cdot t} \frac{\mathcal{O}_K^\vee}{q\mathcal{O}_K^\vee}$$

The first map f is induced by the inclusion $\mathcal{O} \subset \mathcal{O}_K$ and is an isomorphism under the assumption that q is coprime to $[\mathcal{O}_K : \mathcal{O}]$ (Lemma 2.19). The second map $f^\vee$ is induced by multiplication by t. It is an isomorphism for $\mathcal{I} = \mathcal{C}_{\mathcal{O}}$, $\mathcal{J} = q\mathcal{O}$ and $\mathcal{M} = \mathcal{O}^\vee$ as $t\mathcal{M} + \mathcal{I}\mathcal{J}\mathcal{M} = \mathcal{I}\mathcal{M}$. See Remark 2.18. Both maps can be efficiently computed. We further extend the second map to $K_{\mathbb{R}}$, $\overline{f^\vee} : K_{\mathbb{R}}/\mathcal{O}^\vee \longrightarrow K_{\mathbb{R}}/\mathcal{O}_K^\vee$ as $\overline{f^\vee}(\frac{1}{q} \cdot x) = \frac{1}{q} \cdot t \cdot x$, for any $x \in K_{\mathbb{R}}/q\mathcal{O}^\vee$. With these maps, define the following transformation

$$\begin{array}{rcl} \frac{\mathcal{O}}{q\mathcal{O}} \times \frac{K_{\mathbb{R}}}{\mathcal{O}^\vee} & \longrightarrow & \frac{\mathcal{O}_K}{q\mathcal{O}_K} \times \frac{K_{\mathbb{R}}}{\mathcal{O}_K^\vee} \\ (a, b) & \mapsto & (a' = f(a),\ b' = \overline{f^\vee}(b) := t \cdot b \mod \mathcal{O}_K^\vee) \end{array}$$

Since the maps, f and $\overline{f^\vee}$ are isomorphisms, this transformation maps uniform samples to uniform samples. Further, if $b = \frac{1}{q} \cdot a \cdot s + e \mod \mathcal{O}^\vee$ is sampled from the $\mathcal{O}$-LWE distribution $\mathcal{O}_{s,\varphi}$, where s is uniform in $\mathcal{O}^\vee/q\mathcal{O}^\vee$ and $e \leftarrow \varphi$, for $\varphi \leftarrow \Upsilon$, then,

$$\begin{aligned} b' &= \frac{1}{q} \cdot f^\vee(a \cdot s) + \overline{f^\vee}(e) \mod \mathcal{O}_K^\vee \\ &= \frac{1}{q} \cdot a \cdot f^\vee(s) + \overline{f^\vee}(e) \mod \mathcal{O}_K^\vee \\ &= \frac{1}{q} \cdot f(a) \cdot f^\vee(s) + \overline{f^\vee}(e) \mod \mathcal{O}_K^\vee \end{aligned}$$

The second equality follows from the fact that $f^\vee$ is an $\mathcal{O}$-module homomorphism. The third equality follows from the fact the following cosets are equal; $a \cdot f^\vee(s) + q\mathcal{O}_K^\vee = (a + q\mathcal{O}_K) \cdot f^\vee(s) + q\mathcal{O}_K^\vee = f(a) \cdot f^\vee(s) + q\mathcal{O}_K^\vee$. Finally, as $e \leftarrow \varphi$, its image $\overline{f^\vee}(e) \leftarrow t \cdot \varphi$. This yields an efficient transformation from $\mathcal{O}$-LWE$_{(q\mathcal{O},1/q),\Upsilon}$ to Ring-LWE$_{q,t\cdot\Upsilon}$. □

Pre-composing this reduction (Proposition 4.5) by the $\mathcal{O}$-LWE hardness result, Theorem 4.1 yields the following improved hardness result for $\mathcal{O}_K$-LWE.

Theorem 4.6. *Let K be a number field of degree n and $\mathcal{O} \subset \mathcal{O}_K$, an order. Let q be an integer coprime to $[\mathcal{O}_K : \mathcal{O}]$. Let $Id(\mathcal{O})$ denote the set of $\mathcal{O}$-ideals. Choose $t \in \mathcal{C}_{\mathcal{O}} \setminus \bigcup_i \mathcal{C}_{\mathcal{O}}\mathfrak{q}_i$ and choose $\alpha \in (0, 1)$ such that $\alpha q \geq 2\omega(1)$. Then there is a polynomial time quantum reduction from*

$$Id(\mathcal{O}) - DGS_\gamma \longrightarrow \mathcal{O}_K - \text{LWE}_{q,t\cdot\Upsilon_\alpha},$$

where

$$\gamma = max\left\{\eta(\mathcal{L}) \cdot \sqrt{2} \cdot /\alpha \cdot \omega(1), \frac{\sqrt{2n}}{\lambda_1(\mathcal{L}^\vee)}\right\}.$$

Comparison with previous work. We note that [BBPS19, Thm 3.8, Cor 5.2] also showed a connection between Order-LWE and Ring-LWE. While the error and the approximation factors obtained from the two reductions are comparable, the results are complementary in terms of other parameters. Further, the prior requires a set of field elements that generate $\mathcal{O}^\vee$ over $\mathcal{O}_K^\vee$ to map between the order and the ring of integers, which is similar to the role of our t. Our result poses a significant improvement in the size of the set of lattices and the set of relevant moduli, since it considers solving lattice problems on the set of all $\mathcal{O}$-ideals, whereas the prior result considers solving lattice problems on the set of $\mathcal{O}$-ideals whose duals are invertible. Our theorem also expands the choice of the moduli for the Ring-LWE problem: the previous result only holds under the assumption that the modulus q be a factor of $[\mathcal{O}_K : \mathcal{O}]$, reducing the choice for q to a finite set, whereas, Theorem 4.6 assumes that q is coprime to $[\mathcal{O}_K : \mathcal{O}]$, tapping an infinite set of choices and also complementing the previous result by bridging the gap.

Solving DGS on p-ary lattices. We view Theorem 4.6 in a different light. Instead of solving DGS on $\mathcal{O}$-ideals where $\mathcal{O}$ varies over the set of orders of indices coprime to a fixed modulus q, we use the $\mathcal{O}_K$-LWE oracle to solve DGS on the set of (embeddings of) all p-ary lattices. This would in turn solve DGS on integer p-ary lattices up to an approximation factor related to the field (of embedding) K. See Section 3 for more details. The image $\mathcal{L}$ of a p-ary lattice L when embedded in a monogenic number field satisfies $p\mathcal{O}_K \subseteq \mathcal{L}$, thereby making $\mathcal{L}$ an ideal of the order $\mathbb{Z} + p\mathcal{O}_K$. See Lemma 3.7. However, this order may be strictly contained in the ring of multiplier $\mathcal{O}_\mathcal{L}$ of $\mathcal{L}$.

Corollary 4.7. *Let K be a monogenic number field. Let $\mathcal{L} \subset K$ be a lattice such that $p\mathcal{O}_K \subseteq \mathcal{L}$, for a fixed prime p. Choose an integer q, coprime to p, and an $\alpha \in (0, 1)$ such that $\alpha q \geq 2\omega(1)$. For $t \in \mathcal{C}_{\mathcal{O}_\mathcal{L}} \setminus \bigcup_i \mathfrak{q}_i\mathcal{C}_{\mathcal{O}_\mathcal{L}}$, there is a polynomial time quantum reduction*

$$\mathcal{L}\text{-DGS}_{\widetilde{\gamma}} \longrightarrow \mathcal{O}_K\text{-LWE}_{q,\Upsilon_\alpha}, \text{ where } \widetilde{\gamma} = max\left\{\eta(\mathcal{L}) \cdot \sqrt{2} \cdot \|t\|_\infty/\alpha \cdot \omega(1), \frac{\sqrt{2n}}{\lambda_1(\mathcal{L}^\vee)}\right\}$$

Proof. The result follows from Theorem 4.6 with the order $\mathcal{O} = \mathcal{O}_\mathcal{L}$, as the index $[\mathcal{O}_K : \mathcal{O}_\mathcal{L}] \mid [\mathcal{O}_K : p\mathcal{O}_K]$ and therefore is a power of p, coprime to q. □

Observe that for the integer p-ary lattice $\mathcal{L}$, the approximation factor γ obtained above only makes sense as long as $\|t\|_\infty < p$. This may be achievable if $\mathcal{C}_{\mathcal{O}_\mathcal{L}}$ is a proper factor of $p\mathcal{O}_K$. However, the DGS problem on $\mathcal{L}$ can also be solved using either an $\mathcal{O}_\mathcal{L}$-LWE oracle or a $\mathbb{Z}+p\mathcal{O}_K$-LWE oracle. The approximation factor from both of these reductions is equal to γ, as in the hardness result, Theorem 4.1, which is an improvement by $\|t\|_\infty$ from the approximation factor in the Corollary 4.7.

5 Gradients of hardness between Ring-LWE and LWE

In this section, we describe chains of Order-LWE problems that begin with the well-known Ring-LWE (often denoted as $\mathcal{O}_K$-LWE) and increase in hardness until they reach an Order-LWE problem

that is equivalent to the unstructured LWE problem. The descending chain of orders (w.r.t inclusion) creates a gradient of increasing hardness from Ring-LWE to LWE. Its relevance is two-fold; it describes a collection of orders in K such that their corresponding (Order-)LWE problems lie between Ring-LWE and LWE, the former being the most efficient and the latter, hardest and least efficient. Secondly, it instantiates the LWE problem in an algebraic avatar, as an Order-LWE problem.

To ease notation, we denote by $\mathcal{O}$-LWE$_{q,\psi}$, the Order-LWE problem for the order $\mathcal{O}$, with modulus ideal $q\mathcal{O}$, the element $u = 1/q$ and an error distribution ψ over $K_{\mathbb{R}}$. The following result is a building block in creating the chains. It gives an error preserving reduction between Order-LWE problems, as long as the index of the two orders is coprime to the LWE modulus.

Theorem 5.1 ([PP19, Theorem 4.3])**.** *Given $\mathcal{O} \subseteq \mathcal{O}'$ and a positive integer q coprime to the index $[\mathcal{O}' : \mathcal{O}]$, there is an efficient, deterministic and error preserving reduction from $\mathcal{O}'$-LWE$_{q,\psi}$ to $\mathcal{O}$-LWE$_{q,\psi}$. In particular, if $\mathcal{O}'$ is the maximal order, $\mathcal{O}_K$, then we have an efficient, deterministic and error preserving reduction from $\mathcal{O}_K$-LWE$_{q,\psi}$ to $\mathcal{O}$-LWE$_{q,\psi}$.*

With repetitive application of Theorem 5.1, we get a chain of algebraic LWEs as follows. Let $\mathcal{L} \subset \mathcal{O}_K$ be a lattice in K. Then, $\mathcal{L}$ is an ideal of the order $\mathbb{Z} + m\mathcal{O}_K$, where m is the exponent of the quotient group $\mathcal{O}_K/\mathcal{L}$. See Lemma 3.7. The order $\mathbb{Z} + m\mathcal{O}_K$ may be strictly contained in the ring of multipliers, $\mathcal{O}_{\mathcal{L}}$. Hence, the inclusion, $\mathbb{Z} + m\mathcal{O}_K \subseteq \mathcal{O}_{\mathcal{L}} \subseteq \mathcal{O}_K$, by Theorem 5.1, implies the error preserving reduction

$$\mathcal{O}_K\text{-LWE}_{q,\psi} \longrightarrow \mathcal{O}_{\mathcal{L}}\text{-LWE}_{q,\psi} \longrightarrow (\mathbb{Z} + m\mathcal{O}_K)\text{-LWE}_{q,\psi}$$

as long as q is coprime to m. Coprimality of q with m is sufficient as both the indices, $[\mathcal{O}_{\mathcal{L}} : (\mathbb{Z} + m\mathcal{O}_K)]$ and $[\mathcal{O}_K : \mathcal{O}_{\mathcal{L}}]$ divide $[\mathcal{O}_K : m\mathcal{O}_K] = m^n$, owing to the fact that $m\mathcal{O}_K \subset \mathbb{Z} + m\mathcal{O}_K$. This chain of LWE problems, increasing in hardness, may be longer depending on the factorization of $m\mathcal{O}_K$ as an $\mathcal{O}_K$-ideal, as we describe in Theorem 5.2.

Let $Spec_{\mathcal{O}_K}(m\mathcal{O}_K) = \{\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_r\}$. Define $\mathcal{O}_i := \mathbb{Z} + \mathfrak{m}_1 \cdot \ldots \cdot \mathfrak{m}_i$. Then, by Lemma 3.6, each $\mathcal{O}_i$ is an order in K. Further, $\mathcal{O}_i \subset \mathcal{O}_j$, for $i \geq j$, and $\mathbb{Z} + m\mathcal{O}_K \subset \mathcal{O}_i$, for all i. By the same argument, for any lattice, $\mathcal{J} \subseteq \mathcal{O}_K$, the order $\mathbb{Z} + m\mathcal{J} \subseteq \mathbb{Z} + m\mathcal{O}_K$. This yields the following chain of orders: $\mathcal{O}_K \supseteq \mathcal{O}_1 \supseteq \cdots \supseteq \mathcal{O}_r \supseteq \mathbb{Z} + m\mathcal{O}_K \supseteq \mathbb{Z} + m\mathcal{J}$.

Theorem 5.2. *Let m and q be coprime integers, and let $\mathcal{J}$ be a lattice in $\mathcal{O}_K$ such that $([\mathcal{O}_K : \mathcal{J}], q) = 1$. Then, we have the following efficient, deterministic and error preserving reductions*

$$\mathcal{O}_K - \text{LWE}_{q,\psi} \to \cdots \to \mathcal{O}_r - \text{LWE}_{q,\psi} \to \mathbb{Z} + m\mathcal{O}_K - \text{LWE}_{q,\psi} \to \mathbb{Z} + m\mathcal{J} - \text{LWE}_{q,\psi}.$$

Proof. Each reduction follows from Theorem 5.1 under the observation that the indices $[\mathcal{O}_K : \mathcal{O}_i] \mid [\mathcal{O}_K : m\mathcal{O}_K] = m^n$, and $[\mathbb{Z} + m\mathcal{O}_K : \mathbb{Z} + m\mathcal{J}]$ are coprime to q. The last index $[\mathbb{Z} + m\mathcal{O}_K : \mathbb{Z} + m\mathcal{J}]$ is a factor of $m \cdot [\mathcal{O}_K : \mathcal{J}]$, as it is equal to

$$\left| \frac{(\mathbb{Z} + m\mathcal{O}_K)/m\mathcal{J}}{(\mathbb{Z} + m\mathcal{J})/m\mathcal{J}} \right| = \frac{|(\mathbb{Z} + m\mathcal{O}_K)/m\mathcal{O}_K| \cdot |m\mathcal{O}_K/m\mathcal{J}|}{|(\mathbb{Z} + m\mathcal{J})/m\mathcal{J}|} = \frac{|\mathbb{Z}/m\mathbb{Z}| \cdot |\mathcal{O}_K/\mathcal{J}|}{|\mathbb{Z}/\ (\mathbb{Z} \cap m\mathcal{J})|}$$

□

We now describe (non-maximal) orders such that the corresponding Order-LWE problems, with error sampled from a spherical Gaussian, become equivalent to the unstructured LWE problem.

Suppose $\mathcal{O} \subseteq K$ be such an order. Since an elliptical Gaussian from, say, Υ_α is wider than D_α, the $\mathcal{O}$-LWE$_{q,\Upsilon_\alpha}$ problem is also equivalent to LWE. In unison with Theorem 5.2, this result yields various chains of algebraic LWEs in the field K that begin with Ring-LWE and terminate at LWE.

The $\mathbb{Z}$-bases of these special orders satisfy a particular property that we describe now. Some notation; let $\mathcal{O}$ be an order of K. Fix $\vec{p} = \{p_0 = 1, p_1, \ldots, p_{n-1}\}$ as a $\mathbb{Z}$-basis of $\mathcal{O}$. See Lemma 2.13 for the existence of $\vec{p}$. Denote by $\vec{p^\vee} = \{p_i^\vee\}_{i=0}^{n-1}$, the $\mathbb{Z}$-basis of $\mathcal{O}^\vee$ that satisfies $Tr(p_i p_j^\vee) = \delta_{ij}$, where $Tr = Tr_{K_\mathbb{R}/\mathbb{R}}$.

Definition 5.3. *Let K be a number field and $e \in K_\mathbb{R}$ be sampled from the distribution D_α over $K_\mathbb{R}$, for some $\alpha > 0$. We say that an order $\mathcal{O}$ in K is α-drowning if there exists a $\mathbb{Z}$-basis $\vec{p}$ of $\mathcal{O}$, as described above, such that the coefficients $(e_0, e_1, \ldots, e_{n-1})$ of e with respect to the $\mathbb{Z}$-basis $\vec{p^\vee}$ of $\mathcal{O}^\vee$ satisfy the following: the marginal distribution of $e_0 \mod \mathbb{Z}$ is*

$$e_0 \mod \mathbb{Z} \leftarrow D_{\alpha\sqrt{n}} \mod \mathbb{Z}$$

and, for any $x_0 \in \mathbb{R}$, the conditional distribution,

$$(e_1, e_2, \ldots, e_{n-1}) \,|e_0 = x_0 \mod \mathbb{Z}^{n-1} \approx_{s.i} U((\mathbb{R}/\mathbb{Z})^{n-1})$$

where $\approx_{s.i}$ means that the two distributions are statistically indistinguishable.

Theorem 5.4. *Let K be a number field of degree n and let $\mathcal{O}$ be an α-drowning order, for $\alpha \cdot q \geq 2 \cdot \omega(1)$. Then, the $\mathcal{O}$-LWE$_{q,D_\alpha}$ problem is equivalent to the LWE$_{q,D_{\alpha\cdot\sqrt{n}}}$ problem.*

Proof. We first give a reduction from LWE to $\mathcal{O}$-LWE. This is the non-trivial part of the proof. As is standard, for this reduction, we define a transformation that sends uniform samples over $(\mathbb{Z}/q\mathbb{Z})^n \times \mathbb{R}/\mathbb{Z}$ to uniform samples over $\mathcal{O}/q\mathcal{O} \times K_\mathbb{R}/\mathcal{O}^\vee$ and LWE samples to $\mathcal{O}$-LWE samples.

Let $Tr = Tr_{K_\mathbb{R}/\mathbb{R}}$ denote the trace map. For $i \in [n-1]$, sample uniform elements in $\mathbb{R}/\mathbb{Z}$; $u_i \leftarrow U(\mathbb{R}/\mathbb{Z})$. We define the transformation as follows: given a pair $(\vec{a}, b_0) \in (\mathbb{Z}/q\mathbb{Z})^n \times \mathbb{R}/\mathbb{Z}$, output

$$(a := a_1 p_0 + \ldots + a_n p_{n-1},\ \ b := b_0\, p_0^\vee + u_1\, p_1^\vee + \ldots + u_{n-1}\, p_{n-1}^\vee) \in \mathcal{O}/q\mathcal{O} \times K_\mathbb{R}/\mathcal{O}^\vee$$

It is straightforward to see that this transformation is well-defined and maps uniform samples from the domain to uniform samples in the range. We claim that if $b_0 = \frac{1}{q} \cdot \langle \vec{a}, \vec{s} \rangle + e$, with a secret $\vec{s} \leftarrow U((\mathbb{Z}/q\mathbb{Z})^n)$ and an error $e \leftarrow D_{\alpha\sqrt{n}}$, then $b \in K_\mathbb{R}/\mathcal{O}^\vee$, as defined above, is statistically indistinguishable from $b' := \frac{1}{q} \cdot a \cdot s + e' \in K_\mathbb{R}/\mathcal{O}^\vee$, where $s := \langle \vec{s}, \vec{p^\vee} \rangle = s_1 p_0^\vee + \ldots + s_n p_{n-1}^\vee \in \mathcal{O}^\vee/q\mathcal{O}^\vee$ and $e' \leftarrow D_\alpha$ over $K_\mathbb{R}$. In fact, we show that the coefficients of b are statistically indistinguishable from the coefficients of b' in the basis $\{p_i^\vee\}_i$ of $\mathcal{O}^\vee$. Notice that (a, b') is an $\mathcal{O}$-LWE$_{q,D_\alpha}$ sample with the uniformly sampled secret s, since $\vec{s} \leftarrow U((\mathbb{Z}/q\mathbb{Z})^n)$.

The linearity of the Trace map along with the equality, $Tr(p_i p_j^\vee) = \delta_{ij}$, implies that $a \cdot s = \sum_{i=0}^{n-1} Tr(a \cdot s \cdot p_i)\, p_i^\vee$, and $Tr(a \cdot s) = \sum_{i=1}^{n} a_i s_i = \langle \vec{a}, \vec{s} \rangle$. Therefore,

$$b = \frac{1}{q} \cdot \langle \vec{a}, \vec{s} \rangle\, p_0^\vee + e\, p_0^\vee + \sum_{i=1}^{n-1} u_i p_i^\vee = \left(\frac{1}{q} \cdot Tr(a \cdot s) + e \right) \cdot\ p_0^\vee + \sum_{i=1}^{n-1} u_i p_i^\vee \mod \widetilde{\mathcal{O}}^\vee,$$

whereas

$$b' = \left(\frac{1}{q} \cdot Tr(a \cdot s) + e'_0 \right) \cdot\ p_0^\vee + \sum_{i=1}^{n-1} \left(\frac{1}{q} \cdot Tr(a \cdot s \cdot p_i) + e'_i \right) \cdot p_i^\vee \mod \mathcal{O}^\vee.$$

Here, $e' = \sum_{i=0}^{n-1} e'_i \, p_i^\vee$ is the representation of the error (from the $\mathcal{O}$-LWE sample) in the $\mathbb{Z}$-basis of $\mathcal{O}^\vee$. Since $\mathcal{O}$ is α-drowning, the marginal distribution of $e_0 \mod \mathbb{Z}$ is $D_{\alpha\sqrt{n}} \mod \mathbb{Z}$, whereas the conditional distribution of $(e'_1, \ldots, e'_{n-1})|e'_0$ equals $x_0 \mod \mathbb{Z}^{n-1}$ is statistically indistinguishable from $U((\mathbb{R}/\mathbb{Z})^{n-1})$, for any $x_0 \in \mathbb{R}$. This shows that $(e'_0, e'_1, \ldots, e'_{n-1}) \mod \mathbb{Z}^n$ is statistically indistinguishable from $(e, u_1, \ldots, u_{n-1}) \mod \mathbb{Z}^n \leftarrow D_{\alpha\sqrt{n}} \mod \mathbb{Z} \times U((\mathbb{R}/\mathbb{Z})^{n-1})$. Therefore, the coefficients of b and of b' with respect to the $\mathbb{Z}$-basis of $\mathcal{O}^\vee$ are statistically indistinguishable, as desired.
The converse, from $\mathcal{O}$-LWE to LWE, is a special case of [PP19, Thm 6.1]. □

Examples of α-drowning orders. We describe two orders that are α-drowning, for an $\alpha > 0$ satisfying $\alpha \cdot q > 2 \cdot \omega(1)$.

(*i*) For a number field K, let $\{1, \theta_1, \ldots, \theta_{n-1}\}$ be a fixed $\mathbb{Z}$-basis for $\mathcal{O}_K$. See Lemma 2.13 for its existence. For a $d \times d$ matrix M, let $e_d(M)$ denote the smallest eigenvalue of M. Let $\tau := e_{n-1}(T)$, where $T = (Tr(\theta_i\overline{\theta_j}) - \frac{1}{n} \cdot Tr(\theta_i)Tr(\theta_j))_{1 \le i,j \le n-1}$. Choose $r \in \mathbb{N}$ such that $\tau \cdot m^{2r-2} \ge n$. Let $\widetilde{\mathcal{O}} := \mathbb{Z} + m^r\mathcal{O}_K$. Then, a $\mathbb{Z}$-basis for $\widetilde{\mathcal{O}}$ is $\vec{p} := (p_i)_{i=0}^{n-1} = \{1, m^r\theta_1, \ldots, m^r\theta_{n-1}\}$. Let $\vec{p^\vee} = (p_0^\vee, p_1^\vee, \ldots, p_{n-1}^\vee)$ be the (dual) $\mathbb{Z}$-basis for $\widetilde{\mathcal{O}}^\vee$. Then, for $\alpha > 0$ satisfying $\alpha \cdot q \ge 2\omega(1)$, the order $\widetilde{\mathcal{O}}$ is α-drowning. When $\mathcal{O}_K$ has an orthogonal $\mathbb{Z}$-basis containing 1, then the matrix T is a diagonal matrix with $\tau = e_{n-1}(T) \ge \sqrt{n}$. Therefore, the condition $\tau \cdot m^{2r-2} \ge n$ is achieved with $r = 1$. See Remark 2.16.

(*ii*) In fields that are closed under complex conjugation, i.e. $\overline{K} \subseteq K$, one may be able to choose a smaller order $\widetilde{\mathcal{O}'}$ that is α-drowning. Note that all Galois fields and totally real number fields are closed under complex conjugation. As $\overline{K} \subseteq K$, the trace map, $Tr_{K_\mathbb{R}/\mathbb{R}}|_K$, when restricted to K takes rational values. Therefore, by repeated application of [Cona, Lem. 4.6], $K = \mathbb{Q} \cdot 1 \oplus \mathbb{Q} \cdot \theta'_1 \oplus \ldots \oplus \mathbb{Q} \cdot \theta'_{n-1}$, decomposes orthogonally into $\mathbb{Q}$ vector subspaces, for $\theta'_i \in K$. Consider the $\mathbb{Z}$-module generated by this orthogonal basis and call it $\mathcal{J}$. It is a full-rank lattice and hence an ideal in its ring of multipliers. We multiply by a scalar to make sure that $\mathcal{J}$ is an integral ideal. Then, by Lemma 3.6, the set $\widetilde{\mathcal{O}'} := \mathbb{Z} + m\mathcal{J}$ is an order, generated by $\vec{p'} = (p'_i)_{i=0}^{n-1} := \{1, m\theta'_1, \ldots, m\theta'_{n-1}\}$ over $\mathbb{Z}$. Let $\vec{p'}^\vee = \{p_i'^\vee\}_{i=0}^{n-1}$ be the corresponding $\mathbb{Z}$-basis for $\widetilde{\mathcal{O}'}^\vee$. Then, $\widetilde{\mathcal{O}'}$ is an α-drowning order, for $\alpha > 0$ satisfying $\alpha \cdot q > 2\omega(1)$.

Recall that, when $e \leftarrow D_\alpha$ over $K_\mathbb{R}$, the coefficients $(e_0, e_1, \ldots e_{n-1})$ of e, w.r.t to the $\mathbb{Z}$-basis of the dual of the order in consideration, call it $\mathcal{O}$, follow the Gaussian distribution of covariance matrix $\alpha^2 \cdot P_\mathcal{O}$. (See Lemma 2.39.) To prove that this order is α-drowning, we show that the $n-1 \times n-1$ covariance matrix of the conditional distribution of the coefficients $(e_1, \ldots e_{n-1})$ satisfies that the smallest singular value of its square root exceeds the smoothing parameter of $\mathbb{Z}^{n-1}$. This implies that given any value for e_0, $(e_1, \ldots e_{n-1}) \mod \mathbb{Z}^{n-1}$ is indistinguishable from a uniform element in $(\mathbb{R}/\mathbb{Z})^{n-1}$, by Lemma 2.5. We also show that $e_0 \mod \mathbb{Z} \leftarrow D_{\alpha\sqrt{n}}$.

Proposition 5.5. *Let K be a number field of degree n and m be an integer greater than q. Then, for $\alpha > 0$ satisfying $\alpha \cdot q > 2 \cdot \omega(1)$,*

(i) $\widetilde{\mathcal{O}}$ is an α-drowning order; and

(ii) when $\overline{K} \subseteq K$, the order $\widetilde{\mathcal{O}'}$ is α-drowning.

Proof. For both the cases, let $X_a := e_0$ and $X_b := (e_1, e_2, \ldots, e_{n-1})$. The covariance matrix for the appropriate order $\mathcal{O} = \widetilde{\mathcal{O}}$ or $\widetilde{\mathcal{O}}'$ can be expressed as,

$$\alpha^2 P_{\mathcal{O}} = \alpha^2 \left(Tr(p_i \overline{p_j})\right)_{ij} = \alpha^2 \begin{pmatrix} \Sigma_{aa} & \Sigma_{ab} \\ \Sigma_{ba} & \Sigma_{bb} \end{pmatrix},$$

where $\Sigma_{aa} \in M_{1\times 1}(\mathbb{R})$, $\Sigma_{bb} \in M_{n-1\times n-1}(\mathbb{R})$, and the matrices $\Sigma_{ab} = \Sigma_{ba}^t \in M_{1\times n-1}(\mathbb{R})$. By Proposition 2.3(i), the marginal distribution of X_a is a Gaussian distribution over $\mathbb{R}$ of covariance matrix $\alpha^2 \cdot \Sigma_{aa} = \alpha^2 \cdot Tr(p_0\overline{p_0}) = \alpha^2 \cdot n$. By part (ii) of the same proposition, the conditional distribution of $X_b | X_a = x_0$ is a Gaussian distribution over $\mathbb{R}^{n-1}$ of mean $x_0 \alpha^2 \Sigma_{ba} (\alpha^2 \Sigma_{aa})^{-1} = \frac{x_0}{n} \cdot \Sigma_{ba}$ and of covariance matrix $\alpha^2 \left(\Sigma_{bb} - \Sigma_{ba}\Sigma_{aa}^{-1}\Sigma_{ab}\right)$.

Proof of (i) When $\mathcal{O} = \widetilde{\mathcal{O}}$, the covariance matrix $\alpha^2 \left(\Sigma_{bb} - \Sigma_{ba}\Sigma_{aa}^{-1}\Sigma_{ab}\right) = \alpha^2 \cdot m^{2r} \cdot T$, where T was defined above. As r was chosen such that $\tau \cdot m^{2r-2} \geq n$, for $\tau = e_{n-1}(T)$, the smallest singular value, $s_{n-1}(\sqrt{T})$, of $\sqrt{T}$ equals $\sqrt{\tau}$, and

$$\alpha \cdot m^r \cdot s_{n-1}(\sqrt{T}) \geq \alpha \cdot m^r \cdot \sqrt{\tau} \geq \alpha \cdot m \cdot \sqrt{n} \geq \omega(1) \cdot \sqrt{n} > \eta(\mathbb{Z}^{n-1}).$$

The last inequality follows from the fact that $\eta(\mathbb{Z}^{n-1}) < \sqrt{n}$, for $\varepsilon = (e^{\pi n}/(2n-2) - 1)^{-1}$. See Lemma 2.6. Thus, since $\alpha^2 \cdot m^{2r} \cdot T \geq \alpha^2 \cdot m^{2r} \cdot s_{n-1}(\sqrt{T})^2$, by Lemma 2.5, the distribution of $X_b | X_a = x_0 \bmod \mathbb{Z}^{n-1}$ is ε-close to the uniform distribution $U((\mathbb{R}/\mathbb{Z})^{n-1})$. This proves the result.

Proof of (ii) When $\mathcal{O} = \widetilde{\mathcal{O}}'$, the $\mathbb{Z}$-basis $\vec{p'}$ is orthogonal. Therefore, the covariance matrix

$$\alpha^2 \left(\Sigma_{bb} - \Sigma_{ba}\Sigma_{aa}^{-1}\Sigma_{ab}\right) = \alpha^2 \cdot diag(m^2\|\theta'_1\|^2, \ldots, m^2\|\theta'_{n-1}\|^2)$$

Now, for $1 \leq i \leq n-1$, each e_i is an independent variable drawn from $D_{\sqrt{\alpha_i}}$, with $\alpha_i = m^2\|\theta'_i\|^2$. As $\theta'_i \in \mathcal{O}_K$, by Remark 2.16, $\|\theta'_i\| \geq \sqrt{n}$. Hence,

$$e_i \mod \mathbb{Z} \leftarrow D_{\sqrt{\alpha_i}} \mod \mathbb{Z} \quad \text{for } \sqrt{\alpha_i} \geq \alpha \cdot m \cdot \sqrt{n}.$$

Under the assumption on α and the fact that $m \geq q$, for $i > 0$, the parameter $\sqrt{\alpha_i} > \eta(\mathbb{Z})$. The last inequality follows from the fact that $\eta(\mathbb{Z}) < \sqrt{n}$, for $\varepsilon = (e^{\pi n}/2 - 1)^{-1}$. See Lemma 2.6. Finally, by Lemma 2.5, the distribution $D_{\sqrt{\alpha_i}} \bmod \mathbb{Z}$, for $i > 0$, is statistically ε-close to the uniform distribution $U(\mathbb{R}/\mathbb{Z})$. This proves the result. □

Remark 5.6. *The parameters $m \geq q$ in Theorem 5.4 cannot satisfy $m \gg q$. This is because when $m \gg q$, the error parameter $\alpha > \frac{2\omega(1)}{q} \gg \frac{1}{m}$ is greater than the smoothing parameter of $(\mathbb{Z}+m\mathcal{O}_K)^\vee$, thereby making the second coordinate from the $\mathbb{Z} + m\mathcal{O}_K$-LWE problem, $b \in K_\mathbb{R}/(\mathbb{Z} + m\mathcal{O}_K)^\vee$, indistinguishable from uniform.*

The α-drowning orders from the examples above are particularly easy to describe in the case of the power-of-two cyclotomic extensions.

Corollary 5.7. *Let $K = \mathbb{Q}(\zeta_{2n})$ be a power of two cyclotomic extension. Let m and q be distinct integers, with $m \geq q$. Let $\alpha \in (0, 1)$ be such that $\alpha \cdot q \geq 2 \cdot \omega(1)$. Then, for $\widetilde{\mathcal{O}} := \mathbb{Z} + m\mathcal{O}_K$, the problems $\widetilde{\mathcal{O}}$-LWE$_{q,D_\alpha}$ and LWE$_{q,D_{\alpha\cdot\sqrt{n}}}$ are equivalent.*

Proof. Let $\{\theta_i\}_{i=0}^{n-1} = \{1, \zeta_{2n}, \ldots, \zeta_{2n}^{n-1}\}$ be a power basis of $\mathcal{O}_K$ as a $\mathbb{Z}$-module. Note that this is an orthogonal $\mathbb{Z}$-basis with respect to the Trace map, i.e., $Tr(\theta_i\overline{\theta_j}) = 0$, when $i \neq j$, and $Tr(\theta_i\overline{\theta_i}) = n$. Therefore, the matrix $T = (Tr(\theta_i\overline{\theta_j}) - \frac{1}{n} \cdot Tr(\theta_i)Tr(\theta_j))_{1 \leq i,j \leq n-1}$ is the diagonal matrix $n \cdot Id_{n-1 \times n-1}$, and the smallest eigenvalue value $\tau := e_{n-1}(T)$ equals n. This implies that we may choose $r = 1$, for then $\tau \cdot m^{2r-2} \geq n$. Then, by either of the proofs of (i) or (ii) in Proposition 5.5, we have $\widetilde{\mathcal{O}}$ is α-drowning. The conclusion follows by applying Theorem 5.4.

□

6 Analyzing lattice problems on unstructured integer lattices with algebraic tools

In this section, we embed a p-ary lattice L into a monogenic number field $K = \mathbb{Q}(\theta)$, and give an algorithm that describes the conductor of the ring of multipliers $\mathcal{O}_{\mathcal{L}}$ of $\mathcal{L}$, the image of L in K, under the coefficient embedding. Recall that the image $\mathcal{L}$ of a p-ary lattice L when embedded in a monogenic number field satisfies $[\mathcal{O}_K : \mathcal{L}] = \det(L) = p^k$, for some $k \in \mathbb{N}$. (Remark 3.2). The algorithm, however, in its present form, generalizes to non-monogenic fields K as long as the modulus p is coprime to the index $n_\theta := [\mathcal{O}_K : \mathbb{Z}[\theta]]$. In this case, the algorithm outputs the prime decomposition of the conductor $\mathcal{C}_\theta$ as a $\mathbb{Z}[\theta]$-ideal. Notice that since $\mathcal{C}_\theta$ is an invertible $\mathbb{Z}[\theta]$-ideal, as guaranteed by the condition $(p, n_\theta) = 1$, (Lemma 3.9), this prime decomposition yields a prime decomposition of $\mathcal{C}_\theta\mathcal{O}_K$, by just inflating the respective prime ideals. See Theorem 2.27. Finally, the conductor $\mathcal{C}_{\mathcal{L}}$ of $\mathcal{O}_{\mathcal{L}}$ in $\mathcal{O}_K$ is sandwiched between the following $\mathcal{O}_K$-ideals, $\mathcal{C}_\theta \cdot n_\theta\mathcal{O}_K \subseteq \mathcal{C}_{\mathcal{L}} \subseteq \mathcal{C}_\theta\mathcal{O}_K$, which reveals information about the prime decomposition of $\mathcal{C}_{\mathcal{L}}$ as an $\mathcal{O}_K$-ideal.

6.1 Algorithm for computing the conductor $\mathcal{C}_{\mathcal{L}}$

We keep the running notation. Let $\mathcal{L}$ be a lattice in a monogenic field K such that $p\mathcal{O}_K \subseteq \mathcal{L} \subseteq \mathcal{O}_K$ and $[\mathcal{O}_K : \mathcal{L}] = p^k$, for an integer $1 \leq k \leq n$. Let $\mathcal{O}_{\mathcal{L}}$ denote its ring of multipliers. Then, by Lemma 2.26 and Proposition 2.24, we have the following equality,

$$\mathcal{C}_{\mathcal{L}} \cdot \mathcal{O}_{\mathcal{L}}^\vee = \mathcal{C}_{\mathcal{L}} \cdot \mathcal{L} \cdot \mathcal{L}^\vee = \mathcal{O}_K^\vee = \frac{1}{f'(\theta)} \cdot \mathcal{O}_K$$

The equality, for $\mathcal{O}_K^\vee$, uses Proposition 2.22. Let $p\mathcal{O}_K = \prod_i \mathfrak{p}_i$ be the prime factorization of the $\mathcal{O}_K$-ideal. As $p\mathcal{O}_K \subseteq \mathcal{C}_{\mathcal{L}} \subseteq \mathcal{O}_{\mathcal{L}}$, and $\mathcal{C}_{\mathcal{L}}$ is the largest $\mathcal{O}_K$ ideal in $\mathcal{O}_{\mathcal{L}}$, the conductor $\mathcal{C}_{\mathcal{L}} \mid p\mathcal{O}_K$ and the above equality yields,

$$p \cdot f'(\theta) \cdot \mathcal{L}\mathcal{O}_K \cdot \mathcal{L}^\vee\mathcal{O}_K = \frac{p\mathcal{O}_K}{\mathcal{C}_{\mathcal{L}}} \tag{6.1.1}$$

Both $\mathcal{L}\mathcal{O}_K$ and $p \cdot f'(\theta) \cdot \mathcal{L}^\vee\mathcal{O}_K$ are integral $\mathcal{O}_K$-ideals, as proven in the following lemma:

Lemma 6.1. *Both $\mathcal{L}\mathcal{O}_K$ and $p \cdot f'(\theta) \cdot \mathcal{L}^\vee\mathcal{O}_K$ are integral $\mathcal{O}_K$-ideals that divide $p\mathcal{O}_K$.*

Proof. The fact that $p\mathcal{O}_K \subset \mathcal{L} \subseteq \mathcal{O}_K$ implies that the inflation $\mathcal{L}\mathcal{O}_K$ is an integral $\mathcal{O}_K$-ideal that divides $p\mathcal{O}_K$. Further, dualizing $p\mathcal{O}_K \subseteq \mathcal{L} \subseteq \mathcal{O}_K$ implies that

$$\frac{1}{f'(\theta)}\mathcal{O}_K = \mathcal{O}_K^\vee \subseteq \mathcal{L}^\vee \subseteq (p\mathcal{O}_K)^\vee = \frac{1}{p}\mathcal{O}_K^\vee = \frac{1}{p} \cdot \frac{1}{f'(\theta)}\mathcal{O}_K.$$

Multiplying this chain by $p \cdot f'(\theta) \cdot \mathcal{O}_K$, yields that $p\mathcal{O}_K \subseteq p \cdot f'(\theta) \cdot \mathcal{L}^\vee\mathcal{O}_K \subseteq \mathcal{O}_K$, as desired. □

Then, Equation (6.1.1) implies that

$$\mathcal{C}_{\mathcal{L}} = \prod_{\mathfrak{p}_i \notin S} \mathfrak{p}_i, \qquad \text{where} \quad S := Spec_{\mathcal{O}_K}\{p \cdot f'(\theta) \cdot \mathcal{L}\mathcal{O}_K \cdot \mathcal{L}^\vee \mathcal{O}_K\}.$$

In order to find the prime decomposition of the integral $\mathcal{O}_K$-ideals, we first find their generators, as $\mathcal{O}_K$-modules. It is well-known that an $\mathcal{O}_K$-ideal is generated by at most 2 elements, as an $\mathcal{O}_K$-module. See [Coh96, Prop 4.7.7]. As the ideals of interest for us both contain $p\mathcal{O}_K$, the element p may be one of the generators. The following result describes what the other generator should be.

Proposition 6.2. *(Adaptation of [Neu99, Prop 8.3]) Let K be a monogenic number field generated by the root θ of a monic irreducible polynomial f. Let $\mathcal{I}$ be an integral $\mathcal{O}_K$-ideal such that $p\mathcal{O}_K \subseteq \mathcal{I}$. Suppose $\mathcal{I} = p\mathcal{O}_K + \sum_{i=1}^{r} T_i(\theta) \cdot \mathcal{O}_K$, for some polynomials $T_i(x) \in \mathbb{F}_p[x]$. Then $\mathcal{I} = p\mathcal{O}_K + h_{\mathcal{I}}(\theta) \cdot \mathcal{O}_K$, where $h_{\mathcal{I}} = gcd(T_1(x), T_2(x), \ldots, T_r(x), f(x))$ in $\mathbb{F}_p[x]$.*

Proof. The image of $\mathcal{I}$ under the following surjective ring homomorphism

$$\mathcal{O}_K \twoheadrightarrow \mathcal{O}_K/p\mathcal{O}_K \simeq \mathbb{F}_p[x]/\langle f(x)\rangle.$$

is an ideal in $\mathbb{F}_p[x]/\langle f(x)\rangle$ generated by $\langle\{\overline{T_i(x)}\}_{i=1}^r\rangle$, where $\overline{T_i(x)} := T_i(x) \mod f(x)$. In the ring $\mathbb{F}_p[x]$, this ideal is generated by $\langle\{T_i(x)\}_{i=1}^r, f(x)\rangle$. Since $\mathbb{F}_p[x]$ is a principal ideal domain (PID), it follows that this ideal is generated by the single element, the gcd $h_{\mathcal{I}}(x)$ of $\{T_i(x)\}_{i=1}^r$ and $f(x)$. Taking its image mod p and then a pre-image under the quotient map, given above, implies that $\mathcal{I} = p\mathcal{O}_K + h_{\mathcal{I}}(\theta) \cdot \mathcal{O}_K$. □

To apply Proposition 6.2 to the ideal $\mathcal{L}\mathcal{O}_K$, let

$$B := \begin{pmatrix} Id_{n-k\times n-k} & A_{n-k\times k} \\ 0 & pId_{k\times k} \end{pmatrix} \tag{6.1.2}$$

denote the row wise HNF basis for the integer matrix L, where $A \in M_{n-k\times k}(\mathbb{F}_p)$. (See Section 2.2.3) Then, the coefficient embedding with respect to $\vec{\theta}$ implies that the inflation $\mathcal{L}\mathcal{O}_K = p\mathcal{O}_K + \sum_{i=1}^{n-k} B_i(\theta)\mathcal{O}_K$, where $B_i(x) \in \mathbb{F}_p[x]$ is the polynomial obtained by taking the inner product of the i-th row of B with $(1, x, \ldots x^{n-1})^t$. Therefore, by Proposition 6.2,

$$\mathcal{L}\mathcal{O}_K = p\mathcal{O}_K + h_{\mathcal{L}}(\theta) \cdot \mathcal{O}_K, \text{ where } h_{\mathcal{L}}(x) := gcd(\{B_i(x)\}_{i=1}^{n-k}, f(x)) \in \mathbb{F}_p[x] \tag{6.1.3}$$

We argue similarly for the generators of $p \cdot f'(\theta) \cdot \mathcal{L}^\vee\mathcal{O}_K$. By Proposition 3.4, the $\mathbb{Z}$-basis for $\mathcal{L}^\vee$ are the elements obtained by taking the inner product with $(1x \ldots x^{n-1})^t$ of the rows of

$$B^\vee := (B^{-1})^t \cdot (V_f^t V_f)^{-1} = \begin{pmatrix} Id & 0 \\ \frac{-A^t}{p} & \frac{Id}{p} \end{pmatrix} \cdot (V_f^t V_f)^{-1}$$

Let $B_i^\vee \in \mathbb{Z}^n$ denote the i-th row of $p \cdot f'(\theta) \cdot (B^{-1})^t \cdot (V_f^t V_f)^{-1}$. Then, $pf'(\theta)\mathcal{L}^\vee = \sum_{i=1}^n \mathbb{Z} \cdot B_i^\vee(\theta)$, as a $\mathbb{Z}$-module, and the inflation

$$pf'(\theta)\mathcal{L}^\vee\mathcal{O}_K = p\mathcal{O}_K + \sum_{i=1}^{n} B_i^\vee(\theta) \cdot \mathcal{O}_K = p\mathcal{O}_K + h_{\mathcal{L}^\vee}(\theta)\mathcal{O}_K \tag{6.1.4}$$

where $h_{\mathcal{L}^\vee}(\theta) := gcd(\{B_i^\vee(x)\}_i, f(x)) \in \mathbb{F}_p[x]$, by Proposition 6.2.

Now, in a monogenic field, the prime ideal decomposition of the ideal $p\mathcal{O}_K$ is closely related to the decomposition of the generating polynomial $f(x)$ into irreducible factors in $\mathbb{F}_p[x]$. This is described in the following result.

Theorem 6.3 (Dedekind, [Cond, Thm. 1])**.** *Let K be a monogenic number field generated by the root θ of a monic irreducible polynomial $f(x) \in \mathbb{Z}[x]$. Fix a prime p. If $f(x) = \prod_{i=1}^{r} f_i(x)^{e_i}$ splits into r distinct irreducible polynomials $f_i(x) \in \mathbb{F}_p[x]$, then $p\mathcal{O}_K = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdot\ldots\cdot\mathfrak{p}_r^{e_r}$ splits into a product of r distinct primes ideals $\mathfrak{p}_i$ in $\mathcal{O}_K$, with multiplicity e_i. The prime $\mathfrak{p}_i = p\mathcal{O}_K + f_i(\theta)\mathcal{O}_K$.*

In particular, a prime $\mathfrak{p}_i \mid \mathcal{L}\mathcal{O}_K$ if and only if $f_i(x) \mid h_{\mathcal{L}}(x)$, for $1 \le i \le r$. This follows from the fact that both the conditions are equivalent to the condition that $\mathfrak{p}_i \mod p\mathcal{O}_K \mid \mathcal{L}\mathcal{O}_K \mod p\mathcal{O}_K$. Multiplicities of the primes (or the polynomials) follow suit, i.e., for each $1 \le i \le r$

$$\begin{aligned} \mathcal{L}\mathcal{O}_K = \prod_{\nu_i \ge 0} \mathfrak{p}_i^{\nu_i} \quad &\iff \quad f_i(x)^{\nu_i} \mid h_{\mathcal{L}}(x), \qquad \text{and} \\ pf'(\theta)\mathcal{L}^\vee\mathcal{O}_K = \prod_{\mu_i \ge 0} \mathfrak{p}_i^{\mu_i} \quad &\iff \quad f_i(x)^{\mu_i} \mid h_{\mathcal{L}^\vee}(x). \end{aligned}$$

This discussion proves the following proposition describing the conductor $\mathcal{C}_{\mathcal{L}}$ of $\mathcal{O}_{\mathcal{L}}$. For an $\mathcal{O}_K$ ideal $\mathcal{I}$ and a prime ideal $\mathfrak{p}$, let $\mathfrak{p}^s \parallel \mathcal{I}$ mean that $\mathfrak{p}^s \mid \mathcal{I}$ and $\mathfrak{p}^{s+1} \nmid \mathcal{I}$. We extend the same notation to polynomials in $\mathbb{F}_p[x]$.

Proposition 6.4. *Let L be a p-ary integer lattice and let $\mathcal{L}$ denote its image in K under the coefficient embedding with respect to $\vec{\theta}$. Let $\mathcal{O}_{\mathcal{L}}$ be the ring of multiplier for $\mathcal{L}$. Then, the conductor $\mathcal{C}_{\mathcal{L}} \mid p\mathcal{O}_K$, as $\mathcal{O}_K$-ideals. Further, let $p\mathcal{O}_K = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$, where each $\mathfrak{p}_i = p\mathcal{O}_K + f_i(\theta)\mathcal{O}_K$ is a prime ideal in $\mathcal{O}_K$, with $f_i(x) \in \mathbb{F}_p[x]$. Then, for $1 \le i \le r$, and $0 \le s_i \le e_i$,*

$$\mathfrak{p}_i^{e_i - s_i} \parallel \mathcal{C}_{\mathcal{L}} \iff f_i^{s_i}(x) \parallel h_{\mathcal{L}}(x) \cdot h_{\mathcal{L}^\vee}(x) \qquad \text{in } \mathbb{F}_p[x].$$

In the special case, when $p\mathcal{O}_K$ splits completely in K, i.e., the prime factors $\mathfrak{p}_i = (\theta - w_i)\mathcal{O}_K + p\mathcal{O}_K$, for a root w_i of $f(x)$ in $\mathbb{F}_p$, then

$$\mathfrak{p}_i \mid \mathcal{C}_{\mathcal{L}} \iff h_{\mathcal{L}}(w_i) \cdot h_{\mathcal{L}^\vee}(w_i) \neq 0 \mod p$$

Proof. The fact that $\mathcal{C}_{\mathcal{L}} \mid p\mathcal{O}_K$ follows from the fact that $\mathbb{Z} + p\mathcal{O}_K \subseteq \mathcal{O}_{\mathcal{L}}$ (Lemma 3.7) and that the conductor is the largest $\mathcal{O}_K$-ideal in $\mathcal{O}_{\mathcal{L}}$, thereby implying that $p\mathcal{O}_K \subseteq \mathcal{C}_{\mathcal{L}}$.

Fix an index i, and let $\mathfrak{p}_i := p\mathcal{O}_K + f_i(x)\mathcal{O}_K$ be a prime ideal (over p) in $\mathcal{O}_K$. Assume that $\mathfrak{p}_i^{e_i - s_i} \parallel \mathcal{C}_{\mathcal{L}}$. Then, $0 \le s_i \le e_i$, as $\mathcal{C}_{\mathcal{L}}$ is an integral $\mathcal{O}_K$-ideal that divides $p\mathcal{O}_K$ and $\mathfrak{p}_i^{e_i} \parallel p\mathcal{O}_K$. Now,

$$\begin{aligned} \mathfrak{p}_i^{e_i - s_i} \parallel \mathcal{C}_{\mathcal{L}} \quad &\implies \quad \mathfrak{p}_i^{s_i} \parallel \frac{p\mathcal{O}_K}{\mathcal{C}_{\mathcal{L}}} \\ &\implies \quad \mathfrak{p}_i^{s_i} \parallel pf'(\theta)\mathcal{L}^\vee\mathcal{O}_K \cdot \mathcal{L}\mathcal{O}_K, \qquad \text{by Equation (6.1.1)} \end{aligned}$$

As, by Equations (6.1.3) and (6.1.4),

$$\mathfrak{p}_i^{s_i} = p\mathcal{O}_K + f_i^{s_i}(\theta)\mathcal{O}_K, \quad \text{and} \quad pf'(\theta)\mathcal{L}^\vee\mathcal{O}_K \cdot \mathcal{L}\mathcal{O}_K = p\mathcal{O}_K + h_{\mathcal{L}}(\theta) \cdot h_{\mathcal{L}}^\vee(\theta)\mathcal{O}_K,$$

viewing the ideals in $\mathcal{O}_K/p\mathcal{O}_K \simeq \mathbb{F}_p[x]/f$, implies that $f_i^{s_i}(x) \parallel h_{\mathcal{L}}(x) \cdot h_{\mathcal{L}^\vee}(x)$. Conversely, if $f_i^{s_i}(x) \parallel h_{\mathcal{L}}(x) \cdot h_{\mathcal{L}^\vee}(x)$, for $s_i \ge 0$, then the ideals

$$\mathfrak{p}_i^{s_i} = p\mathcal{O}_K + f_i^{s_i}(\theta)\mathcal{O}_K \supseteq p\mathcal{O}_K + h_{\mathcal{L}}(\theta) \cdot h_{\mathcal{L}}^\vee(\theta)\mathcal{O}_K = pf'(\theta)\mathcal{L}^\vee\mathcal{O}_K \cdot \mathcal{L}\mathcal{O}_K$$

implies that $\mathfrak{p}_i^{s_i} \parallel pf'(\theta)\mathcal{L}^\vee\mathcal{O}_K \cdot \mathcal{L}\mathcal{O}_K$, which in turn implies that $\mathfrak{p}_i^{e_i - s_i} \parallel \mathcal{C}_\mathcal{L}$, as before.

Finally, if $p\mathcal{O}_K$ splits completely in K, then the irreducible factors $f_i(x) \in \mathbb{F}_p[x]$ are linear, say $f_i(x) := x - w_i$. The claim follows from the observation that for a polynomial $g(x) \in \mathbb{F}_p[x]$,

$$f_i(x) \mid g(x) \iff g(w_i) = 0 \mod p.$$

□

The algorithm to find $\mathcal{C}_\mathcal{L}$: We present an algorithm that given a HNF basis for a p-ary integer lattice L and a monogenic number field $K := \mathbb{Q}(\theta)$ as input, computes the prime decomposition of the conductor of the ring of multipliers of $\mathcal{L}$ and expresses it in a (prime-ideal,multiplicity)-tuple. Given the minimal polynomial $f(x) \in \mathbb{Z}[x]$ of θ, we first factorize $f(x) \mod p \in \mathbb{F}_p[X]$ into irreducible factors $f_i(x) \in \mathbb{F}_p[x]$, which requires $\widetilde{O}(n^2 \log p)$ operations in $\mathbb{F}_p$, [vzGG13, Thm 14.14]. Then, we compute the polynomials $h_\mathcal{L}$ and $h_{\mathcal{L}^\vee}$ as in Equations (6.1.3) and (6.1.4). We use the probabilistic algorithm [vzGG13, Alg 6.45], which requires $O(n^2)$ operations to find the gcd in $\mathbb{F}_p$. We finally factorize $T = h_\mathcal{L} \cdot h_{\mathcal{L}^\vee}$ in $\mathbb{F}_p[x]$ to obtain the maximal power $f_i^{s_i}$ of f_i that divides $h_\mathcal{L} \cdot h_{\mathcal{L}^\vee}$ in $\mathbb{F}_p[x]$. Therefore, the total number of operations required is $\widetilde{O}(n^2 \log p)$. As $pf'(\theta)\mathcal{L}^\vee\mathcal{O}_K \cdot \mathcal{L}\mathcal{O}_K = p\mathcal{O}_K + T(\theta)\mathcal{O}_K$ divides $p\mathcal{O}_K = p\mathcal{O}_K + f(\theta)\mathcal{O}_K$, the polynomials $T \mid f$. We remark that the algorithm becomes relatively simpler when the prime p splits completely in $\mathcal{O}_K$. As, in this case, the polynomial $f(x)$ splits into n linear factors in $\mathbb{F}_p[x]$ and steps 2, 3 and 5 of the algorithm merely become evaluating the respective polynomials at the roots of $f(x)$.

Algorithm 1 The algorithm for the conductor

Input: an HNF basis for a p-ary integer lattice L, a monogenic number field $K := \mathbb{Q}[x]/\langle f(x)\rangle$ and a primitive root θ of $f(x) \in \mathbb{Z}[x]$

Output: the prime decomposition, as an $\mathcal{O}_K$-ideal, of the conductor $\mathcal{C}_\mathcal{L}$ of the ring of multipliers of the embedding, $\mathcal{L}$, of L into K

1: factorize f over $\mathbb{F}_p[X]$ as $f = f_1^{e_1} \cdot \ldots \cdot f_r^{e_r}$
2: find the polynomials B_i and the gcd $h_\mathcal{L}$ as in Equation (6.1.3)
3: find the polynomials $B_i^\vee$ and the gcd $h_{\mathcal{L}^\vee}$ as in Equation (6.1.4)
4: $T = h_\mathcal{L} \cdot h_{\mathcal{L}^\vee}$
5: factorize T over $\mathbb{F}_p[X]$ as $T = f_1^{s_1} \cdot \ldots \cdot f_r^{s_r}$
6: **for** $i \leftarrow 1, r$ **do**
7: $\quad \mathfrak{p}_i = p\mathcal{O}_K + f_i(\theta)\mathcal{O}_K$
8: $\quad$ output $(\mathfrak{p}_i, e_i - s_i)$
9: **end for**

Remark 6.5. *When K is a non-monogenic number field, the above algorithm yields the conductor, $\mathcal{C}_\theta$, of the ring of multipliers $\mathcal{O}_\mathcal{L}$ with respect to the order $\mathcal{O} := \mathbb{Z}[\theta]$, as long as p is coprime to the index $[\mathcal{O}_K : \mathcal{O}]$. As, under this coprimality assumption, $p\mathcal{O}$ is an invertible $\mathcal{O}$-ideal and admits a unique factorization into prime ideals in $\mathcal{O}$. This factorization is achieved exactly as in Theorem 6.3, with $\mathcal{O}_K = \mathcal{O}$. Further, as discussed at the end of Section 3, the conductor $\mathcal{C}_\theta$ is an invertible $\mathbb{Z}[\theta]$-ideal if $(p, [\mathcal{O}_K : \mathbb{Z}[\theta]]) = 1$, implying that Equation (6.1.1) holds with $\mathcal{O}_K$ replaced by $\mathbb{Z}[\theta]$. Therefore, Algorithm 1, when run with $\mathcal{O}_K$ replaced by $\mathcal{O}$ yields the factorization of $\mathcal{C}_\theta$ as an $\mathcal{O}$-ideal, if p is chosen to be co-prime to $[\mathcal{O}_K : \mathcal{O}]$. See the discussion before Subsection 6.1 to learn what $\mathcal{C}_\theta$ can say about $\mathcal{C}_\mathcal{L}$.*

6.2 p-ary lattices in the power-of-two cyclotomic extension

We fix the field K to be the power-of-two cyclotomic extension and embed all integer p-ary lattices into K, via the coefficient embedding with respect to the power basis, to study the behavior of the corresponding ring of multipliers. Recall that the coefficient embedding introduces a distortion in the geometry of the complex space, i.e., the Minkowski image of K lies in $V_f \cdot \mathbb{C}^n$, where n is the degree of K, and V_f is the Vandermonde matrix corresponding to the minimal polynomial of K. When K is the power-of-two cyclotomic extension, the Vandermonde matrix turns out to be a rotation of the complex space, up to scaling by $\sqrt{n}$. In other words, the geometry of the complex space remains invariant (up to scaling) under this embedding. It is the preservation of the norm and the geometry, in this case, that motivates us to explore how the set of p-ary lattices behave under the algebraic structure induced from the power-of-two cyclotomics.

Fix n to be a power-of-two and let ζ_{2n} denote the primitive $2n$-th root of unity. Let $K := \mathbb{Q}(\zeta_{2n})$, a power-of-two extension of degree n. It is well known that its ring of integers $\mathcal{O}_K$ equals $\mathbb{Z}[\zeta_{2n}]$, and hence under the coefficient embedding with respect to $\vec{\zeta_{2n}} := (1\ \zeta_{2n} \dots \zeta_{2n}^{n-1})$, the lattice $\mathbb{Z}^n$ corresponds to $\mathcal{O}_K$. For a fixed prime p, let L denote an integer p-ary lattice, i.e., $p\mathbb{Z}^n \subseteq L \subseteq \mathbb{Z}^n$. Then the image $\mathcal{L}$ of L in K satisfies $p\mathcal{O}_K \subseteq \mathcal{L} \subseteq \mathcal{O}_K$, and the ring of multipliers $\mathcal{O}_\mathcal{L}$ contains the order $\mathbb{Z} + p\mathcal{O}_K$, which in turn implies that the conductor, $\mathcal{C}_\mathcal{L}$, satisfies $p\mathcal{O}_K \subseteq \mathcal{C}_\mathcal{L} \subseteq \mathcal{O}_K$. Even though the conductor does not describe the order uniquely, i.e., there may be two distinct orders with the same conductor, it gives a fair idea of the size of the ring. The ideal scenario would be that the conductor equals $\mathcal{O}_K$, for in that case $\mathcal{O}_\mathcal{L}$ equals $\mathcal{O}_K$ and one would be able to apply the results from [CDPR16, CDW17, PHS19, BRL20] to solve lattice problems on $\mathcal{L}$, and in turn solve lattice problems on L, using Proposition 3.3. The worst case scenario would be that $\mathcal{O}_\mathcal{L} = \mathbb{Z} + p\mathcal{O}_K$ and hence the conductor equals $p\mathcal{O}_K$, for then solving lattice problems on L would be at least as hard as solving $\mathbb{Z} + p\mathcal{O}_K$-LWE, (Theorem 4.1) which is as hard as unstructured LWE, as proved in Corollary 5.7. Thereby proving the additional algebraic structure from K, a redundant piece of information. Finally, as mentioned in the introduction of Section 3, in all the other scenarios, when the conductor is strictly between $\mathcal{O}_K$ and $p\mathcal{O}_K$, one may use the Ring-LWE oracle to solve DGS on $\mathcal{L}$ (Corollary 4.7). Recall that the approximation factor for DGS is directly related to the short vectors in $\mathcal{C}_\mathcal{L}$. In other words, this approach yields short vectors on $\mathcal{L}$ as long as $\mathcal{C}_\mathcal{L}$ has vectors shorter than p. One of the necessary conditions for that is, that $p\mathcal{O}_K$ be properly contained in $\mathcal{C}_\mathcal{L}$.

We fix $p = 1 \mod 2n$ to be a prime that splits completely in $\mathcal{O}_K$. We use Proposition 6.4 to count the number of p-ary lattices that fall in the worst case scenario, i.e., lattices $\mathcal{L}$ for which the conductor equals $p\mathcal{O}_K$. As we will see, the count yields that the ratio of the size of the subset

$$S_k := \{L : p\mathbb{Z}^n \subseteq L \subseteq \mathbb{Z}^n,\ [\mathbb{Z}^n : L] = p^k,\ \text{and}\ \ \mathcal{C}_\mathcal{L} = p\mathcal{O}_K\}$$

to the size of the set of all p-ary lattices of index p^k embedded in the power-of-two cyclotomic, can be bounded to be extremely close to 1, i.e., $1 - o(1)$ or even negligibly close in some cases. See Corollary 6.8 for a precise bound. This implies that the power-of-two cyclotomic field that preserves the geometry of $\mathbb{Z}^n$ does not yield a 'good enough' algebraic structure for integer p-ary lattices.

Let $\widetilde{S}_k$ be the set of all p-ary integer lattices of det p^k. By Equation (6.1.2), the set $\widetilde{S}_k$ is in one-to-one correspondence with the set $\{A \in M_{n-k\times k}(\mathbb{F}_p)\}$ and hence $|\widetilde{S}_k| = p^{(n-k)k}$. The next result describes the subset of $M_{n-k\times k}(\mathbb{F}_p)$ that corresponds to S_k. Let L be a p-ary lattice of determinant p^k, and let $B := \begin{pmatrix} Id_{n-k\times n-k} & A_{n-k\times k} \\ 0 & pId_{k\times k} \end{pmatrix}$ be the row-wise HNF basis for L. Let w_i,

for $1 \le i \le n$, be the roots of $f(x) := x^n + 1 \bmod p$. We denote by $\widetilde{Id}_{k\times k}$, the $k \times k$ matrix with 1's on the anti-diagonal and 0's elsewhere.

Proposition 6.6. *Let L be a p-ary lattice generated by the matrix B defined above. Let $\mathcal{L}$ denote the image of L in K. Let $p\mathcal{O}_K = \prod_{i=1}^{n} \mathfrak{p}_i$, with the prime ideal $\mathfrak{p}_i = p\mathcal{O}_K + (\zeta - w_i)\mathcal{O}_K$. Then,*

$$\mathfrak{p}_i \parallel \mathcal{L}\mathcal{O}_K \iff \vec{V}(w_i) := (-A|Id)\begin{pmatrix}1 & w_i & \dots & w_i^{n-1}\end{pmatrix}^t = \vec{0}, \quad \text{and}$$

$$\mathfrak{p}_i \parallel p\cdot n\cdot \mathcal{L}^\vee\mathcal{O}_K \iff \vec{W}(w_i) := \begin{pmatrix}w_i^{n-k-1} & \dots & w_i & 1 & w_i^{n-k} & \dots & w_i^{n-1}\end{pmatrix}\begin{pmatrix}A\\ -\\ \widetilde{Id}_{k\times k}\end{pmatrix} = \vec{0}$$

Therefore, the set

$$S_k \simeq \left\{A \in M_{n-k\times k}(\mathbb{F}_p) : \vec{V}(w_i) \neq \vec{0} \text{ and } \vec{W}(w_i) \neq \vec{0}, \quad \text{for all } 1 \le i \le n\right\}$$

Here, $\vec{0}$ denotes the zero vector of the appropriate size.

Proof. Recall that when $K = \mathbb{Q}(\zeta_{2n})$, the dual ideal $\mathcal{O}_K^\vee = \frac{1}{n}\mathcal{O}_K$. Therefore, by Proposition 2.24 and Lemma 2.26, the conductor $\mathcal{C}_\mathcal{L} \subset K$ satisfies, $\mathcal{C}_\mathcal{L} \cdot \mathcal{L}\mathcal{O}_K \cdot \mathcal{L}^\vee\mathcal{O}_K = \mathcal{O}_K^\vee = \frac{1}{n}\mathcal{O}_K$. Rewriting this equation yields the following equality of integral $\mathcal{O}_K$-ideals,

$$(\mathcal{L}\mathcal{O}_K)\cdot\left(p\cdot n\cdot \mathcal{L}^\vee\mathcal{O}_K\right) = \frac{p\mathcal{O}_K}{\mathcal{C}_\mathcal{L}}. \tag{6.2.1}$$

Further, by Equations (6.1.3) & (6.1.4),

$$\mathcal{L}\mathcal{O}_K = p\mathcal{O}_K + h_\mathcal{L}(\zeta)\cdot\mathcal{O}_K \qquad \text{and} \qquad p\cdot n\cdot\mathcal{L}^\vee\mathcal{O}_K = p\mathcal{O}_K + h_{\mathcal{L}^\vee}(\zeta)\mathcal{O}_K,$$

for polynomials $h_\mathcal{L}(\zeta), h_{\mathcal{L}^\vee}(\zeta) \in \mathbb{F}_p[\zeta]$. By the discussion before Proposition 6.4, the prime $\mathfrak{p}_i \parallel \mathcal{L}\mathcal{O}_K$ if and only if $h_\mathcal{L}(w_i) = 0$. Recall that $h_\mathcal{L}(x) := gcd(\{B_i(x)\}_{i=1}^{n-k}, x^n + 1) \in \mathbb{F}_p[x]$, where each $B_i(x)$ is obtained by taking the inner product of the i-th row of the HNF basis B with the vector $(1\ x \dots x^{n-1})$. See Section 6.1 for details. Under the assumption that $x^n + 1 = 0$, the description of $B_i(x)$'s in matrix form looks like;

$$\begin{pmatrix}-A \mid & Id\end{pmatrix}\begin{pmatrix}1\\ x\\ \vdots\\ x^{n-1}\end{pmatrix} = \begin{pmatrix}x^k B_1(x)\\ \vdots\\ x^k B_{n-k}(x)\end{pmatrix} \tag{6.2.2}$$

Viewing these values mod p, we get for any $1 \le j \le n-k$

$$h_\mathcal{L}(w_i) = 0 \iff B_j(w_i) = 0 \iff w_i^k B_j(w_i) = 0 \quad \text{as } w_i \neq 0 \mod p$$

For the other condition, Remark 3.5 describes the basis of $\mathcal{L}^\vee$ in K, as

$$B^\vee := (B^{-1})^t \cdot (V_f^t V_f)^{-1} = \frac{1}{n}\begin{pmatrix}Id & 0\\ \frac{-A^t}{p} & \frac{Id}{p}\end{pmatrix}\cdot(\mathbf{e}_1 - \mathbf{e}_n \dots - \mathbf{e}_2)$$

For $1 \leq j \leq k$, let $B_j^\vee(x) \in \mathbb{F}_p[x]$ be the polynomial obtained by taking the inner product of the $(n-k+j)$-th row of $p \cdot n \cdot B^\vee$ with the vector $(1\ x \ldots x^{n-1})$. A straightforward computation, along with the fact that $x^n + 1 = 0$, implies that the the polynomial $\frac{B_j^\vee(x)}{x^{k+1}}$ is obtained as follows;

$$\begin{pmatrix} x^{n-k-1} & x^{n-k-2} & \ldots & x & 1 & x^{n-k} & x^{n-k+1} & \ldots & x^{n-1} \end{pmatrix} \begin{pmatrix} A \\ - \\ \widetilde{Id}_{k\times k} \end{pmatrix} = \begin{pmatrix} \frac{B_1^\vee(x)}{x^{k+1}} & \ldots & \frac{B_k^\vee(x)}{x^{k+1}} \end{pmatrix} \tag{6.2.3}$$

Now, $h_{\mathcal{L}^\vee}(x) := gcd(\{B_j^\vee(x)\}_{j=1}^k, x^n + 1) \in \mathbb{F}_p[x]$, and $\mathfrak{p}_i \parallel p \cdot n \cdot \mathcal{L}^\vee \mathcal{O}_K$ if and only if $h_{\mathcal{L}^\vee}(w_i) = 0$, which in turn is true if and only if $\frac{B_j^\vee(w_i)}{w_i^{k+1}} = 0 \mod p$, for any $1 \leq j \leq k$, as $w_i \neq 0 \mod p$. This proves the second condition.

Finally, a p-ary lattice L of det$= p^k$ lies in S_k if and only if $\mathfrak{p}_i \nmid \mathcal{L}\mathcal{O}_K$ and $\mathfrak{p}_i \nmid p \cdot n \cdot \mathcal{L}^\vee \mathcal{O}_K$, for all i. See Equation (6.2.1). Using the equivalent conditions above yields the final claim in the statement. □

For each $1 \leq i \leq n$, let $V_i := \{A \in M_{n-k\times k}(\mathbb{F}_p) : \vec{V}(w_i) = \vec{0}\}$ and $W_i := \{A \in M_{n-k\times k}(\mathbb{F}_p) : \vec{W}(w_i) = \vec{0}\}$. Then, by Proposition 6.6,

$$S_k \simeq \widetilde{S}_k \setminus \bigcup_{i=1}^{n} (V_i \cup W_i)$$

Proposition 6.7. *The size of the set S_k is*

$$\sum_{s=0}^{k-1} p^{(k-s)(n-k)} \left[(-1)^s \binom{n}{s} \left(1 - p^{-(k-s)}\right)^{n-s} - \sum_{i=n-k+s+1}^{n} (-1)^i \binom{n}{i} \binom{i}{s} p^{-(k-s)(i-s)} \right]$$

Proof. The inclusion-exclusion principle implies that,

$$|S_k| = |\widetilde{S}_k| + \sum_{i=1}^{2n} (-1)^i \left(\sum_{l+l'=i} |V_{i_1} \cap \ldots \cap V_{i_l} \cap W_{j_1} \cap \ldots \cap W_{j_{l'}}| \right) \tag{6.2.4}$$

We prove that

- $|V_i| = p^{(k-1)(n-k)}$, and $|V_{i_1} \cap V_{i_2} \cap \ldots \cap V_{i_l}| = p^{(k-l)(n-k)}$, as long as $1 \leq i_j \leq n$ are distinct and $l \leq k$. For $l > k$, the intersection is a null set.
- $|W_i| = p^{k(n-k-1)}$, and $|W_{i_1} \cap W_{i_2} \cap \ldots \cap W_{i_{l'}}| = p^{k(n-k-l')}$, as long as $1 \leq i_j \leq n$ are distinct indices and $l' \leq n-k$. For $l' > n-k$, the intersection is a null set.
- $|V_i \cap W_i| = \emptyset$, for $1 \leq i \leq n$.
- For $l + l'$ distinct indices, $|V_{i_1} \cap \ldots \cap V_{i_l} \cap W_{j_1} \cap \ldots \cap W_{j_{l'}}| = p^{(k-l)(n-k-l')}$ if $0 \leq l \leq k$ and $0 \leq l' \leq n-k$, and 0, otherwise.

An element of the set V_i yields $n-k$ polynomials in $\mathbb{F}_p[x]$ whose coefficients are given by each of the $n-k$ rows in $(-A|Id)$. Since A has k columns, each polynomial has k free variables. However, being an element of V_i, all the polynomials simultaneously vanish at w_i. Therefore, each

polynomial has $k-1$ free variables, and we have $|V_i| = p^{(k-1)(n-k)}$. The same argument proves that if A lies in $l \leq k$ distinct V_i's, then each polynomial has $k-l$ free variables, implying that $|V_{i_1} \cap \ldots \cap V_{i_l}| = p^{(k-l)(n-k)}$. If $l > k$, the degree k polynomial corresponding to the first row of $(-A|Id)$ would have more roots than k-many, yielding a contraction. Therefore, for $l > k$, the intersection is empty.

The count for the intersection of W_i's follows from an exact same argument, once we observe that an element of W_i yields k polynomials in $\mathbb{F}_p[x]$ whose coefficients are given by each of the k columns of $(A|\widetilde{Id})^t$. As A has $n-k$ rows, each polynomial has $n-k$ free variables. However, being an element of W_i, all the polynomials simultaneously vanish at w_i. Therefore, each polynomial has $n-k-1$ free variables, and we have $|W_i| = p^{k(n-k-1)}$. Similarly, $|W_{i_1} \cap W_{i_2} \cap \ldots \cap W_{i_{l'}}| = p^{k(n-k-l')}$, as long as $1 \leq i_j \leq n$ are distinct indices and $l' \leq n-k$. If $l' > n-k$, this intersection is a null set.

Further, if $A \in V_i \cap W_i$, then, by Proposition 6.6 the prime $\mathfrak{p}_i$ divides both $\mathcal{L}\mathcal{O}_K$ and $p \cdot n \cdot \mathcal{L}^\vee \mathcal{O}_K$ implying that $\mathfrak{p}_i^2 \mid p\mathcal{O}_K$, which contradicts the fact that p splits completely.

Finally, the fact that, $|V_{i_1} \cap \ldots \cap V_{i_l} \cap W_{j_1} \cap \ldots \cap W_{j_{l'}}| = p^{(k-l)(n-k-l')}$, for $l+l'$ distinct indices with $0 \leq l \leq k$ and $0 \leq l' \leq n-k$ essentially follows from combining the first two arguments. A detailed proof is included in Appendix A. Compiling this information, along with the equality $(x+y)^n = \sum_{i=1}^n \binom{n}{i} x^i y^{n-i}$, we get

$$\begin{aligned}
|S_k| &= |\widetilde{S}_k| - \sum_{i=1}^{n} (|V_i| + |W_i|) + \sum_{i \neq j} (|V_i \cap V_j| + |V_i \cap W_j| + |W_i \cap W_j|) \\
&\quad + \sum_{i=3}^{n} (-1)^i \sum_{l+l'=i} |V_{i_1} \cap \ldots \cap V_{i_l} \cap W_{j_1} \cap \ldots \cap W_{j_{l'}}| \\
&= p^{(n-k)\cdot k} - \sum_{i=1}^{n} \left(p^{(k-1)(n-k)} + p^{k(n-k-1)} \right) + \sum_{i \neq j} \left(p^{(k-2)(n-k)} + p^{(k-1)(n-k-1)} + p^{k(n-k-2)} \right) \\
&\quad + \sum_{i=3}^{n} (-1)^i \sum_{l+l'=i} p^{(k-l)(n-k-l')} \\
&= \sum_{s=0}^{k-1} p^{(k-s)(n-k)} \left[(-1)^s \binom{n}{s} \left(1 - p^{-(k-s)}\right)^{n-s} - \sum_{i=n-k+s+1}^{n} (-1)^i \binom{n}{i} \binom{i}{s} p^{-(k-s)(i-s)} \right]
\end{aligned}$$

For a step-by-step computation of this equality, we refer the reader to Appendix A. □

In the particular case of p-ary lattices of determinant p, the Proposition above proves that the cardinality of the set S_1 is $\frac{(p-1)^n-1}{p}$. Therefore, the ratio of S_1 to the set of all p-ary lattices of det p is

$$|S_1|/|\widetilde{S}_1| = \frac{(p-1)^n - 1}{p^n} \approx 1.$$

In the next result, we give a rough lower bound for the ratio $|S_k|/|\widetilde{S}_k|$ and argue that the lattices of S_k are indeed dense in the set of all p-ary lattices of index p^k.

Corollary 6.8. *Let $S_k \subseteq \widetilde{S}_k$ be the sets defined above. Then,*

$$\frac{|S_k|}{|\widetilde{S}_k|} \geq 1 - \frac{n}{p^k} - \frac{n}{p^{n-k}}.$$

Proof. Recall that $S_k = \widetilde{S}_k \setminus \bigcup_{i=1}^{n}(V_i \cup W_i)$, and $|\widetilde{S}_k| = p^{k(n-k)}$. As explained in the proof of Proposition 6.7, $|V_i| = p^{(k-1)(n-k)}$ and $|W_i| = p^{k(n-k-1)}$, for $1 \leq i \leq n$. We use the fact that $|\bigcup_{i=1}^{n}(V_i \cup W_i)| \leq \sum_{i=1}^{n}(|V_i| + |W_i|)$, to get the following:

$$\begin{aligned}
|S_k| &= |\widetilde{S}_k| - |\bigcup_{i=1}^{n}(V_i \cup W_i)| \\
&\geq p^{k(n-k)} - \sum_{i=1}^{n}(|V_i| + |W_i|) \\
&= p^{k(n-k)} - n \cdot p^{(k-1)(n-k)} - n \cdot p^{k(n-k-1)} \\
&= p^{k(n-k)}\left(1 - \frac{n}{p^{n-k}} - \frac{n}{p^k}\right),
\end{aligned}$$

which leads to the lower bound on the ratio $|S_k|/|\widetilde{S}_k|$, as claimed. □

A Deferred details from Proof of Proposition 6.7

We will make use of the following lemma involving primitive roots of order $2n$ mod p.

Lemma A.1. *Let n be a power of 2. For any x and w distinct primitive roots of order $2n$ mod p, i.e. $x^n = w^n = -1$, then*

$$x^{n-k-1}w^k + x^{n-k-2}w^{k+1} + \ldots + w^{n-1} = -(x^{n-1} + x^{n-2}w + \ldots + x^{n-k}w^{k-1})$$

Proof. Notice that $\frac{x^n - w^n}{x - w} = x^{n-1}w + x^{n-2}w^2 + \ldots + xw^{n-1}$, which is 0, since $x^n = w^n = -1$. □

Now we prove the size of the mixed terms involved in Equation (6.2.4).

Proposition A.2. *For $l + l'$ distinct indices, $|V_{i_1} \cap \ldots \cap V_{i_l} \cap W_{j_1} \cap \ldots \cap W_{j_{l'}}| = p^{(k-l)(n-k-l')}$ if $0 \leq l \leq k$ and $0 \leq l' \leq n - k$.*

Proof. Let $A \in M_{n-k\times k}(\mathbb{F}_p)$ such that $A \in V_{i_1} \cap \ldots \cap V_{i_l}$. By definition of the set V_i, we have

$$(-A|Id)\begin{pmatrix} 1 & 1 & \ldots & 1 \\ w_{i_1} & w_{i_2} & \ldots & w_{i_l} \\ \vdots & \vdots & \ddots & \vdots \\ w_{i_1}^{n-1} & w_{i_2}^{n-1} & \ldots & w_{i_l}^{n-1} \end{pmatrix} = (-A|Id)\begin{pmatrix} \mathrm{Vand}_1 \\ \mathrm{Vand}_2 \\ M \end{pmatrix} = \underline{0}. \tag{A.0.1}$$

where $\mathrm{Vand}_1 \in M_{l\times l}(\mathbb{F}_p)$, $\mathrm{Vand}_2 \in M_{k-l\times l}(\mathbb{F}_p)$ and $M \in M_{n-k\times l}(\mathbb{F}_p)$. Now consider $A = (A_1|A_2)$ for $A_1 \in M_{n-k\times l}(\mathbb{F}_p)$ and $A_2 \in M_{n-k\times k-l}(\mathbb{F}_p)$. Equation (A.0.1) can be written using these notations as follows

$$A_1\mathrm{Vand}_1 + A_2\mathrm{Vand}_2 = M \tag{A.0.2}$$

Notice that the matrix Vand_1 is the $l\times l$ Vandermonde matrix corresponding to the distinct elements $w_{i_1}, \ldots, w_{i_l} \in \mathbb{F}_p$, and hence invertible over $\mathbb{F}_p$. Therefore Equation (A.0.2) gets rewritten as

$$A_1 = (M - A_2\mathrm{Vand}_2) \cdot \mathrm{Vand}_1^{-1} \tag{A.0.3}$$

Now consider that $A \in W_{j_1} \cap \ldots \cap W_{j_{l'}}$. Using the definition of the set W_i, we have

$$\begin{pmatrix} w_{j_1}^{n-k-1} & \ldots & w_{j_1} & 1 & w_{j_1}^{n-k} & \ldots & w_{j_1}^{n-1} \\ w_{j_2}^{n-k-1} & \ldots & w_{j_2} & 1 & w_{j_2}^{n-k} & \ldots & w_{j_2}^{n-1} \\ \vdots & \ldots & \vdots & \vdots & \vdots & \ldots & \vdots \\ w_{j_{l'}}^{n-k-1} & \ldots & w_{j_{l'}} & 1 & w_{j_{l'}}^{n-k} & \ldots & w_{j_{l'}}^{n-1} \end{pmatrix} \begin{pmatrix} A \\ - \\ \widetilde{Id} \end{pmatrix} = \underline{0} \tag{A.0.4}$$

Let $E_1 = \begin{pmatrix} w_{j_1}^{n-k-1} & \ldots & w_{j_1} & 1 \\ w_{j_2}^{n-k-1} & \ldots & w_{j_2} & 1 \\ \vdots & \ddots & \vdots & \vdots \\ w_{j_{l'}}^{n-k-1} & \ldots & w_{j_{l'}} & 1 \end{pmatrix}$ and $E_2 = \begin{pmatrix} w_{j_1}^{n-k} & \ldots & w_{j_1}^{n-1} \\ w_{j_2}^{n-k} & \ldots & w_{j_2}^{n-1} \\ \vdots & \ddots & \vdots \\ w_{j_{l'}}^{n-k} & \ldots & w_{j_{l'}}^{n-1} \end{pmatrix}$. Further, let $E_2 \cdot \widetilde{Id} = (F_1|F_2)$, where $F_1 \in M_{l' \times l}(\mathbb{F}_p)$ and $F_2 \in M_{l' \times k-l}(\mathbb{F}_p)$.

Then we can write Equation (A.0.4) as follows

$$(E_1A_1 + F_1|E_1A_2 + F_2) = \underline{0} \tag{A.0.5}$$

We claim the following:

Claim A.2.1. *Equation* (A.0.3) *and*

$$E_1A_2 + F_2 = \underline{0} \tag{A.0.6}$$

imply

$$E_1A_1 + F_1 = \underline{0}. \tag{A.0.7}$$

Using Claim A.2.1, by Equation (A.0.5) we can tell that

$$|V_{i_1} \cap \ldots V_{i_l} \cap W_{j_1} \cap \ldots \cap W_{j_{l'}}| = |\{A_2 \in M_{n-k \times k-l}(\mathbb{F}_p)|\ E_1A_2 + F_2 = \underline{0}\}|$$

Notice that E_1 is a $l' \times n-k$ matrix of maximum rank l'. Therefore the set has cardinality $p^{(k-l)(n-k-l')}$, since each column of A_2 has $n-k-l'$ free variables. □

Proof of Claim A.2.1 Using Equation (A.0.3), Equation (A.0.6) and Lemma A.1, the left hand side of Equation (A.0.7) can be computed as follows:

$$\begin{aligned} E_1A_1 + F_1 &= E_1 \cdot (M - A_2\mathrm{Vand}_2)\mathrm{Vand}_1^{-1} + F_1 \\ &= \begin{pmatrix} w_{j_1}^{n-k-1} & \ldots & w_{j_1} & 1 \\ w_{j_2}^{n-k-1} & \ldots & w_{j_2} & 1 \\ \vdots & \ddots & \vdots & \vdots \\ w_{j_{l'}}^{n-k-1} & \ldots & w_{j_{l'}} & 1 \end{pmatrix} \cdot \begin{pmatrix} w_{i_1}^k & w_{i_2}^k & \ldots & w_{i_l}^k \\ w_{i_1}^{k+1} & w_{i_2}^{k+1} & \ldots & w_{i_l}^{k+1} \\ \vdots & \vdots & \ddots & \vdots \\ w_{i_1}^{n-1} & w_{i_2}^{n-1} & \ldots & w_{i_l}^{n-1} \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & \ldots & 1 \\ w_{i_1} & w_{i_2} & \ldots & w_{i_l} \\ \vdots & \vdots & \ddots & \vdots \\ w_{i_1}^{l-1} & w_{i_2}^{l-1} & \ldots & w_{i_l}^{l-1} \end{pmatrix}^{-1} - \\ &- E_1A_2 \cdot \begin{pmatrix} w_{i_1}^l & w_{i_2}^l & \ldots & w_{i_l}^l \\ w_{i_1}^{l+1} & w_{i_2}^{l+1} & \ldots & w_{i_l}^{l+1} \\ \vdots & \vdots & \ddots & \vdots \\ w_{i_1}^{k-1} & w_{i_2}^{k-1} & \ldots & w_{i_l}^{k-1} \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & \ldots & 1 \\ w_{i_1} & w_{i_2} & \ldots & w_{i_l} \\ \vdots & \vdots & \ddots & \vdots \\ w_{i_1}^{l-1} & w_{i_2}^{l-1} & \ldots & w_{i_l}^{l-1} \end{pmatrix}^{-1} + F_1 \end{aligned}$$

$$= - \begin{pmatrix} w_{j_1}^{n-1} & \dots & w_{j_1}^{n-k+1} & w_{j_1}^{n-k} \\ w_{j_2}^{n-1} & \dots & w_{j_2}^{n-k+1} & w_{j_2}^{n-k} \\ \vdots & \ddots & \vdots & \vdots \\ w_{j_{l'}}^{n-1} & \dots & w_{j_{l'}}^{n-k+1} & w_{j_{l'}}^{n-k} \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & \dots & 1 \\ w_{i_1} & w_{i_2} & \dots & w_{i_l} \\ \vdots & \vdots & \ddots & \vdots \\ w_{i_1}^{k-1} & w_{i_2}^{k-1} & \dots & w_{i_l}^{k-1} \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & \dots & 1 \\ w_{i_1} & w_{i_2} & \dots & w_{i_l} \\ \vdots & \vdots & \ddots & \vdots \\ w_{i_1}^{l-1} & w_{i_2}^{l-1} & \dots & w_{i_l}^{l-1} \end{pmatrix}^{-1}$$

$$+ F_2 \cdot \begin{pmatrix} w_{i_1}^{l} & w_{i_2}^{l} & \dots & w_{i_l}^{l} \\ w_{i_1}^{l+1} & w_{i_2}^{l+1} & \dots & w_{i_l}^{l+1} \\ \vdots & \vdots & \ddots & \vdots \\ w_{i_1}^{k-1} & w_{i_2}^{k-1} & \dots & w_{i_l}^{k-1} \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & \dots & 1 \\ w_{i_1} & w_{i_2} & \dots & w_{i_l} \\ \vdots & \vdots & \ddots & \vdots \\ w_{i_1}^{l-1} & w_{i_2}^{l-1} & \dots & w_{i_l}^{l-1} \end{pmatrix}^{-1} + F_1$$

$$= - \begin{pmatrix} w_{j_1}^{n-1} & \dots & w_{j_1}^{n-k+1} & w_{j_1}^{n-k} \\ w_{j_2}^{n-1} & \dots & w_{j_2}^{n-k+1} & w_{j_2}^{n-k} \\ \vdots & \ddots & \vdots & \vdots \\ w_{j_{l'}}^{n-1} & \dots & w_{j_{l'}}^{n-k+1} & w_{j_{l'}}^{n-k} \end{pmatrix} \cdot \left(\begin{matrix} \mathrm{Id}_{l\times l} \\ \begin{pmatrix} w_{i_1}^{l} & w_{i_2}^{l} & \dots & w_{i_l}^{l} \\ w_{i_1}^{l+1} & w_{i_2}^{l+1} & \dots & w_{i_l}^{l+1} \\ \vdots & \vdots & \ddots & \vdots \\ w_{i_1}^{k-1} & w_{i_2}^{k-1} & \dots & w_{i_l}^{k-1} \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & \dots & 1 \\ w_{i_1} & w_{i_2} & \dots & w_{i_l} \\ \vdots & \vdots & \ddots & \vdots \\ w_{i_1}^{l-1} & w_{i_2}^{l-1} & \dots & w_{i_l}^{l-1} \end{pmatrix}^{-1} \end{matrix} \right)$$

$$+ \begin{pmatrix} w_{j_1}^{n-l-1} & \dots & w_{j_1}^{n-k} \\ w_{j_2}^{n-l-1} & \dots & w_{j_2}^{n-k} \\ \vdots & \ddots & \vdots \\ w_{j_{l'}}^{n-l-1} & \dots & w_{j_{l'}}^{n-k} \end{pmatrix} \cdot \begin{pmatrix} w_{i_1}^{l} & w_{i_2}^{l} & \dots & w_{i_l}^{l} \\ w_{i_1}^{l+1} & w_{i_2}^{l+1} & \dots & w_{i_l}^{l+1} \\ \vdots & \vdots & \ddots & \vdots \\ w_{i_1}^{k-1} & w_{i_2}^{k-1} & \dots & w_{i_l}^{k-1} \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & \dots & 1 \\ w_{i_1} & w_{i_2} & \dots & w_{i_l} \\ \vdots & \vdots & \ddots & \vdots \\ w_{i_1}^{l-1} & w_{i_2}^{l-1} & \dots & w_{i_l}^{l-1} \end{pmatrix}^{-1} + F_1 = \underline{0}.$$

□

Knowing the size of mixed intersections, we show how we complete the final summation in the proof of Proposition 6.7.

Proof of final summation from Proposition 6.7 In order to compute the cardinality of S_k, for $0 \leq l \leq k$, we collect the intersections of any $V_{i_1} \cap \ldots \cap V_{i_l}$ of fixed l factors with any $W_{j_1} \cap \ldots \cap W_{j_{l'}}$, for any $0 \leq l' \leq n-k$ as following:

$$T_l = \sum_{l'=0}^{n-k} \sum_{1 \leq i_1 \neq \ldots \neq i_l \neq j_1 \neq \ldots \neq j_{l'} \leq n} (-1)^{l+l'} |V_{i_1} \cap \ldots \cap V_{i_l} \cap W_{j_1} \cap \ldots \cap W_{j_{l'}}|.$$

Therefore, $|S_k| = \sum_{l=0}^{k} T_l$. Notice that for any $0 \leq l \leq k$ and $0 \leq l' \leq n-k$, there are $\binom{n}{l+l'} \cdot \binom{l+l'}{l}$ intersections $V_{i_1} \cap \ldots \cap V_{i_l} \cap W_{j_1} \cap \ldots \cap W_{j_{l'}}$. Using Proposition A.2, we get

$$\begin{aligned} T_l &= \sum_{l'=0}^{n-k} \binom{n}{l+l'} \cdot \binom{l+l'}{l} \cdot (-1)^{l+l'} \cdot p^{(k-l)(n-k-l')} \\ &= p^{(k-l)(n-k)} \sum_{i=l}^{n-k+l} \binom{n}{i} \cdot \binom{i}{l} \cdot (-1)^i \cdot \left(\frac{1}{p^{k-l}} \right)^{i-l}. \end{aligned}$$

Now we make use of the l-th partial derivative with respect to X of $(1-X)^n$:

$$\frac{\delta^l}{\delta X^l}(1-X)^n = l! \cdot \sum_{i=l}^{n} \binom{n}{i} \binom{i}{l} (-1)^i X^{i-l}$$

On the other hand, $\frac{\delta^l}{\delta X^l}(1-X)^n = l! \cdot (-1)^l \binom{n}{l}(1-X)^{n-l}$. When evaluating at $X = \frac{1}{p^{k-l}}$, we get

$$(-1)^l \cdot \binom{n}{l} \cdot \left(1 - \frac{1}{p^{k-l}}\right)^{n-l} = \sum_{i=l}^{n} \binom{n}{i}\binom{i}{l}(-1)^i \left(\frac{1}{p^{k-l}}\right)^{i-l}$$

This leads to

$$T_l = p^{(k-l)(n-k)} \left[(-1)^l \cdot \binom{n}{l} \cdot \left(1 - \frac{1}{p^{k-l}}\right)^{n-l} - \sum_{i=n-k+l+1}^{n} \binom{n}{i} \cdot \binom{i}{l} \cdot (-1)^i \cdot \left(\frac{1}{p^{k-l}}\right)^{i-l}\right].$$

Summing up all the terms T_l, for any $0 \leq l \leq k$, we get the desired cardinality. □

References

[Ajt96] M. Ajtai. Generating hard instances of lattice problems (extended abstract). In *Proceedings of STOC*, pages 99–108. ACM, 1996.

[Ban93] W. Banaszczyk. New bounds in some transference theorems in the geometry of numbers. *Mathematische Annalen*, 296(1):625–635, 1993.

[BBPS19] M. Bolboceanu, Z. Brakerski, R. Perlman, and D. Sharma. Order-lwe and the hardness of ring-lwe with entropic secrets. In *Proceedings of ASIACRYPT*, pages 91–120, 2019.

[BRL20] O. Bernard and A. Roux-Langlois. Twisted-phs: Using the product formula to solve approx-svp in ideal lattices. Cryptology ePrint Archive, Report 2020/1081, 2020. https://eprint.iacr.org/2020/1081.

[CDPR16] R. Cramer, L. Ducas, C. Peikert, and O. Regev. Recovering short generators of principal ideals in cyclotomic rings. In *Proceedings of EUROCRYPT 2016*, pages 559–585. Springer, 2016.

[CDW17] R. Cramer, L. Ducas, and B. Wesolowski. Short stickelberger class relations and application to ideal-svp. In *Proceedings of EUROCRYPT 2017*, volume 10210, pages 324–348, 2017.

[CGS14] P. Campbell, M. Groves, and D. Sheperd. Soliloquy: A cautionary tale. ETSI 2nd quantum-safe crypto workshop https://docbox.etsi.org/workshop/2014/201410_CRYPTO/S07_Systems_and_Attacks/S07_Groves_Annex.pdf, 2014.

[Chu] T. Church. Math 210a: Modern algebra. Expository papers/Lecture notes. Available at: http://math.stanford.edu/~church/teaching/210A-F17/math210A-F17-hw3-sols.pdf.

[Coh96] H. Cohen. *A Course in Computational Algebraic Number Theory*. 1996.

[Cona] K. Conrad. Bilinear forms. Expository papers/Lecture notes. Available at: https://kconrad.math.uconn.edu/blurbs/linmultialg/bilinearform.pdf.

[Conb] K. Conrad. The conductor ideal. Expository papers/Lecture notes. Available at: http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/conductor.pdf.

[Conc] K. Conrad. The different ideal. Expository papers/Lecture notes. Available at: http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/different.pdf.

[Cond] K. Conrad. Factoring after dedekind. Expository papers/Lecture notes. Available at: https://kconrad.math.uconn.edu/blurbs/gradnumthy/dedekindf.pdf.

[Cone] K. Conrad. Ideal factorization. Expository papers/Lecture notes. Available at: https://kconrad.math.uconn.edu/blurbs/gradnumthy/idealfactor.pdf.

[DF91] D. S. Dummit and R. M. Foote. *Abstract Algebra*. Prentice Hall, 1991.

[DPW19] Léo Ducas, Maxime Plançon, and Benjamin Wesolowski. On the shortness of vectors to be found by the ideal-svp quantum algorithm. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part I*, volume 11692 of *Lecture Notes in Computer Science*, pages 322–351. Springer, 2019.

[GPV08] C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of STOC*, pages 197–206. ACM, 2008.

[HPS98] J. Hoffstein, J. Pipher, and J. H. Silverman. NTRU: A ring-based public key cryptosystem. In *ANTS98*, pages 267–288, 1998.

[LM06] V. Lyubashevsky and D. Micciancio. Generalized compact knapsacks are collision resistant. In *Proceedings of ICALP*, pages 144–155, 2006.

[LPR10] V. Lyubashevsky, C. Peikert, and O. Regev. On ideal lattices and learning with errors over rings. In *Proceedings of EUROCRYPT 2010*, pages 1–23, 2010.

[LPR13] V. Lyubashevsky, C. Peikert, and O. Regev. A toolkit for ring-lwe cryptography. In *Proceedings of EUROCRYPT 2013*, pages 35–54, 2013.

[LS12] A. Langlois and D. Stehlé. Worst-case to average-case reductions for module lattices. *IACR Cryptol. ePrint Arch.*, 2012:90, 2012.

[MR07] D. Micciancio and O. Regev. Worst-case to average-case reductions based on gaussian measures. *SIAM Journal on Computing*, 37(1):267–302, 2007.

[Neu99] J. Neukirch. *Algebraic Number Theory*. 1999.

[Pei10] C. Peikert. An efficient and parallel gaussian sampler for lattices. In *Annual Cryptology Conference*, pages 80–97. Springer, 2010.

[Pei16] C. Peikert. A decade of lattice cryptography. *Found. Trends Theor. Comput. Sci.*, 10(4):283–424, 2016.

[PHS19] A. Pellet-Mary, G. Hanrot, and D. Stehlé. Approx-svp in ideal lattices with preprocessing. In Yuval Ishai and Vincent Rijmen, editors, *Proceedings of EUROCRYPT 2019*, volume 11477, pages 685–716, 2019.

[PP19] C. Peikert and Z. Pepin. Algebraically structured lwe, revisited. In *Proceedings of TCC 2019*, pages 1–23, 2019.

[PR06] C. Peikert and A. Rosen. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. In *Proceedings of TCC*, pages 145–166, 2006.

[PRSD17] C. Peikert, Oded Regev, and Noah Stephens-Davidowitz. Pseudorandomness of ring-lwe for any ring and modulus. *IACR Cryptology ePrint Archive*, 2017:258, 2017.

[Reg05] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In Harold N. Gabow and Ronald Fagin, editors, *STOC*, pages 84–93. ACM, 2005. Full version in [Reg09].

[Reg09] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6), 2009.

[RSSS17] M. Rosca, A. Sakzad, D. Stehlé, and R. Steinfeld. Middle-product learning with errors. In *Proceedings of CRYPTO 2017*, volume 10403, pages 283–297, 2017.

[RSW18] M. Rosca, D. Stehlé, and A. Wallet. On the ring-lwe and polynomial-lwe problems. In *Proceedings of EUROCRYPT 2018*, pages 146–173, 2018.

[SSTX09] D. Stehlé, R. Steinfeld, K. Tanaka, and K. Xagawa. Efficient public key encryption based on ideal lattices. In *Proceedings of ASIACRYPT 2009*, pages 617–635, 2009.

[Ste08] P. Stevenhagen. The arithmetic of number rings. *Algorithmic number theory: lattices, number fields, curves and cryptography*, 44:209–266, 2008.

[vzGG13] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra (3. ed.)*. Cambridge University Press, 2013.

[Was04] L. Wasserman. *All of Statistics: A Concise Course in Statistical Inference*. Springer Texts in Statistics. Springer, 2004.