Algebraic lattices: minima, transferences and algorithms

Abstract. The reduction theory of Euclidean lattices is a classical topic in algorithmic number theory and can be thought of as an effective take on the geometry of numbers. Since the celebrated LLL algorithm, many others have achieved a range of trade-offs between their runtime and output quality (e.g. shortness of vectors) have been studied. However, their counterpart for algebraic lattices (also known as module lattices) are not as studied theoretically and algorithmically, although these objects are nowadays pervasive in cryptography, as illustrated by schemes to be standardized relying on module lattices. In this work, we aim to provide a comprehensive framework and its associated toolkit for the algorithmic processing of algebraic lattices. Recovering and unifying [20, 26], we show how our framework allows us to translate properties but also algorithm analyses directly from their description over $\mathbf{Z}$-lattices to algebraic ones. This gives new (but qualitatively equivalent to prior) reductions from shortest vector problems in algebraic lattices over orders in number fields and also provides new reductions up to now known only for $\mathbf{Z}$-lattices. Our toolkit also gives us enough tools to describe new transference results, tailored specifically for algebraic lattices and their notion of "short vectors".

1 Introduction

A lattice $\mathcal{L}$ is a free $\mathbf{Z}$-module of finite rank, endowed with a Euclidean form on its ambient real space. Equivalently, these discrete subgroups of Euclidean space. These elementary objects are surprisingly prevalent in number theory, offering geometric insights into number fields. In particular, a natural generalization of Euclidean lattices involves replacing the base ring $\mathbf{Z}$ with an order $\mathcal{O}$ of a number field $\mathbf{K}$ — that is, a subring spanning the field itself — and equipping finitely generated $\mathcal{O}$-modules with, also, the analogue of euclidean forms[1] over a field $\mathbf{K}$. Such objects are termed *algebraic lattices* or *module lattices*. They also play a central role in arithmetic geometry and Arakelov theory (see, for instance, [4] for an account of this aspect of the theory). Algebraic lattices possess a richer algebraic structure, but also come with more arithmetic intricacies: while all ideals are principal over $\mathbf{Z}$, and thus, act as pure scaling, this is generally not the case for orders. As arithmetic and geometry interleave for lattices, perhaps surprisingly, intuitive geometric notions over $\mathbf{Z}$ become more delicate to even define over orders. This is observed, for instance, in the concept of successive minima, where several, distinct notions coexist. This boils down to the apparently innocuous but core question: *what does it mean to be short?*

[1] They were introduced under the name of Humbert forms in [28].

Length in the Algebraic Setting: Linearity vs. Multiplicativity. Indeed, lattice algorithms and hard problems, particularly cryptographic ones, ask to find short elements. Over $\mathbf{Z}$, the situation has a well-understood meaning, as we use the Euclidean norm on the ambient space to define the length of an element. Rational themselves have a well-defined notion of (geometric) length: the absolute value $|x| = \sqrt{x^2}$. The situation becomes more complex over number fields as there isn't a unique way to define the length of an element in a number field. For instance, letting $\bar{x}$ be the complex conjugate of x, for an element x in a number field $\mathbf{K}$, the standard choice involves the trace norm $(\operatorname{Tr} \bar{x}x)^{1/2}$. Another less explored approach (see e.g. [20]) is to use the algebraic norm $N(\bar{x}x)^{1/2}$ The former keeps the additivity of the absolute value of $\mathbf{Z}$, whereas the latter retains its multiplicativity. This means, in particular, that the units of the field (i.e., the generalization of $\{-1, 1\}$ in $\mathbf{K}$) leave the algebraic norm invariant, but not the trace. Thus, none of them fully preserves the desirable properties of $|\cdot|$. Geometrically, these two notions can be interpreted as follows: the number field $\mathbf{K}$ can be embedded in a canonical Euclidean space, with the trace corresponding—loosely speaking—to the Euclidean length of this embedding, whereas the algebraic norm encodes the volume of the parallelepiped spanned by the element and its conjugates. While additivity is desirable for maintaining a sort of triangular inequality, multiplicativity becomes far more important when dealing with ideals. In particular, multiplicativity turns out to be a very convenient notion in any (algebraic) lattice reduction algorithms [20, 26]. This makes the algebraic norm an attractive choice.

Short Vectors or Short Lines?. In a lattice $\mathcal{L}$ over the integers, discreteness ensures the existence of (at least) an element with the smallest positive norm, *a shortest vector*. Successive minima are defined similarly (shortest elements spanning a subspace):

$$\lambda_i(\mathcal{L}) = \inf\{\max\{\|e_1\|, \ldots, \|e_i\|\} : \dim \operatorname{Span}(e_1, \ldots, e_i) = i\}.$$

For algebraic lattices, the situation becomes more subtle. When one selects the algebraic norm as a notion of size, non-principality rapidly appears as an obstacle already for the simplest of algebraic lattices, that is, ideals in $\mathbf{K}$. Indeed a shortest element may not generate the ideal, or in other words, a shortest element may not span the densest submodule. Should we aim at finding a shortest element, or a densest submodule? Can we find both? This has in particular created a dichotomy between cryptographic problems, and some reductions and studies were provided in [27, 11]. In some context, the lack of principality can be mitigated, at the cost of increasing the dimension [25]. For a more foundational approach, this leads to distinct notions of minima and thus leads to the question of the hierarchy between them.

Cryptanalytical relevance. Cryptanalyses relying on the reduction of (Euclidean) lattices have been crucial for a couple of decades and are not limited

to the realm of lattice-based cryptography, with for example the Coppersmith attack [7] against the celebrated RSA cryptosystem in certain settings. Nowadays, with the prevalence of algebraic lattice schemes as *practical* cryptosystems (`Kyber, Dillithium, Falcon, NTRU-Prime`, *etc.*, it is of utmost importance to extend these techniques to non-Euclidean rings. Indeed, most lattice-based cryptosystems proposed at the NIST Post-Quantum competition bases their security on the *assumed* hardness of reducing structured lattices, a.k.a. ideal or module lattices [23, 19]. We also note that the problem of quadratic form equivalence over number fields, founding the security of the recent proposal `Hawk` [9], naturally translates to a problem of algebraic lattice equivalence. [2] Purely algebraic reduction algorithms remains theoretical, technical to even describe. Compared to the vast, extensive litterature for the $\mathbf{Z}$ setting, few general works exist for them, especially in the cryptography community [20, 26, 25]. Dedicated algorithms exist for specific fields (cyclotomic) [18]. From a complexity theory point of view, these algorithms also provide reductions from finding short objects in algebraic lattices of large rank to finding short objects in small, fixed-rank algebraic lattices, up to a loss in the approximation factor over the shortest possible. This translates into effective estimates for fundamental constants in the geometry of numbers, but most of such constants are mostly studied for the $\mathbf{Z}$ case.

Overview of contributions

An algorithmic toolkit for algebraic lattices. We describe propose a generic framework and for algorithmic processing of algebraic lattices and lattice reduction algorithms over arbitrary number fields *and orders*, aiming to provide robust algorithmic foundations to the concept of filtration. Our goal here is to help in systematizing this aspect of the theory, borrowing from and unifying with [5] and prior cryptographic litterature [20, 26]. The standard approach to represent algebraic lattices is to rely on pseudo-bases: arithmetic data of coefficient ideals, and geometric data as a basis of the ambient space. With our formalism, the separation and interplay between these two aspects appear clearly and allow us to recover all useful properties that are well-known for $\mathbf{Z}$-lattices. We also highlight properties that are, to our knowledge, not identified in the cryptographic literature. This provides an encompassing description of results in [26]), and can act as a core toolbox for future work on algebraic lattices.

Local analyses of reduction algortihms for algebraic lattices. We apply our the framework through a detailed examination of an LLL-type algorithm and a general slide-type reduction framework applicable to any number field. Our method offers an alternative to the approach presented in [20] and extends

[2] More specifically, they rely on the average-case/hard-case, algebraically structured variants of the problems learning with errors (LWE) [29] and short integer solution (SIS) [2] problems, which have been proved to be as hard as solving worst-case instances of lattice problems, such as finding a good basis.

the findings of [26]. More precisely, we provide *local* analyses for these two algorithms: instead of showing the decrease of the global potential of the input basis, it analyses directly the behaviour on smaller sublattices as a dynamical system [17, 32]. This gives an illustration on how to use our framework to translate existing works (e.g. [32] directly to the algebraic lattices. As is common for algebraic lattices, our algorithms (and therefore reductions) rely on oracle to find shortest objects, where "short" is in the algebraic norm sense. A limitation for local analyses is that the quality of their output is expressed in a "Hermite"-way (relative to the ambient volume instead of the target shortest element). We provide an extension of the (possibly folklore) reduction of Lenstra-Schnorr-Lovasz [22] to algebraic lattices reducing "shortest object problem" to "Hermite-shortest object problem" up to a quadratic loss in the approximation factor. We also provide a reduction to the densest subline problem (so, to an object of rank 1) building upon the work of [8] to describe an oracle capable of identifying the densest submodule in any number field, using only calls to a densest line oracle. The algorithms are mostly theoretical in nature, as it is not known how to instantiate these oracles efficiently; nonetheless, we believe that this narrows the gap between the rich literature for $\mathbf{Z}$-lattices and the available tools for algebraic ones.

On transference for algebraic lattices. The celebrated transference result of Banaszczyk [3] gives a beautiful estimate of lattice minima and their dual as

$$1 \leqslant \lambda_i(\mathcal{L})\lambda_{n-i+1}(\mathcal{L}^\vee) \leqslant n.$$

Apart from using that algebraic lattices are, in particular, plain lattices, there are no results of the same nature for them. Following our framework and definition of minima, we provide a first step in this direction, under a mild but quite reasonable constraint. More specifically, we prove the following novel result, relating the lengths *in the sense of the algebraic norm* of primal and dual algebraic lattices.

Theorem 1. *Let $\mathcal{L}$ be an $\mathcal{O}$-lattice of rank n over a number field $\mathbf{K}$ of degree d, where $\mathcal{O}^\circ$ is principal. Then for all $1 \leqslant i \leqslant n$, we have:*

$$1 \leqslant \lambda_i(\mathcal{L})\lambda_{n-i+1}(\mathcal{L}^\vee) \leqslant n \cdot \Delta(\mathcal{O})^{\frac{1}{d}}.$$

The ideal $\mathcal{O}^\circ$ is called the *co-different* of the order and is involved in duality for ideals. In most relevant cases and certainly all the relevant cryptographic ones, the invertibility condition is achieved (see also Section 5). A term related to the discriminant of the order due to the pushforward to $\mathbf{Z}$. The restriction to invertible $\mathcal{O}^\circ$ is mild: in $\mathcal{O}_\mathbf{K}$ all ideals are invertible, and in most of the practical use-cases, where the order is of the form $\mathcal{O} = \mathbf{Z}[\zeta]$ and then $\mathcal{O}^\circ$ is even principal. Unfortunately, the result is still unsatisfactory in terms of tightness. For the power of two cyclotomic fields for example, which have small discriminants, we have already $\Delta(\mathcal{O}_\mathbf{K})^{1/d} = d$. Finding a tighter bound for the algebraic transference is an exciting open question we hope to challenge in future works.

Organization of the article

While we have tried to provide all proofs and details, the space constraints have forced us to defer many to appendices. We hope that our choices for the core of the text highlight the more novel or less known results or proofs. Section 2 recalls the necessary base material over number fields and their geometry. Our framework is presented in Section 3, and is followed by our local analyses for algebraic lattice reduction algorithms in Section 4. Transference results and related lemmata are dealt with in Section 5. The paper is concluded in Section 6 with the reduction from Densest Sublattices to Densest Subline.

2 Background

2.1 Algebraic number theory

Number Fields and their real algebras Let $\mathbf{K} = \mathbf{Q}(\alpha)$ be a number field of dimension d, then there exists a monic irreducible degree-d polynomial $P \in \mathbf{Z}[X]$ such that $\mathbf{K} \cong \mathbf{Q}[X]/(P)$ and $P(\alpha) = 0$. Each root of P induces a field embedding τ from $\mathbf{K}$ to either $\mathbf{R}$ or $\mathbf{C}$. Complex roots come as pairs of conjugates, giving corresponding pairs of complex embeddings $(\tau, \bar{\tau})$. We denote by $\{\sigma\}$ the collection of all real embeddings and (a choice of) one embedding by complex pair. Let $\mathbf{K}_\sigma = \mathbf{R}$ when σ is real and $\mathbf{C}$ when σ is complex. Then the real algebra $\mathbf{K_R} := \mathbf{K} \otimes_{\mathbf{Q}} \mathbf{R}$ identifies to $\prod_\sigma \mathbf{K}_\sigma$, and the *canonical embedding* $\varphi(x) = (\sigma(x))_\sigma$ embeds $\mathbf{K}$ in $\mathbf{K_R}$.

If $\Re(z)$ is the real part of a complex number z, the trace and the norm maps are defined for all $x \in \mathbf{K_R}$ respectively as

$$\mathrm{Tr}(x) = \sum_{\sigma \text{ real}} x_\sigma + 2 \sum_{\sigma \text{ complex}} \Re(x_\sigma) \quad \text{and} \quad \mathrm{N}(x) = \prod_{\sigma \text{ real}} x_\sigma \cdot \prod_{\sigma \text{ complex}} |x_\sigma|^2.$$

The trace is $\mathbf{R}$-linear and the norm is multiplicative. We also denote by $\mathbf{K}_\mathbf{R}^{++}$ the *totally positive elements* of the algebra $\mathbf{K_R}$, that is, the elements (x_σ) of $\mathbf{K_R}$ such that $x_\sigma \in \mathbf{R}_+^*$ for all σ (complex and real). For the canonical involution $x \mapsto \bar{x} = (\overline{x_\sigma})$, we have $\mathrm{Tr}(\overline{x}) = \mathrm{Tr}(x)$ and $\mathrm{N}(\overline{x}) = \mathrm{N}(x)$. Note that $\overline{\mathbf{K}} \neq \mathbf{K}$ in general. We extend the involution coordinate-wise to vectors and matrices with entries in $\mathbf{K_R}$, and additionally let $G^* := \overline{G}^t$. A useful tool is the AG inequality: $\sqrt{d}\,\mathrm{N}(\overline{v}v)^{1/d} = \mathrm{Tr}(\overline{v}v)$.

Number rings If $d = [\mathbf{K} : \mathbf{Q}]$, an *order* $\mathcal{O}$ in K is a $\mathbf{Z}$-submodule of rank d in K which is also a ring (stable under multiplication). There exists a maximal order for the inclusion, denoted $\mathcal{O}_\mathbf{K}$, also called the *ring of integers* of $\mathbf{K}$. By definition there exists a finite family $(\beta_i)_{i\in[d]} \subset \mathbf{K}$, called an integral *basis*, such that $\mathcal{O} \cong \bigoplus_{i\in[d]} \beta_i \mathbf{Z}$. The discriminant of $\mathcal{O}$ is $\Delta(\mathcal{O}) = \det(B^*B)$, where B is the matrix with columns $\varphi(\beta_i) \in \mathbf{C}^d$. The *absolute discriminant* of $\mathbf{K}$ is $\Delta_\mathbf{K} = \Delta(\mathcal{O}_\mathbf{K})$, and we have $\Delta(\mathcal{O}) = [\mathcal{O}_\mathbf{K} : \mathcal{O}]^2 \cdot \Delta_\mathbf{K}$ for all orders in $\mathbf{K}$.

Integral and fractional ideals Let $\mathcal{O}$ be an order in K. The finitely generated $\mathcal{O}$-submodules in $\mathbf{K}$ are also called $\mathcal{O}$-*fractional ideals*, and even *integral* ideals if they are included in $\mathcal{O}$. We omit the mention of $\mathcal{O}$ when the context is clear. For any fractional ideal $\mathfrak{a}$, there exists $x \in \mathbf{K}$ such that $x\mathfrak{a} \subset \mathcal{O}$. For a fixed $\mathfrak{a}$, the set of all such x's is a fractional ideal denoted by $\mathfrak{a}^{-1}$. Moreover, $\mathfrak{a}^{-1}$ can be identified to the *dual module* of $\mathfrak{a}$, that is, the set of $\mathcal{O}$-linear homomorphisms from $\mathfrak{a}$ to $\mathcal{O}$. We always have $\mathfrak{a}\mathfrak{a}^{-1} \subset \mathcal{O}$, and when it is an equality, $\mathfrak{a}$ is said to be invertible and $\mathfrak{a}^{-1}$ is the *inverse* of $\mathfrak{a}$. When $\mathcal{O} = \mathcal{O}_{\mathbf{K}}$, all ideals are invertible. An ideal generated by a single element a is called a *principal* ideal and denoted $a\mathcal{O}$. The norm of an integral ideal is $\mathrm{N}(\mathfrak{a}) = \left|\mathcal{O}/\mathfrak{a}\right|$, and we have $\mathrm{N}(a\mathcal{O}) = |\mathrm{N}(a)|$. It extends to fractional ideals as $\mathrm{N}(\mathfrak{a}) = \mathrm{N}(x\mathfrak{a})/|\mathrm{N}(x)|$. For $\mathfrak{a}, \mathfrak{b}$ two invertible ideals one has $\mathrm{N}(\mathfrak{a}\mathfrak{b}) = \mathrm{N}(\mathfrak{a})\,\mathrm{N}(\mathfrak{b})$, and thus, for invertible ideals, one has $\mathrm{N}(\mathfrak{a}^{-1}) = \mathrm{N}(\mathfrak{a})^{-1}$. As noted, we generally $\overline{\mathbf{K}} \neq \mathbf{K}$. Since the involution is compatible with algebraic operations, sets such as $\overline{\mathcal{O}}$ are orders in $\overline{\mathbf{K}}$ and we thus have a notion of $\overline{\mathcal{O}}$-ideals, the images of $\mathcal{O}$-ideals under the involution. One checks that $\mathrm{N}(\overline{\mathfrak{a}}) := |\overline{\mathcal{O}}/\overline{\mathfrak{a}}| = \mathrm{N}(\mathfrak{a})$ and for invertible ideals that $(\overline{\mathfrak{a}})^{-1} = \overline{\mathfrak{a}^{-1}} =: \mathfrak{a}^{-*}$.

Minkowski's bound. An important result of algebraic number theory is the finiteness of the class group for any order $\mathcal{O}$ in a number field (see e.g. [31, Thm. 5.4]) — that is, there are finitely many invertible ideals up to multiplications by elements of $\mathbf{K}$. The standard argument relies on the fact that, for any invertible ideal $\mathfrak{a}$, there exists $x \in \mathfrak{a}$ such that $\mathrm{N}(x) \leqslant M_{\mathcal{O}} \cdot \mathrm{N}(\mathfrak{a})$, where $M_{\mathcal{O}}$ is the *Minkowski constant* of $\mathcal{O}$ and is dependent on $\mathcal{O}$ only. From e.g. [31, Thm. 5.8]) we have $1 \leqslant M_{\mathcal{O}} \leqslant (\frac{4}{\pi})^s \cdot \frac{d!}{d^d} \cdot \Delta(\mathcal{O})^{1/2}$, where s is the number of complex embeddings of $\mathbf{K}$. If $M_{\mathcal{O}} = 1$ then $\mathcal{O}$ is principal.

Representation of algebraic numbers In this work, we will always assume that we are given any order $\mathcal{O}$ by a $\mathbf{Z}$-basis[3] $(\beta_i)_{i \leqslant d}$ "of good quality" which is always LLL-reduced for the T_2-norm. The quality of the basis ensures some control on the bit-length of algebraic integers; the next result is standard for our setting; we provide a proof for completeness in Appendix A.

Lemma 1 (Adapted from [13], Le.2 and [20], Le.2.4). *The quantity* $\log \|x\|_{T_2}$ *is bounded by a polynomial in* $\log \Delta(\mathcal{O})$ *and* $\log \max |x_i|$ *for all* $x \in \mathbf{K}$*; every* $x \in \mathcal{O}$ *can be represented with at most Poly*$(d, \log \|x\|_{T_2})$ *bits; and any fractional ideal* $\mathfrak{a}$ *can be represented with Poly*$(\log \Delta(\mathcal{O}), \log \mathrm{N}(x\mathfrak{a}), \log x)$ *bits for the smallest positive integer* x *such that* $x\mathfrak{a} \subset \mathcal{O}$*.*

2.2 Geometry over number algebras

Hermitian forms We say that a $\mathbf{K_R}$-bilinear form $g : \mathbf{K_R}^n \times \mathbf{K_R}^n \to \mathbf{K_R}$ is non-degenerate when $g(x, x) = 0$ if and only if $x = 0$, and is positive definite if

[3] For large degree number fields, computing the maximal order is usually an expensive task. Certain orders however are known explicitely, such as the natural order $\mathbf{Z}[\alpha]$.

$g(x,x) \in \mathbf{K}_{\mathbf{R}}^{++}$ for all $x \in \mathbf{K}_{\mathbf{R}}^n \setminus \{0\}$. Mildly abusing terminology, a *hermitian form* is a non-degenerate positive definite $\mathbf{K}_{\mathbf{R}}$-bilinear form g which is hermitian with respect to the involution, that is: $g(x,y) = \overline{g(y,x)}$ for any $x, y \in \mathbf{K}_{\mathbf{R}}$. In particular it satisfies $g(x, \lambda y) = g(\overline{\lambda} x, y) = \lambda g(x,y)$ for all $x, y \in \mathbf{K}_{\mathbf{R}}^n$ and $\lambda \in \mathbf{K}_{\mathbf{R}}$. This terminology is justified as a form g as above corresponds uniquely to a collection of real symmetric or complex hermitian (in the usual sense) forms $(g_\sigma)_\sigma$ defined by

$$g_\sigma(x_\sigma, y_\sigma) = \sum_{i,j} \overline{x_{i,\sigma}} y_{j,\sigma} g(b_i, b_j)_\sigma,$$

where $(b_i)_{i \leqslant n}$ is any $\mathbf{K}_{\mathbf{R}}$-basis of $\mathbf{K}_{\mathbf{R}}^n$ and $x = \sum_i x_i b_i$ and $y = \sum_i y_i b_i$. This correspondence does not depend on the choice of the basis, and in matrix form, if we let $G = [g(b_i, b_j)]_{i,j}$, we have $G^* = G$ and $g(x,y)_\sigma = (\overline{x} G y)_\sigma = \overline{x_\sigma} G_\sigma y_\sigma$. The set of hermitian forms is denoted $\mathcal{H}_n(\mathbf{K}_{\mathbf{R}})$. We also let $\|x\|_g^2 = g(x,x)$ for all $x \in \mathbf{K}_{\mathbf{R}}^n$.

We have a partial order over $\mathbf{K}_{\mathbf{R}}^{++}$: $\alpha \geqslant \beta$ when $\alpha_\sigma \geqslant \beta_\sigma$ for all σ. For ordered elements $\alpha \geqslant \beta$ in $\mathbf{K}_{\mathbf{R}}^{++}$, we have $\mathrm{N}(\alpha) \geqslant \mathrm{N}(\beta)$. Then, on each embedding, a hermitian form g is nothing but a regular hermitian form. Thus we can extend the Cauchy-Schwarz inequality to such forms: $\overline{g(x,y)} g(x,y) \leqslant \|x\|_g^2 \cdot \|y\|_g^2$ (see also Appendix A).

Orthogonality We then say that x, y are g-orthogonal (or orthogonal if the context is clear) when $g(x,y) = 0$. Given a $\mathbf{K}_{\mathbf{R}}$-subspace[4] V of $\mathbf{K}_{\mathbf{R}}^n$, we define the *orthogonal complement* of V as $V^\perp = \{y \in \mathbf{K}_{\mathbf{R}}^n \mid \forall\, x \in V, g(x,y) = 0\}$. It is a $\mathbf{K}_{\mathbf{R}}$-space of dimension $n - \dim_{\mathbf{K}_{\mathbf{R}}} V$. We denote by π_V^g the (g-)orthogonal projection (as linear map) onto V and $\pi_{V^\perp}^g = \mathrm{Id} - \pi_V$ its orthogonal complement, that is, the orthogonal projection onto $V^\perp$. We again omit superscripts when the context is clear. It is then checked that $\|\pi_{V^\perp}(x)\| = \|x - \pi_V(x)\| \leqslant \|x - x'\|$ holds for all $x \in \mathbf{K}_{\mathbf{R}}^n$ and $x' \in V$.

Gram-Schmidt process The well-known Gram-Schmidt *orthogonalization process* extends to hermitian forms. Given such a form g, let $b_1, \ldots, b_r$ be a set of $\mathbf{K}_{\mathbf{R}}$-linearly independent vectors. Define iteratively a family of pairwise g-orthogonal vectors $\widetilde{b}_1, \ldots, \widetilde{b}_r$ by

$$\widetilde{b}_1 = b_1, \text{ and } \widetilde{b}_i = b_i - \sum_{j<i} \frac{g(b_j, \widetilde{b}_i)}{g(\widetilde{b}_i, \widetilde{b}_i)} \cdot \widetilde{b}_i.$$

We will denote by $\mathsf{GSO}(B, g)$ the orthogonalization of a basis B with respect to g. It preserves the flag induced by the b_i's: for all $1 \leqslant i \leqslant r$, we have $\mathrm{span}_{\mathbf{K}_{\mathbf{R}}}(b_1, \ldots, b_i) = \mathrm{span}_{\mathbf{K}_{\mathbf{R}}}(\widetilde{b}_1, \ldots, \widetilde{b}_i)$.

[4] Technically, we mean a $\mathbf{K}_{\mathbf{R}}$-free submodule of $\mathbf{K}_{\mathbf{R}}^n$, that is, the module spanned by $\mathbf{K}_{\mathbf{R}}$-linearly independent vector $b_1, \ldots, b_m$.

3 An algorithmic toolkit for algebraic lattices

This section is devoted to the definition, core properties, and generally the concrete manipulation of algebraic lattices. In particular, we aim to illustrate the relations between pseudo-bases formalism and filtration formalism. A good additional reference is [5, Chap. 1]. We define them as finitely generated projective modules over an order $\mathcal{O}$, together with an additional metric datum — a hermitian form g. Separating the arithmetic data (the coefficients ideals) from the geometric data fits well with $\mathcal{O}$-linear transformation: the linearity guarantees that scalars in linear combinations behave as wanted. This transfers in many proofs of the following sections, where many arguments will boil down to an argument about a basis transformation, allowing to keep most useful properties known for $\mathbf{Z}$-lattices to be true as well for $\mathcal{O}$-lattices, with little changes. This also makes such proofs possibly uneventful to experts, and for this reason but for the sake of completeness, we have deferred most of them to Appendix B. We leave comments when the arithmetic part is involved and twists the proof.

Let us fix a number field $\mathbf{K}$ and an order $\mathcal{O}$ for this section. Denote by $d = [\mathbf{K} : \mathbf{Q}]$ the degree of $\mathbf{K}$ and suppose that $\mathcal{O}$ is represented by a reduced basis $(\beta_i)_{1 \leqslant i \leqslant n}$ in the sense of Lemma 1.

3.1 Algorithmic representation of modules

Let $\mathcal{M}$ be a finitely generated $\mathcal{O}$-module included in $\mathbf{K}^m$, for some integer m.

Definition 1 (Pseudo-bases). *The datum $(\mathfrak{a}_i, b_i)_{1 \leqslant i \leqslant n}$ of a collection of ideals and vectors satisfying $\mathcal{M} = \bigoplus_{i=1}^{n} \mathfrak{a}_i \cdot b_i$ is called a* pseudo-basis *of $\mathcal{M}$. The ideals $\mathfrak{a}_i$'s are called the* coefficient ideals*, and the b_i's the* basis vectors*. We also write $((\mathfrak{a}_i)_i, B)$ where B is a (column) matrix representation of the basis vectors.*

Note that the b_i's do not necessarily belong to the module they generate. The rank of a finitely generated $\mathcal{O}$-module $\mathcal{M}$ is $\operatorname{rank} \mathcal{M} = \dim_{\mathbf{K}} \operatorname{span}_{\mathbf{K}}(\mathcal{M})$, that is, the dimension of the $\mathbf{K}$-linear space spanned by $\mathcal{M}$. If a finitely generated module has a pseudo-basis, it is also the number of elements in this basis. If $\mathcal{M}$ is moreover *projective* of rank n, then there always exists a pseudo-basis, and its coefficient ideals are all *invertible* — this can also be taken as a definition for such modules. When $\mathcal{O} = \mathcal{O}_{\mathbf{K}}$, all finitely generated modules are projective. Non-projective modules are involved in Section 5 of this paper.

We can always "multiply" modules with fractional ideals. If a pseudo-basis $\mathcal{M} = \bigoplus_i \mathfrak{a}_i b_i$ is given, and $\mathfrak{b}$ is a fractional ideal, then $\mathfrak{b}\mathcal{M} = \bigoplus_i \mathfrak{b}\mathfrak{a}_i b_i$. If $\mathfrak{b}$ is not invertible, then $\mathfrak{b}\mathcal{M}$ is not projective even if $\mathcal{M}$ was.

Definition 2 (Primitivity). *Let $\mathcal{M}$ be a rank n projective $\mathcal{O}$-module. A projective submodule $\mathcal{M}'$ is said to be primitive in $\mathcal{M}$ if there exists a projective submodule $\mathcal{N}$ such that $\mathcal{M} = \mathcal{M}' \oplus \mathcal{N}$.*

Equivalently, $\mathcal{M}'$ is primitive when $\mathcal{M}/\mathcal{M}'$ is torsion-free, or when $\mathcal{M}' = \mathcal{M} \cap \mathbf{K}\mathcal{M}'$. Two pseudo-bases $(\mathfrak{a}_i, b_i)_i$ and $(\mathfrak{c}_i, d_i)_i$ generate the same projective

module if and only if there exists an invertible matrix $U = (u_{ij}) \in \mathbf{K}^{n\times n}$ such that

$$[b_1 \dots b_n]U = [d_1 \dots d_n] \quad \text{and} \quad u_{ij} \in \mathfrak{a}_i\mathfrak{c}_j^{-1}, \quad u'_{ij} \in \mathfrak{a}_i^{-1}\mathfrak{c}_j,$$

for all $1 \leqslant i, j \leqslant n$, where $U^{-1} = (u'_{ij})$. Such transformations of pseudo-bases are sometimes called admissible. Let us write $D = \det U$. By e.g. Laplace expansion formula and induction, one sees that these conditions imply $D\mathcal{O} \subset \prod_i \mathfrak{a}_i\mathfrak{c}_i^{-1}$ and $(D\mathcal{O})^{-1} \subset \prod_i \mathfrak{a}_i^{-1}\mathfrak{c}_i$. This means that $D\mathcal{O} = \prod_i \mathfrak{a}_i^{-1}\mathfrak{c}_i$ for any admissible transformation of $\mathcal{M}$. This leads to the definition of the so-called Steinitz class $\mathfrak{s} = [\prod_i \mathfrak{a}_i]$, an invariant of the isomorphism class. In particular, from [5, Lem. 1.2.20], any projective module $\mathfrak{a}_1 b_1 \oplus \dots \oplus \mathfrak{a}_n b_n$ is isomorphic to $\mathcal{O}^{n-1} \oplus \prod_i \mathfrak{a}_i$.

Now that admissible transformations are defined, we give a result to complete a basis of a projective $\mathcal{O}$-module of rank 2, given a primitive submodule of rank 1. Its associated algorithm is given and analyzed in Appendix B, for reasons of space. Astute readers will recognize [5, Algorithm 1.3.2] extended to handle $\mathcal{O}$-lattices. Another point of view sees it as a very general algorithm to complete bases of NTRU lattices, although the output is certainly not a short basis.

Lemma 2. *Let $\mathcal{M} = \mathfrak{a}_1 b_1 \oplus \mathfrak{a}_2 b_2$ be a rank 2 projective $\mathcal{O}$-module, and $(\mathfrak{c}_1, d_1)$ be one of its primitive submodules. Let $(u, v) = [b_1, b_2]^{-1} d_1$, then $(u, v) \in \mathfrak{a}_1\mathfrak{c}_1^{-1} \times \mathfrak{a}_2\mathfrak{c}_1^{-1}$, and there exists $(x, y) \in \mathfrak{a}_2^{-1}\mathfrak{c}_1 \times \mathfrak{a}_1^{-1}\mathfrak{c}_1$ such that:*

$$uy - vx = 1 \qquad \text{and} \qquad \mathcal{M} = \mathfrak{c}_1 d_1 \oplus \mathfrak{a}_1\mathfrak{a}_2\mathfrak{c}_1^{-1}(xb_1 + yb_2).$$

Moreover, there is an algorithm that runs in polynomial time in $\Delta(\mathcal{O})$ and the input bit-size to compute (x, y).

3.2 Algebraic lattices

Basic properties of algebraic lattices are described in e.g. [4], in an arguably more abstract formalism. As our objective is to design algorithms, we aim for concrete and constructive definitions in this section. We restate and prove (differently) several results of [26], and also extend their toolkit with more identifications (and proofs) of $\mathcal{O}$-lattice results with their $\mathbf{Z}$-lattice counterpart. Unless the proofs bring an unusual insight, we deferred them to Appendix B.

Definition 3. *A (hermitian) [5] $\mathcal{O}$-lattice $\mathcal{L} = (\mathcal{M}, g)$ is a finite rank projective $\mathcal{O}$-module $\mathcal{M}$ endowed with a hermitian form g over $\mathcal{M} \otimes_{\mathcal{O}} \mathbf{R} \simeq \mathbf{K}_{\mathbf{R}}^{\operatorname{rank}\mathcal{M}}$. The rank of $\mathcal{L}$ is the rank of $\mathcal{M}$.*
Equivalently, an $\mathcal{O}$-lattice is also a triple $\mathcal{L} = ((\mathfrak{a}_i, b_i)_{i\leqslant n}, g)$, where $(\mathfrak{a}_i, b_i)_i$ is a pseudo-basis of the underlying projective module.

Hermitian forms capture the notion of "semicanonical product" proposed in [26] (their main choice is the standard form $g(x, y) = \sum_i \overline{x}_i y_i$). In our context,

[5] In commutative algebra, a $\mathcal{O}$-lattice is usually a finitely generated $\mathcal{O}$-module $\mathcal{M} \subset \mathbf{K}^m$ such that $\mathbf{K}\mathcal{M} \simeq \mathbf{K}^m$. The adjective "hermitian" distinguishes between this purely algebraic notion and the geometric context of this article.

the projectivity condition ensures the existence of pseudo-bases, but also the invertibility of the coefficients ideals — several core results can fail for non-invertible ideals. Algorithmically indeed, we can also consider triples as $\mathcal{L} = ((\mathfrak{a}_i)_i, B, G)$ where B is a matrix representation of the b_i's in some basis $(e_i)_i$ of $\mathbf{K}^n$, and $G = [g(e_i, e_j)]_{ij}$. If $\mathcal{L} = (\mathcal{M}, g)$ is a $\mathcal{O}$-lattice, a sublattice is $\mathcal{L}' = (\mathcal{M}', g|_{\mathbf{K}\mathcal{M}'})$ where $\mathcal{M}'$ is a projective submodule of $\mathcal{M}$ and its form is the restriction of g to the space spanned by $\mathcal{M}'$. A sublattice is primitive when its associated submodule is primitive. Given two $\mathcal{O}$-lattices $\mathcal{L}_1 = (\mathcal{M}_1, g_1), \mathcal{L}_2 = (\mathcal{M}_2, g_2)$, the direct sum lattice is $\mathcal{L}_1 \oplus \mathcal{L}_2 := (\mathcal{M}_1 \oplus \mathcal{M}_2, (g_1 + g_2)^{1/2})$. The next result gives a standard form for algebraic lattices, which can be useful[6] in proofs. We give a proof in Appendix B based on the isomorphism $\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n \simeq \mathcal{O}^{n-1} \oplus \prod_i \mathfrak{a}_i$.

Lemma 3 (Steinitz form for a lattice). *Let $\mathcal{L} = ((\mathfrak{a}_i, b_i), g)$ be a $\mathcal{O}$-lattice of rank n. There exists a hermitian form g' such that $\mathcal{L}$ is isometric to $\big((\mathcal{O}, b_1), \ldots, (\mathcal{O}, b_{n-1}), (\prod_i \mathfrak{a}_i, b_n)), g'\big)$.*

Definition 4 (Invariants). *Let $\mathcal{L} = ((\mathfrak{a}_i, b_i)_i, g)$ an $\mathcal{O}$-lattice. Its* (co)volume *is defined as* $\mathrm{Vol}(\mathcal{L}) = \mathrm{N}(\det[g(b_i, b_j)])^{1/2} \cdot \mathrm{N}(\prod_i \mathfrak{a}_i)$. *Its* degree *is* $\deg \mathcal{L} = \log \mathrm{Vol}(\mathcal{L})$.

The volume of a $\mathbf{Z}-$lattice corresponds to the the usual definition of co-volume. Two $\mathcal{O}$-lattices $\mathcal{L}_1, \mathcal{L}_2$ are isometric when there is an isomorphism of $\mathcal{O}$-modules $\phi : \mathcal{M}_1 \to \mathcal{M}_2$ such that $\|\phi(x)\|_{g_2} = \|x\|_{g_1}$. Isometric lattices have the same volume. Using the Gram-Schmidt procedure to compute $(\tilde{b_i})_i$ from $(b_i)_i$, or a mild modification corresponding to the QR factorization, one may compute the volume of a $\mathcal{O}$-lattice as $\mathrm{Vol}(\mathcal{L}) = \prod_i \mathrm{N}(\mathfrak{a}_i)\, \mathrm{N}\left(g(\tilde{b_i}, \tilde{b_i})^{1/2}\right)$ (see also [20, 26]).

3.2.1 Successive minima, optimal bounding constants

Let $\mathcal{L}$ be a $\mathcal{O}$-lattice of rank n. Among all sublattices of rank k, an element minimizing the volume is called a *densest sublattice* (of rank k). The next result is a generalization to $\mathcal{O}$-lattices that a densest sublattice is always primitive. We give a proof by contradiction in Appendix B.

Lemma 4. *Let $\mathcal{L}' \subsetneq \mathcal{L}$ be $\mathcal{O}$-lattices, and assume that $\mathcal{L}'$ is a densest sublattice of rank $k = \mathrm{rk}\, \mathcal{L}'$. Then $\mathcal{L}'$ is primitive.*

For $i \leqslant n$, we let $\delta_i(\mathcal{L}) := \min_{\substack{\mathcal{L}' \subset \mathcal{L} \\ \mathrm{rank}\, \mathcal{L}' = i}} \mathrm{Vol}\, \mathcal{L}'$ the volume of its *densest* sublattice of rank i. We also let

$$\gamma_{\mathcal{O}}(n, i) = \sup_{\substack{\mathcal{O}\text{-lattice} \mathcal{L} \\ \mathrm{rank}\, \mathcal{L} = n}} \left(\frac{\delta_i(\mathcal{L})}{(\mathrm{Vol}\, \mathcal{L})^{\frac{i}{n}}} \right)^2.$$

When $\mathcal{O} = \mathbf{Z}$, the minimum of a Euclidean lattice is $\delta_1(\mathcal{L})$, and $\gamma_{\mathbf{Z}}(n, i)$ is Hermite or Rankin constants.

[6] Because its last coefficient ideal can be quite big, it is probably less interesting concretely.

Definition 5 (Height). *The height of $\mathcal{L}$ is $H(\mathcal{L}) = \mathrm{Vol}(\mathcal{L})^{1/nd}$. For $u \in \mathcal{L}$, the height of u is $H(u) = \min_{\mathfrak{a}u \subset \mathcal{L}} H(\mathfrak{a}u)$, where the minimum is taken over all invertible fractional ideals $\mathfrak{a}$.*

For the special case of $\mathcal{L} = (\mathfrak{a}, 1, 1)$, we have $H(\mathcal{L}) = \mathrm{N}(\mathfrak{a})^{1/d}$. Then the height is multiplicative in the following sense: if $\mathfrak{b}$ is an invertible fractional ideal, we have $H(\mathfrak{b}\mathcal{L}) = H(\mathfrak{b}) \cdot H(\mathcal{L})$. When $\mathcal{O} = \mathbf{Z}$, the height of an element is $H(u) = \mathrm{Vol}(u\mathbf{Z}) = \|u\|_g$, its Euclidean norm. We now define two notions of successive minima:

$$\lambda_i(\mathcal{L}) = \inf\left\{ \max\{H(e_1), \ldots, H(e_i)\} \ : \ \dim_{\mathbf{K}} \mathrm{Span}_{\mathbf{K}}(e_1, \ldots, e_i) = i \right\},$$
$$\nu_i(\mathcal{L}) = \inf\left\{ \max\{H(\mathcal{O}e_1), \ldots, H(\mathcal{O}e_i)\} \ : \ \dim_{\mathbf{K}} \mathrm{Span}_{\mathbf{K}}(e_1, \ldots, e_i) = i \right\},$$

where the infimum is taken over all i-uple of points in $\mathcal{L}$. In particular, the first minimum $\lambda_1(\mathcal{L})$ is also the minimum height over the elements of $\mathcal{L}$, and $H(\mathcal{O}e) = \mathrm{N}(g(e,e))^{1/2d}$. When $\mathcal{O} = \mathbf{Z}$ it is the standard notion of lattice minima, and the two notions are the same whenever $\mathcal{O}$ is a principal ring. When $\mathfrak{a}$ is not principal, we have $\lambda_i(\mathfrak{a}) < \nu_i(\mathfrak{a})$. The next result is given for completeness and is an estimate *à la* Minkowski for densest sublattices in terms of the ambient volume. It involves the Minkowski constant, and we do the proof in Appendix B relying on the Steinitz form.

Lemma 5. *Let $\mathcal{L}$ be an $\mathcal{O}$-lattice. Let $M_{\mathcal{O}}$ be the Minkowski constant of $\mathcal{O}$. Write $d_k(\mathcal{L})$ the volume of the densest free sublattice of $\mathcal{L}$. We have $d_k(\mathcal{L}) \leqslant M_{\mathcal{O}} \cdot \delta_k(\mathcal{L})$. In particular, we have $\nu_1(\mathcal{L}) \leqslant M_{\mathcal{O}} \cdot \lambda_1(\mathcal{L})$.*

3.2.2 Quotients, projections, and lifts Our goal is to extend the standard fact that for $\mathbf{Z}$-lattices $\mathcal{L}' \subset \mathcal{L}$ with $\mathcal{L}'$ primitive in $\mathcal{L}$, $\mathcal{L}/\mathcal{L}'$ is isomorphic to $\pi(\mathcal{L})$, where π is the projection on the space orthogonal to $\mathrm{span}_{\mathbf{R}}(\mathcal{L}')$. Using projection gives a concrete way to instantiate the more abstract objects involved with the quotient formalism, and we will indeed show their equivalence.

Let $\mathcal{L}' = (\mathcal{N}, g)$ be a primitive sublattice of $\subset \mathcal{L} = (\mathcal{M}, g)$, and their rank respectively be $r_n < r_m$. Let also $\mathcal{N}_{\mathbf{R}} \subset \mathcal{M}_{\mathbf{R}}$ be the $\mathbf{K}_{\mathbf{R}}$-spaces they generate (so g is hermitian over $\mathcal{M}_{\mathbf{R}}$). We first define the projection lattice in the same manner as for the $\mathbf{Z}$-case through the next result. Our proof in Appendix B uses explicit pseudo-bases coming from the primitivity of the sublattice.

Lemma 6. *Let π be the orthogonal projection from $\mathcal{M}_{\mathbf{R}}$ onto $\mathcal{N}_{\mathbf{R}}^{\perp}$. The module $\pi(\mathcal{M})$ is projective of rank $r_m - r_n$ in $\mathcal{N}_{\mathbf{R}}^{\perp}$. If $(\mathfrak{a}_i, b_i)_{r_n < i \leqslant r_m}$ is any pseudo-basis that completes $\mathcal{N}$ into $\mathcal{M}$, then $(\mathfrak{a}_i, \pi(b_i))_{i > r_n}$ is a pseudo-basis for $\pi(\mathcal{M})$.*

Now letting $g^{\perp}$ be the restriction of g to $\mathcal{N}_{\mathbf{R}}^{\perp}$, then $\pi(\mathcal{L}) := (\pi(\mathcal{M}), g^{\perp})$ is a $\mathcal{O}$-lattice of rank $r_m - r_n$. We turn now to the quotient lattice. Since $\mathcal{N}$ is primitive in $\mathcal{M}$, the quotient module $\mathcal{M}/\mathcal{N}$ is projective of rank $\mathrm{rank}\,\mathcal{M} - \mathrm{rank}\,\mathcal{N}$: a pseudo-basis is now $(\mathfrak{a}_i, b_i + \mathcal{N})_{i > r_n}$. We equip its ambient space $(\mathcal{M}/\mathcal{N}) \otimes_{\mathcal{O}} \mathbf{R}$ with the quotient norm $\|x + \mathcal{N}\|_{\mathcal{M}/\mathcal{N}} = \inf_{y \in \mathcal{N}_{\mathbf{R}}} \|x + y\|_g$. The next lemma is an extension of a standard result for $\mathbf{Z}$-lattice. Its key take is that the quotient norm

corresponds to the hermitian form $g^\perp$, see Appendix B, using the minimizing property of the orthogonal projection.

Lemma 7. *Keeping the notation, we have $\|x+\mathcal{N}\|_{\mathcal{M}/\mathcal{N}} = \|\pi(x)\|_g$ for all $x \in \mathcal{L}$. In particular, $\mathcal{L}/\mathcal{L}' := (\mathcal{M}/\mathcal{N}, \|\cdot\|_{\mathcal{M}/\mathcal{N}})$ is a $\mathcal{O}$-lattice and we have an isometry $\mathcal{L}/\mathcal{L}' \simeq \pi(\mathcal{L})$.*

We now give a concrete description of the objects involved. Without loss of generality, we can assume that $\mathcal{N} = \bigoplus_{i \leqslant r_n} \mathfrak{a}_i b_i$ and $\mathcal{M} = \bigoplus_{i \leqslant r_m} \mathfrak{a}_i b_i$. Write $B_\mathcal{N}$ the column matrix of the b_i for $i \leqslant r_n$, $B_\mathcal{M}$ the column matrix of all the b_i's, and $G = [g(b_i, b_j)]_{i,j}$ its Gram matrix. The orthogonal projection onto $\mathcal{N}_\mathbf{R}$ can be represented by the matrix $P_\mathcal{N} = B_\mathcal{N}(B_\mathcal{N}^* G B_\mathcal{N})^{-1} B_\mathcal{N}^* G$, and its orthogonal complement is $P = \mathrm{Id} - P_\mathcal{N}$ is a representation for π. The corresponding hermitian forms can then be represented by respectively the matrix $G_\mathcal{N} = P_\mathcal{N}^* G P_\mathcal{N}$ and $G^\perp = P^* G P$.

Finitely generated projective modules admit pseudo-bases, which means that given $\mathcal{L}'$ primitive in $\mathcal{L}$, we can always lift $\mathcal{O}$-linearly a pseudo-basis of $\pi(\mathcal{L})$ back to a pseudo-basis of a lattice $\ell(\pi(\mathcal{L}))$ such that $\mathcal{L}' \oplus \ell(\pi(\mathcal{L})) = \mathcal{L}$. This can be summed up by a short exact sequence as

$$0 \longrightarrow \mathcal{L}' \xrightarrow{i} \mathcal{L} \underset{\ell}{\overset{\pi}{\rightleftarrows}} \mathcal{L}/\mathcal{L}' \longrightarrow 0, \tag{1}$$

where i is the natural inclusion. This property leads to the following key component of many (algebraic) lattice-reduction algorithms since it allows to control their progress. It is well-known for $\mathbf{Z}$-lattices, and we can extend also for $\mathcal{O}$-lattices. We give a concrete proof relying on the block determinant formula and properties of orthogonal projections.

Proposition 1 (Multiplicativity of the volume). *Let $\mathcal{L} = (\mathcal{M}, g)$ be an $\mathcal{O}$-lattice, and $\mathcal{L}' = (\mathcal{N}, g|_{\mathcal{N}_\mathbf{R}})$ be a primitive sublattice. We have*

$$\mathrm{Vol}(\mathcal{L}) = \mathrm{Vol}(\mathcal{L}') \cdot \mathrm{Vol}(\pi(\mathcal{L})) = \mathrm{Vol}(\mathcal{L}') \cdot \mathrm{Vol}\left(\mathcal{L}/\mathcal{L}'\right).$$

The proof relies on Shur's complement on the matrix part of the pseudo-basis. The complete proof is given in Appendix B.

3.2.3 Duality for algebraic lattices Abstractly, the dual of a projective $\mathcal{O}$-module $\mathcal{M}$ is the module $\mathrm{Hom}_\mathcal{O}(\mathcal{M}, \mathcal{O})$ of $\mathcal{O}$-linear maps from $\mathcal{M}$ to $\mathcal{O}$. For our algorithmic purpose, it is more convenient to give a concrete representation of the dual module, and following the convention for $\mathbf{Z}$-lattice, to have it "live" in the same ambient space as the primal.

Definition 6. *Let $\mathcal{L}$ be a $\mathcal{O}$-lattice and $\mathcal{L}_\mathbf{R} = \mathcal{L} \otimes_\mathcal{O} \mathbf{R}$ its ambient space. The dual lattice is $\mathcal{L}^\vee = \{y \in \mathcal{L}_\mathbf{R} \ : \ g(y, \mathcal{L}) \in \mathcal{O}\}$.*

We can get a better description as follows. First, the basis vectors of a $\mathcal{O}$-lattice $\mathcal{L}$ or rank n are also a basis of the ambient $\mathbf{K}$-space, equipped with form g. The

dual basis for this hermitian space always exists: it is the unique $\mathbf{K}$-free family $b_1^\vee, \dots, b_n^\vee$ such that $g(b_i^\vee, b_j) = 1$ if $i = j$ and 0 otherwise. Second, from Section 2 the dual of an invertible $\mathcal{O}$-ideal $\mathfrak{a}$ is $\mathfrak{a}^{-*}$. This leads to the next lemma, which can sometimes be taken as a definition. Its proof (Appendix B) follows the same strategy as the case $\mathcal{O} = \mathbf{Z}$, but additionally needs to identify the inverse of an ideal by means of its generators (we also reprove this).

Lemma 8. *If we have a pseudo-basis for $\mathcal{L} = ((\mathfrak{a}_i, b_i)_{i\leqslant n}, g)$, its dual has a pseudo-basis as $\mathcal{L}^\vee = \left((\mathfrak{a}_i^{-*}, b_i^\vee)_{i\leqslant n}, g\right)$.*

Let B be a matrix representation for the basis vectors of $\mathcal{L}$ and G the corresponding representation for the form g. We can identify the dual basis matrix $B^\vee$ using that $(B^\vee)^* G B = \mathrm{Id}$. If B is square, so the dual basis matrix is $B^\vee = G^{-1}B^{-*}$; if B is rectangular, then $B^\vee = B(B^*GB)^{-1}$. Duality is compatible with the determinant and degree in the the following sense, extending the results known for $\mathbf{Z}$:

Lemma 9. *If $\mathcal{L}$ is a $\mathcal{O}$-lattice, then $\det \mathcal{L}^\vee = \det \mathcal{L}^{-*}$ and $\mathrm{Vol}\,\mathcal{L} \cdot \mathrm{Vol}\,\mathcal{L}^\vee = 1$.*

The proof amounts to a routine calculation of matrix products. Recall the notation $g^\perp(x, y) = g(\pi(x), \pi(y))$ when π is an orthogonal projection. We lastly recover a useful property linking dual and projections, which are standard for $\mathbf{Z}$-lattices.

Proposition 2. *Let $\mathcal{L}' \subset \mathcal{L}$ be $\mathcal{O}$-lattices with $\mathcal{L}'$ of rank r_n primitive in $\mathcal{L}$ of rank r_m. Let also $\mathcal{L}'_{\mathbf{R}} = \mathcal{L}' \otimes_{\mathcal{O}} \mathbf{R}$ be the space spanned by $\mathcal{L}'$ and π the orthogonal projection onto ${\mathcal{L}'_{\mathbf{R}}}^\perp$. Then we have $\pi(\mathcal{L})^\vee = \mathcal{L}^\vee \cap {\mathcal{L}'_{\mathbf{R}}}^\perp$, and a pseudo-basis of this lattice is $\left((\mathfrak{a}_i^{-*}, b_i^\vee)_{r_n<i\leqslant r_m}, g^\perp\right)$.*

Combined with Lemma 7, Proposition 2 also gives an isometry $(\mathcal{L}/\mathcal{L}')^\vee \simeq \mathcal{L}^\vee \cap {\mathcal{L}'_{\mathbf{R}}}^\perp$. Considering now the modules $\mathcal{L}^\vee$ and $\mathcal{L}^\vee \cap {\mathcal{L}'_{\mathbf{R}}}^\perp$, we find that their quotient is isometric to $\pi^\perp(\mathcal{L}^\vee)$, where $\pi^\perp$ is now the projection onto $\mathcal{L}'_{\mathbf{K_R}}$ (the complement to π) and another call to Proposition 2 gives that $\pi^\perp(\mathcal{L}^\vee) \simeq (\mathcal{L}')^\vee$. In other words, duality reverses the arrows in the sequence (1):

$$0 \longrightarrow \mathcal{L} \cap \mathcal{L}'_{\mathbf{R}} \longrightarrow \mathcal{L} \underset{\ell}{\overset{\pi}{\rightleftarrows}} \pi(\mathcal{L}) \longrightarrow 0 \tag{2}$$

$$0 \longleftarrow \pi^\perp(\mathcal{L}^\vee) \underset{\ell^\perp}{\overset{\pi^\perp}{\rightleftarrows}} \mathcal{L}^\vee \longleftarrow \mathcal{L}^\vee \cap {\mathcal{L}'_{\mathbf{R}}}^\perp \longleftarrow 0.$$

This contravariance will play a role in the description of the dual filtration, and give a possibly new explanation as to why one needs to take the dual basis in reverse order in certain reduction algorithms. We finish the subsection by introducing a rank 1 lattice of interest in subsequent proofs.

Definition 7. *Let $\mathcal{L}$ resp. $\mathcal{L}'$ be lattices in the same ambient hermitian space $(\mathbf{K}_{\mathbf{R}}^n, g)$. The evaluation ideal $g(\mathcal{P}, \mathcal{D})$ is the $\mathcal{O}$-ideal in $\mathbf{K}_{\mathbf{R}}$ spanned by all $g(x, x')$ for $(x, x') \in \mathcal{L} \times \mathcal{L}'$. The evaluation lattice is $(g(\mathcal{L}, \mathcal{L}'), 1)$.*

This ideal is useful to deal with orthogonality questions when non-principal ideals are involved.

Lemma 10. *For $\mathcal{P} = \mathfrak{a}u, \mathcal{D} = \mathfrak{b}v$ rank 1 lattices, we have $g(\mathcal{P}, \mathcal{D}) = \mathfrak{a}\mathfrak{b}^* \cdot g(u, v)$. If moreover there is a lattice $\mathcal{L}_0$ such that $\mathcal{P} \subset \mathcal{L}_0$ and $\mathcal{D} \subset \mathcal{L}_0^\vee$, then $g(\mathcal{P}, \mathcal{D})$ is an integral ideal, and we have $\mathrm{Vol}(g(\mathcal{P}, \mathcal{D})) \leqslant \mathrm{Vol}(\mathcal{P}) \cdot \mathrm{Vol}(\mathcal{D})$.*

Proof. The first writing follows from the bilinearity of g and the definition of the product ideal $\mathfrak{a}\mathfrak{b}^*$. Next, for $\alpha \in \mathfrak{a}$ and $\beta \in \mathfrak{b}$, we have $\alpha u \in \mathcal{L}_0$ and $\beta v \in \mathcal{L}_0^\vee$, so the definition of the dual lattice gives $g(\beta v, \alpha u) \in \mathcal{O}$ for all $(\alpha, \beta) \in \mathfrak{a} \times \mathfrak{b}$. Last, by definition of the volume, we have

$$\mathrm{Vol}(g(\mathcal{P}, \mathcal{D})) = \mathrm{N}(\mathfrak{a})\,\mathrm{N}(\mathfrak{b})\,\mathrm{N}\left(\overline{g(v,u)}g(v,u)\right)^{1/2}.$$

The result follows from Lemma 17 (Cauchy-Schwarz), ordered elements, and the multiplicativity of the algebraic norm. □

3.2.4 Filtrations of algebraic lattices To conclude this section, we define filtrations for algebraic lattices, reminiscing from [26, 10].

Definition 8. *A* filtration *of a $\mathcal{O}$-lattice $\mathcal{L}$ is a sequence $(\mathcal{L}_j)_{j \leqslant k}$ of $\mathcal{O}$-lattices satisfying the following properties:*

- $\mathcal{L}_0 = \{0\} \subset \mathcal{L}_1 \subset \ldots \subset \mathcal{L}_k = \mathcal{L}$;
- *each $\mathcal{L}_i$ is primitive in $\mathcal{L}_{i+1}$;*
- *the metric induced by g_j is the restriction to $\mathcal{L}_j \otimes_{\mathcal{O}} \mathbf{R}$ of the metric induced by g_{j+1}.*

Letting $V_i = \mathcal{L}_i \otimes_{\mathcal{O}} \mathbf{R}$, a lattice filtration corresponds a *flag* $V_0 \subset V_1 \subset \cdots \subset V_k$ of the ambient space $V = \mathcal{L} \otimes_{\mathcal{O}} \mathbf{R}$. By Section 3.2.2, we also have split short exact sequences for any $0 \leqslant i < j \leqslant k$ as

$$0 \longrightarrow \mathcal{L}_i \xrightarrow{\ i\ } \mathcal{L}_j \underset{\ell_{i,j}}{\overset{\pi_{i,j}}{\rightleftarrows}} \mathcal{L}_j/\mathcal{L}_i \longrightarrow 0.$$

From Lemma 7, we can identify $\pi_{i,j}$ to the orthogonal projection of V_j onto $V_i^\perp \cap V_j$, and the quotient lattice to $\mathcal{L}_{[i,j]} = \pi_{i,j}(\mathcal{L}_j)$ as well. In the following, we use indifferently the notation.

We define a *dual filtration* of $\mathcal{L}^\vee$ that is compatible with a given filtration of $\mathcal{L}$ and duality. The chain $\{0\} \subset V_1 \subset \ldots \subset V_k = V$ leads to a natural[7] dual chain $\{0\} \subset V_{k-1}^\perp \subset \ldots \subset V_1^\perp \subset V$. The latter fact expresses why considering "the reverse dual basis" is comfortable when dealing with lattice reduction algorithms such as slide-reduction [15] or dual BKZ [24], and leads to the definition of the dual filtration.

[7] The orthogonal complement of such a linear space is a possible representation of its dual space, that is, its space of $\mathbf{K}_{\mathbf{R}}$-linear forms.

Definition 9. *Let $(\mathcal{L}_i)_{i\leqslant k}$ be a filtration of a $\mathcal{O}$-lattice $\mathcal{L}$. For all $j \leqslant k$, a filtration of $\mathcal{L}_j$ is $(\mathcal{L}_i)_{i\leqslant j}$, and a filtration of $\mathcal{L}_j/\mathcal{L}_i$ is $(\mathcal{L}_{i+i'}/\mathcal{L}_i)_{i'\leqslant j-i}$, for $j \geqslant i$. The dual filtration for $\mathcal{L}^\vee$ is $(\mathcal{L}_i^\dagger := \mathcal{L}^\vee \cap V_{k-i}^\perp)_{i\leqslant n}$.*

As seen in the previous section, the dual filtration also corresponds to the filtration $((\mathcal{L}/\mathcal{L}_{k-i})^\vee)_{i\leqslant k}$ of $\mathcal{L}^\vee$. The dual of the dual filtration gives back the original one. Any pseudo-basis $(\mathfrak{a}_i, b_i)_i$ of $\mathcal{L}$ induces a filtration as $V_i := \mathrm{span}_{\mathbf{K_R}}(b_1, \ldots, b_i)$ and $\mathcal{L}_i = \mathcal{L} \cap V_i$. By definition of the dual basis, we have $V_{n-i}^\perp = \mathrm{span}_{\mathbf{K_R}}(b_n^\vee, \ldots, b_{n-i+1}^\vee)$ for $1 \leqslant i \leqslant n$. In other words, the *reversed* dual basis $(b_n^\vee, \ldots, b_1^\vee)$ corresponds naturally to the dual filtration. Coefficient ideals must also be reordered, and with Proposition 2, we see that $\mathcal{L}_i^\dagger = ((\mathfrak{a}_{n-j}^{-*}, b_{n-j}^\vee)_{j<i}, g_{n-i}^\perp)$, that is, it is indeed the i-th element of the filtration induced by the dual basis of $\mathcal{L}$. We conclude this toolkit by explicating the relationships in induced filtration of the dual lattice, noting that these results are well-known if $\mathcal{O} = \mathbf{Z}$.

Proposition 3. *Let $\mathcal{L} = ((\mathfrak{a}_i, b_i)_{i\leqslant n}, g)$ be a $\mathcal{O}$-lattice with induced filtration $(\mathcal{L}_i)_{i\leqslant n}$, and $V_i = \mathcal{L}_i \otimes_{\mathcal{O}} \mathbf{R}$. For all $1 \leqslant i < j \leqslant n$, let $(\mathcal{L}_j)_i^\dagger$ be the i-th element of the dual filtration $\mathcal{L}_j$. We have*

$$(\mathcal{L}_j)_i^\dagger = \pi_{j-i,j}(\mathcal{L}_j)^\vee \simeq \left(\mathcal{L}_j \big/ \mathcal{L}_{j-i}\right)^\vee,$$

where the right side is an isometry.

Proof. Since $\mathcal{L}_j$ and $\mathcal{L}_j^\vee$ live in V_j, the involved filtrations are

$$\begin{aligned} 0 \subset \quad & \mathcal{L} \cap V_1 \subset \cdots \subset \mathcal{L} \cap V_{j-1} \quad \subset \mathcal{L}_j \\ 0 \subset \mathcal{L}_j^\vee \cap (V_{j-1}^\perp \cap V_j) \subset & \cdots \subset \mathcal{L}_j^\vee \cap (V_1^\perp \cap V_j) \subset \mathcal{L}_j^\vee, \end{aligned}$$

that is $\mathcal{L}_i = \mathcal{L}_j \cap V_i$ and $\mathcal{L}_i^\dagger = \mathcal{L}_j^\vee \cap (V_{j-i}^\perp \cap V_j)$. We also note that $b_j^\vee, \ldots, b_1^\vee$ is a basis of V_j. By definition of the dual basis, $b_j^\vee, \ldots, b_{j-i+1}^\vee$ also belong to $V_{j-i}^\perp = \mathrm{span}_{\mathbf{K_R}}(b_1, \ldots, b_{j-i})^\perp$. This implies that the set $b_j^\vee, \ldots, b_{j-i+1}^\vee$ is a basis of $V_{j-i}^\perp \cap V_j$, and thus $(\mathcal{L}_j)_i^\dagger = \pi_{j-i,j}(\mathcal{L}_j)^\vee$. The isometry comes from Proposition 2. □

3.3 Controlling the size of representations for algebraic lattices

A recurrent topic deals with how to manage the size of data used to represent algebraic lattices and ensure that the number of calls to these oracles stays polynomially bounded in the input bitsize. However, a common trend in similar works (e.g. [26]) is to not put the focus on such details, since most of the presented algorithms are theoretical in nature. It is necessary in general to handle coefficients ideals when dealing with projective modules. This uses the notion of scaled pseudo-bases where the coefficients ideals and the profile of the associated basis are controlled and gives an algorithm that transforms any pseudo-basis into a scaled pseudo-basis of the same algebraic lattice. An additional notion of size-reduction for algebraic lattice is needed. Both notions of size-reduction and scaled pseudo-basis are borrowed directly from [20]. The interested reader can find more details in Appendix B.

4 Local analyses for algebraic lattices algorithms

On the one hand, *global* analyses of lattice reduction algorithms look at the whole basis of the input lattice, and estimate the progress made during the reduction as a whole through the potential of the basis. Lenstra-Lenstra-Lovàsz [21] used this approach to analyze their eponymous LLL algorithm. For $\mathcal{O}_{\mathbf{K}}$-lattices, the theoretical algorithm of [20] also takes this path, as well as the reductions described in [26] for $\mathcal{O}$-lattices.

On the other hand *local* analyses intervene on (projection of) sublattices and measure the improvements when part of their basis is replaced by a better (shorter, denser) one. This is for example the approach taken by [17, 18] for BKZ-type algorithms, or for recent analyses of slide-reduction algorithms [32]. To our knowledge, there are no versions described in these terms for $\mathcal{O}$-lattices.

In this section we provide local analyses for these algorithms thanks[8] to the framework provided in Section 3, and completing the picture. Section 4.1 analyzes such a version for a LLL-type of algorithms, while Section 4.2 deals with slide-reduction type of algorithms. Certainly, our results are qualitatively equivalent to those of [20, 26, 32], up to possibly minor constant factors, but our analyses and formalism are quite distinct. Local analysis relies on Hermite-style expression for the quality of the output, that is, expressed in terms of the volume of the input lattice. In Section 4.3 we extend all our results by providing a reduction to their "densest sublattice" equivalent (incurring a quadratic loss in the approximation factor).

4.1 A local LLL algorithm for $\mathcal{O}$-lattices

Definition 10. *For $\delta \geqslant 1$, we say that a filtration $(\mathcal{L}_i)_{i\leqslant n}$ of a $\mathcal{O}$-lattice $\mathcal{L}$ is $\delta-\mathcal{O}$-LLL reduced if for all $1 \leqslant i \leqslant n-1$, $\mathrm{Vol}(\mathcal{L}_i/\mathcal{L}_{i-1}) \leqslant \delta \cdot \mathrm{Vol}(\mathcal{L}_{i+1}/\mathcal{L}_{i-1})^{1/2}$.*

Recall from Section 3 that $\mathcal{L}_i/\mathcal{L}_j$ is isometric to the projection of $\mathcal{L}_i$ orthogonally onto the space spanned by $\mathcal{L}_j$. For $\mathbf{Z}$-lattices, the condition on the successive quotients translates into the usual decrease of Gram-Schmidt vectors. We first prove that the first element of an $\delta - \mathcal{O}$-LLL-reduced filtration solves $\delta^n - \mathrm{HDSP}^{\mathcal{O}}_{n,1}$, where n is the $\mathcal{O}$-rank of the input $\mathcal{O}$-lattice. The proof relies on several uses of Proposition 1: the volume of the quotient is the quotient of the volumes, and algorithmically we may use projected lattices thanks to Lemma 7. For example, it gives us $\mathrm{Vol}(\mathcal{L}_{i+1}/\mathcal{L}_{i-1}) = \mathrm{Vol}(\mathcal{L}_{i+1}/\mathcal{L}_i)\,\mathrm{Vol}(\mathcal{L}_i/\mathcal{L}_{i-1})$; for $\mathbf{Z}$-lattices this is nothing but the description of the volume as the product of the Gram-Schmidt vectors.

Lemma 11. *Let $\mathcal{L}$ be a $\mathcal{O}$-lattice of rank n, and $(\mathcal{L}_i)_i$ a $\delta - \mathcal{O}$-LLL reduced filtration of $\mathcal{L}$. For all $1 \leqslant i \leqslant n-1$, we have $\mathrm{Vol}(\mathcal{L}_i) \leqslant \delta^{i(n-i)}\,\mathrm{Vol}(\mathcal{L})^{i/n}$.*

[8] Our framework could also be used for global analyses, recovering the results obtained in prior works.

Proof. By assumption on the filtration, we have for all $1 \leqslant i \leqslant n-1$ that $\mathrm{Vol}(\mathcal{L}_i/\mathcal{L}_{i-1}) \leqslant \delta(\mathrm{Vol}\,\mathcal{L}_{i+1}/\mathcal{L}_{i-1})^{1/2} = \delta(\mathrm{Vol}(\mathcal{L}_i/\mathcal{L}_{i-1})\cdot\mathrm{Vol}(\mathcal{L}_{i+1}/\mathcal{L}_i))^{1/2}$, which implies the decrease of the iterated quotients:

$$\mathrm{Vol}(\mathcal{L}_i/\mathcal{L}_{i-1}) \leqslant \delta^2 \cdot \mathrm{Vol}(\mathcal{L}_{i+1}/\mathcal{L}_i). \tag{3}$$

By induction, we obtain that for all $2 \leqslant i \leqslant n$, $\mathrm{Vol}(\mathcal{L}_1) \leqslant \delta^{2(i-1)}\,\mathrm{Vol}(\mathcal{L}_i/\mathcal{L}_{i-1})$. Taking the product over all i's and using Proposition 1, we obtain

$$\mathrm{Vol}(\mathcal{L}_1)^{n-1} \leqslant \delta^{n(n-1)}\,\mathrm{Vol}(\mathcal{L}/\mathcal{L}_1),$$

which is the wanted result for $i = 1$. Let us now assume that the result is true up to $i-1$, and we will show that it is true for i. Using again Inequality (3) and induction, we find $\mathrm{Vol}(\mathcal{L}_i/\mathcal{L}_{i-1}) \leqslant \delta^{2j}\,\mathrm{Vol}(\mathcal{L}_{i+j}/\mathcal{L}_{i+j-1})$ for all $1 \leqslant j \leqslant n-i$. Taking the product for all these j and with Proposition 1, we obtain

$$\mathrm{Vol}(\mathcal{L}_i/\mathcal{L}_{i-1})^{n-i} \leqslant \delta^{(n-i+1)(n-i)}\,\mathrm{Vol}(\mathcal{L}/\mathcal{L}_i).$$

Equivalently, we have $\mathrm{Vol}(\mathcal{L}_i) \leqslant \delta^{n-i}\,\mathrm{Vol}(\mathcal{L})^{1/(n-i+1)} \cdot \mathrm{Vol}(\mathcal{L}_{i-1})^{\frac{n-i}{n-i+1}}$. Using our induction hypothesis, this implies

$$\mathrm{Vol}(\mathcal{L}_i) \leqslant \delta^{n-i}\,\mathrm{Vol}(\mathcal{L})^{1/(n-i+1)} \cdot (\delta^{(i-1)(n-i+1)}\,\mathrm{Vol}(\mathcal{L})^{(i-1)/n})^{\frac{n-i}{n-i+1}}.$$

The result follows from routine calculations with the exponents. □

Algorithm 1 below mimics the local version of LLL over $\mathbf{Z}$ — equivalently, BKZ with blocksize 2. It uses Algorithm 4 (mentioned in Lemma 2, see Appendix B) to complete a primitive line into its ambient rank 2 lattice.

Algorithm 1: Local $\mathcal{O}$-LLL

Input: A filtration $\{0\} \subset \mathcal{L}_1 \cdots \subset \mathcal{L}_{n-1} \subset \mathcal{L}$ of a rank n $\mathcal{O}$-lattice $\mathcal{L} = ((\mathfrak{a}_i, b_i)_{i\leqslant n}, g)$.
Result: An LLL-reduced filtration of $\mathcal{L}$

while *progress is done* **do**
  for $i = 2$ **to** $n-1$ **do**
    SizeReduce$(\mathcal{L}_{i+1})$
    $(\mathfrak{c}_0, c_0) \leftarrow$ **DensestSubline**$\left(\mathcal{L}_{i+1}/\mathcal{L}_{i-1}\right)$
    $((\mathfrak{c}_0', c_0'), U) \leftarrow$ **Complete**$\left(\mathcal{L}_{i+1}/\mathcal{L}_{i-1}, (\mathfrak{c}_0, c_0)\right)$
    $(\mathfrak{c}, c) \leftarrow$ **Scale**$(\mathfrak{c}_0, c_0)$, $(\mathfrak{c}', c') \leftarrow$ **Scale**$(\mathfrak{c}_0', c_0')$ and write $c = \lambda c_0$, $c' = \lambda' c_0'$
    $U \leftarrow \begin{pmatrix} \lambda u_{11} & \lambda' u_{12} \\ \lambda u_{21} & \lambda' u_{22} \end{pmatrix}$, and $[b_i, b_{i+1}] \leftarrow [b_i, b_{i+1}]U$
    $\mathcal{L}_i \leftarrow \mathcal{L}_{i-1} \oplus \mathfrak{c} b_i$, $\mathcal{L}_{i+1} \leftarrow \mathcal{L}_i \oplus \mathfrak{c}' b_{i+1}$
  end for
end while
SizeReduce$(\mathcal{L}_n)$
return $(\{0\}, \mathcal{L}_1, \ldots, \mathcal{L}_n)$

The steps **SizeReduce** and **Scale** ensure the size of the filtration is controlled. These two algorithms are also described for completeness in Appendix B, but they can certainly be ignored on a first read.

Proposition 4. *If Algorithm 1 terminates, it outputs a* $(\sqrt{\gamma_{\mathcal{O}}(2,1)})-\mathcal{O}$*-LLL reduced filtration.*

Proof. Should the algorithm finish, every successive $\mathcal{L}_i/\mathcal{L}_{i-1}$ is the densest submodule of rank 1 in the rank 2 module $\mathcal{L}_{i+1}/\mathcal{L}_{i-1}$. The claim is then implied by the definition of $\gamma_{\mathcal{O}}(2,1)$. □

To understand the termination of the algorithm, we borrow the strategy of e.g. [32] to show that after a large enough number of iterations, we can interrupt Algorithm 1 and receive a filtration which is essentially $\sqrt{\gamma_{\mathcal{O}}(2,1)}-\mathcal{O}$-LLL-reduced. This can be done through a dynamical system analysis; in fact, most of the proof is the formulation and spectral analysis of the matrix defining the system. We note that, while [18] provides a similar algorithm, their aim for performance makes the underlying dynamical system quite different.

Recall that the degree of a $\mathcal{O}$-lattice is the logarithm of its volume — this is used to turn multiplicativity into additivity and thus linear systems. Write $(\mathcal{L}_i^{(\ell)})_i$ the filtration of $\mathcal{L}$ after the ℓ-th run through the loop, and define the iterated profile vectors

$$\Pi(\mathcal{L}^{(\ell)}) = (\deg \mathcal{L}_i^{(\ell)})_{1\leqslant i\leqslant n-1}.$$

The fixed-point of the dynamical system is intuitively deduced from the "Hermite"-style of reduction as involving $\gamma_{\mathcal{O}}(2,1)$ constant.

Theorem 2. *Let* $((\mathfrak{a}_i,b_i)_i,g)$ *be a pseudo-basis of an algebraic lattice* $\mathcal{L}$ *with* $\mathrm{Vol}(\mathcal{L})=1$ *and rank* n*. Let* $\mu=(i(n-i)\log\sqrt{\gamma_{\mathcal{O}}(2,1)})_{i\leqslant n-1}$*. After* ℓ *iterations of Algorithm 1, we have*

$$\|\Pi(\mathcal{L}^{(\ell)})-\mu\|_\infty \leqslant \exp\left(-\ell\frac{\pi^2}{6(n-1)^2}\right)\|\Pi(\mathcal{L}^{(0)})-\mu\|.$$

Proof. In Appendix C we show that the updates of the filtration do not change the ambient algebraic lattice. We turn to the proof of run-time. Let us fix an index i. Thanks to Algorithm 4, we have $\mathcal{L}_{i+1}=\mathcal{L}_i\oplus\mathfrak{c}'b_{i+1}$. In other words, only $\mathcal{L}_i$ is modified to $\mathcal{L}_i'=\mathcal{L}_{i-1}\oplus\mathfrak{c}b_i$. By definition of the constants $\gamma_{\mathcal{O}}$, we have

$$\mathrm{Vol}(\mathcal{L}_i'/\mathcal{L}_{i-1})\leqslant\sqrt{\gamma_{\mathcal{O}}(2,1)}\cdot\mathrm{Vol}(\mathcal{L}_{i+1}/\mathcal{L}_{i-1})^{1/2}.$$

By properties of the volume and degree, we can then write

$$\deg(\mathcal{L}_i')-\log\sqrt{\gamma_{\mathcal{O}}(2,1)}\leqslant\frac{1}{2}\deg(\mathcal{L}_{i+1}/\mathcal{L}_{i-1})+\deg(\mathcal{L}_{i-1})=\frac{\deg\mathcal{L}_{i+1}+\deg\mathcal{L}_{i-1}}{2}. \tag{4}$$

Consider the family of operators $(\delta_i)_{i<n}$ from $\mathbf{R}^{n-1}$ to $\mathbf{R}^{n-1}$ defined as

$$\delta_1 : (v_j) \mapsto \begin{cases} \frac{v_{j+1}}{2} \text{ if } j = 1 \\ v_j \text{ else} \end{cases}, \delta_{n-1} : (v_j) \mapsto \begin{cases} \frac{v_{j-1}}{2} \text{ if } j = n-1 \\ v_j \text{ else,} \end{cases}$$

and

$$\delta_i : (v_j) \mapsto \begin{cases} \frac{v_{j-1}+v_{j+1}}{2} \text{ if } i = j \\ v_j \text{ else.} \end{cases}$$

and let $\Delta = \delta_{n-1} \circ \ldots \circ \delta_1$. Observe that for any $a > 0$, the vector $x^* = (i(n-i)a)_{i \leqslant n-1}$ is a fixed point of the dynamical system $\{x' = \Delta(x) + a(1, \ldots, 1)\}$. As seen in [18], by taking $a = \log \sqrt{\gamma_{\mathcal{O}}(2,1)}$, Inequality (4) means that the dynamical system provides at step ℓ an upper bound on the profile of $(\mathcal{L}_i^{(\ell)})_i$:

$$\|\Pi(\mathcal{L}^{(\ell)}) - \mu\|_2 \leqslant \|\Delta^\ell(\Pi(\mathcal{L}^{(0)}) - \mu)\|_2.$$

We defer the spectral analysis of Δ to Appendix C for reason of space. Informally, it is done by rewriting $\Delta = P + T$, where P, T are easier to handle separately. In particular, T is tridiagonal Toeplitz. Then, using that for all matrix M, we have $\|M\| \leqslant (\|M\|_1 \|M\|_\infty)^{1/2}$, we combine everything to obtain

$$\|\Delta\| \leqslant \|P\| + \|T\| \leqslant 1 - \frac{\pi^2}{6(n-1)^2}.$$

This finally yields us $\|\Pi(\mathcal{L}^{(\ell)}) - \mu\|_2 \leqslant \left(1 - \frac{\pi^2}{6(n-1)^2}\right)^\ell \|\Pi(\mathcal{L}^{(0)}) - \mu\|_2$, and the claim follows. □

The next corollary makes formal the intuition that after enough turns, the filtration computed by Algorithm 1 is essentially reduced.

Proposition 5. *Let $\varepsilon > 0$ and keep the notation of Theorem 2. For an input filtration $(\mathcal{L}_i)_{i \leqslant n}$, let ℓ be such that*

$$\ell \geqslant \frac{6(n-1)^2}{\pi^2} \log\left(\frac{\sqrt{n} \cdot \max_{i \leqslant n-1} |\deg(\mathcal{L}_i) - \mu_i|}{\log(1+\varepsilon)}\right).$$

Assume that Algorithm 1 is aborted after ℓ turns and outputs its current filtration $(\mathcal{L}'_i)_{i \leqslant n}$. Then we have for all $1 \leqslant i \leqslant n-1$:

$$\mathrm{Vol}(\mathcal{L}'_i)^{1/i} \leqslant (1+\varepsilon) \cdot (\gamma_{\mathcal{O}}(2,1))^{\frac{n-i}{2}} \mathrm{Vol}(\mathcal{L})^{1/n}.$$

Proof. From Proposition 2, the choice of ℓ tells us that $\|\Pi(\mathcal{L}^{(\ell)}) - \mu\|_\infty \leqslant \log(1+\varepsilon)$. The definition of μ implies the result. □

As a first corollary, we get a reduction from $\mathrm{HDSP}^{\mathcal{O}}_{n,1}$ to $\mathrm{HDSP}^{\mathcal{O}}_{2,1}$. We have $\gamma_{\mathcal{O}}(2,1) \leqslant \gamma_{\mathbf{Z}}(2d, d)$, where $d = [\mathbf{K} : \mathbf{Q}]$, since any $\mathcal{O}$-lattice is also a $\mathbf{Z}$-lattice — see also Section 5.

Corollary 1. *Let $\mathcal{L} = (\mathcal{M}, g)$ be a rank n $\mathcal{O}$-lattice in $\mathbf{K}^m$. Let $\varepsilon = 2^{-\omega(n)}$ and $\delta \geqslant 1$. Algorithm 1 solves $(1+\varepsilon) \cdot (\delta\sqrt{\gamma_{\mathcal{O}}(2,1)})^{n-1} - \mathrm{HDSP}^{\mathcal{O}}_{n,1}$ by making polynomially many (in n and the input size) calls to an $\delta\sqrt{\gamma_{\mathcal{O}}(2,1)} - \mathrm{HDSP}^{\mathcal{O}}_{2,1}$-oracle.*

Proof. Since we could only estimate the quality of the DensestSubline algorithm through a "Hermite" argument, we may as well replace it with a $\delta\sqrt{\gamma_{\mathcal{O}}(2,1)} - \mathrm{HDSP}^{\mathcal{O}}_{2,1}$ oracle. From Proposition 5 we see that we need an upper bound on $\max_{i \leqslant n-1} |\deg \mathcal{L}_i - \mu_i|$ to conclude. By the triangle inequality, this amounts to finding an upper bound on $\mu_i = i(n-i)\sqrt{\gamma_{\mathcal{O}}(2,1)}$, which is implied by one over $\gamma_{\mathbf{Z}}(2d, d)$. From [14], we have $\gamma_{\mathbf{Z}}(2d,d) \leqslant (1+\frac{d}{2})^{d\log 2 + \frac{1}{2}} \leqslant (1+\frac{d}{2})^{d+1}$ (for clarity). We also have $i(n-i) \leqslant n^2/4$ for all $1 \leqslant i \leqslant n-1$, so

$$\max_i \mu_i \leqslant \frac{n^2}{4} \cdot \frac{d+1}{2} \cdot \log\left(1 + \frac{d}{2}\right).$$

□

For $\mathbf{Z}$-lattice, the famous Gauss-Lagrange algorithm gives an instantiation of the **DensestSubline** algorithm. The corresponding constant is $\gamma_{\mathbf{Z}}(2,1) = \frac{4}{3}$. At termination, our algorithm outputs a filtration where $\mathrm{Vol}(\mathcal{L}_1) \approx \sqrt{4/3}^{n-1} \mathrm{Vol}(\mathcal{L})^{1/n}$: this is Hermite's celebrated theorem. For the general case, our algorithm is an effective generalization to $\mathcal{O}$-lattices:

Corollary 2. *For any order $\mathcal{O}$, and integers $n \geqslant 2$, we have $\gamma_{\mathcal{O}}(n,1) \leqslant \gamma_{\mathcal{O}}(2,1)^{\frac{n-1}{2}}$.*

4.2 Slide-reduction algorithms for $\mathcal{O}$-lattices

We now move to a more general setting and develop a complete family of block reduction algorithms, encompassing numerous known tradeoffs known for Euclidean lattices. Our algorithms hinge on the following informal principles. For $1 \leqslant r < d$, let $\mathcal{L} = (\mathcal{L}_i)_{i \leqslant d+r}$ be a filtration of a rank $d+r$ algebraic lattice such that we have (1) $\mathcal{L}_d$ and $\mathcal{L}/\mathcal{L}_d$ are both well-reduced; (2) $\mathrm{Vol}\,\mathcal{L}_r$ is not too much larger than $\mathrm{Vol}(\mathcal{L}_{d+r}/\mathcal{L}_d)$; then $\mathcal{L}$ will also be quite well-reduced. We express now these properties in our framework, with the belief that they simplify the exposition of [26].

Definition 11. *Let $\mathcal{L}$ be a $\mathcal{O}$-lattice of rank n and $(\mathcal{L}_i)_{i \leqslant n}$ be the filtration induced by one of its pseudo-bases. For $\gamma \geqslant 1$ and an integer $k \geqslant 1$, a complete filtration $(\mathcal{L}_i)_{i \leqslant n}$ of an algebraic lattice is said (k,γ)-Hermite reduced (or (k,γ)-HR) if $\mathrm{Vol}\,\mathcal{L}_k \leqslant \gamma \cdot (\mathrm{Vol}\,\mathcal{L})^{k/n}$.*

4.2.1 Slide-reduced bases

Definition 12. *Let $1 \leqslant r < d$ be integers. Let $(\mathcal{L}_i)_i$ be the filtration induced by a pseudo-basis of a $\mathcal{O}$-lattice $\mathcal{L}$ of rank $r+d$. The filtration is (r,γ)-twin-Hermite reduced (or (r,γ)-TwHR) if the induced filtrations of $\mathcal{L}_d$ et $\mathcal{L}_d^\dagger$ are both (r,γ)-Hermite reduced.*

This notion of reduction stems from the observation that being able to reduce lattices in rank r allows us to relate the reduction of $\mathcal{L}_d$ to that of $\mathcal{L}_{d+r}/\mathcal{L}_r$ if the dual filtration is also reduced. It leads to the following standard lemma, inspired by [1], which is core to slide-reduction-like algorithms.

Lemma 12. *Let $1 \leqslant r < d$ be integers, and $\mathcal{L}$ be a rank $r+d$ $\mathcal{O}$-lattice given by a (r,γ)-TwHR filtration $(\mathcal{L}_i)_{i\leqslant r+d}$. Then we have*

$$\operatorname{Vol}\mathcal{L}_r \leqslant \gamma^{\frac{2d}{d-r}} \cdot \operatorname{Vol}(\mathcal{L}/\mathcal{L}_d), \text{ and} \tag{5}$$

$$\gamma^{-\frac{d}{r(d-r)}} \cdot (\operatorname{Vol}\mathcal{L}_r)^{\frac{1}{r}} \leqslant (\operatorname{Vol}\mathcal{L})^{\frac{1}{r+d}} \leqslant \gamma^{\frac{d}{r(d-r)}} \cdot \left(\operatorname{Vol}\mathcal{L}/\mathcal{L}_d\right)^{\frac{1}{r}}.$$

Proof. By assumptions and using Proposition 1, we have

$$\operatorname{Vol}\mathcal{L}_r \leqslant \gamma \cdot (\operatorname{Vol}\mathcal{L}_d)^{r/d} = \gamma \cdot (\operatorname{Vol}\mathcal{L})^{r/d} \cdot \left(\operatorname{Vol}(\mathcal{L}/\mathcal{L}_d)\right)^{-r/d}, \tag{6}$$

$$\operatorname{Vol}\mathcal{L}_r^\dagger \leqslant \gamma \cdot (\operatorname{Vol}\mathcal{L}_d^\dagger)^{r/d} = \gamma \cdot (\operatorname{Vol}\mathcal{L}^\vee)^{r/d} \cdot \left(\operatorname{Vol}(\mathcal{L}^\vee/\mathcal{L}_d^\dagger)\right)^{-r/d}. \tag{7}$$

For this second inequality, Lemma 9 gives equivalently that $\operatorname{Vol}(\mathcal{L})^{r/d} \leqslant \gamma \cdot \operatorname{Vol}(\mathcal{L}^\vee/\mathcal{L}_d^\dagger)^{-r/d} \cdot \operatorname{Vol}(\mathcal{L}_r^\dagger)^{-1}$. Using Proposition 3 twice, we identify $(\mathcal{L}^\vee/\mathcal{L}_d^\dagger)^\vee$ to $\mathcal{L}_r$, and $\mathcal{L}_r^\dagger$ to $(\mathcal{L}/\mathcal{L}_d)^\vee$. Then again with Lemma 9, we rewrite Inequality (7) as

$$\operatorname{Vol}(\mathcal{L})^{r/d} \leqslant \gamma \cdot \operatorname{Vol}(\mathcal{L}/\mathcal{L}_d) \operatorname{Vol}(\mathcal{L}_r)^{r/d}. \tag{8}$$

Combining Inequalities (6) and (8), we obtain our first claim. Multiplying each side in (5) by $\operatorname{Vol}\mathcal{L}_d$ and using the reduction assumption, we obtain $\gamma^{-\frac{d}{r}} \cdot (\operatorname{Vol}\mathcal{L}_r)^{\frac{d+r}{r}} \leqslant \gamma^{\frac{2d}{d-r}} \cdot \operatorname{Vol}\mathcal{L}$, which gives the left inequality in our second claim. The last inequality follows e.g. from using Inequality (5) in (8). □

We define slide-reduced filtrations of algebraic lattices and study the density of the first elements in the filtration.

Definition 13. *For $k \geqslant 2$, a filtration $(\mathcal{L}_i)_i$ of a rank $n = kd$ algebraic lattice is (γ, r, d)-slide-reduced if the following conditions are met:*

- *for $1 \leqslant j \leqslant k$, the filtrations $(\mathcal{L}_{jd}/\mathcal{L}_{(j-1)d})_i$ are (r,γ)-Hermite reduced;*
- *for $1 \leqslant j \leqslant k-1$, the filtrations $(\mathcal{L}_{jd+r}/\mathcal{L}_{(j-1)d+r})_i^\dagger$ are (r,γ)-Hermite reduced.*

Proposition 6. *Let $1 \leqslant r \leqslant d \leqslant n = kd$ be integers, with $k \geqslant 2$. If $(\mathcal{L}_i)_i$ is a (γ, r, d)-slide-reduced filtration of a rank $n = kd$ algebraic lattice $\mathcal{L}$, we have*

$$(\operatorname{Vol}\mathcal{L}_r)^{1/r} \leqslant \gamma^{\frac{n-r}{r(d-r)}} \cdot (\operatorname{Vol}\mathcal{L})^{1/n}.$$

Proof. The conditions on the "primal" blocks give us for all $1 \leqslant j \leqslant k$:

$$\operatorname{Vol}\mathcal{L}_{(j-1)d+r}/\mathcal{L}_{(j-1)d} \leqslant \gamma \cdot \left(\operatorname{Vol}(\mathcal{L}_{jd}/\mathcal{L}_{(j-1)d})\right)^{r/d}. \tag{9}$$

Because the corresponding elements in the dual filtration are reduced as well, we know that all the algebraic lattices $\mathcal{L}_{jd+r}/\mathcal{L}_{(j-1)d}$ are (r,γ)-twin-reduced, for $1 \leqslant j \leqslant k-1$. Thanks to Lemma 12, we obtain for these j's that $\operatorname{Vol}\mathcal{L}_{(j-1)d+r}/\mathcal{L}_{(j-1)d} \leqslant \gamma^{\frac{2d}{d-r}} \cdot \operatorname{Vol}\mathcal{L}_{jd+r}/\mathcal{L}_{jd}$. Inductively combining all these inequalities yields for all $2 \leqslant j \leqslant k$:

$$\operatorname{Vol}\mathcal{L}_r \leqslant \gamma^{\frac{2(j-1)d}{d-r}} \cdot \operatorname{Vol}(\mathcal{L}_{(j-1)d+r}/\mathcal{L}_{(j-1)d}). \tag{10}$$

We now cut the whole volume in k blocks of rank d; conditions (9) then gives $\gamma^{n/r} \cdot \operatorname{Vol}\mathcal{L} = \prod_{j=1}^{k} \gamma^{d/r} \cdot \big(\operatorname{Vol}(\mathcal{L}_{jd}/\mathcal{L}_{(j-1)d})\big) \geqslant \prod_{j=1}^{k} \big(\operatorname{Vol}(\mathcal{L}_{(j-1)d+r}/\mathcal{L}_{(j-1)d})\big)^{d/r}$. Next, we use conditions (10) on the right-hand side to obtain

$$\gamma^{n/r} \cdot \operatorname{Vol}\mathcal{L} \geqslant (\operatorname{Vol}\mathcal{L}_r)^{n/r} \prod_{j=1}^{k} \gamma^{-\frac{2(j-1)d^2}{r(d-r)}}.$$

The result follows from routine calculations on the exponents. □

The next algorithm straightforwardly follows the definition for slide-reduced filtrations. We assume that we are given an oracle **DensestSublattice**$(r,\mathcal{F})$ that on input r and a filtration of an algebraic lattice $\mathcal{F}$, outputs (a filtration of) a densest sublattice $\mathcal{F}'$ of rank r. In particular, if/when Algorithm 2 terminates, we have the following.

Proposition 7. *If Algorithm 2 terminates, it outputs a* $(\sqrt{\gamma_{\mathcal{O}}(d,r)}, r, d)$*-slide-reduced filtration.*

Algorithm 2: Slide-reduction for $\mathcal{O}$-lattice

Input: A fitration $\{0\} \subset \mathcal{L}_1 \subset \cdots \subset \mathcal{L}_{n-1} \subset \mathcal{L}$ of a rank $n = kd$ algebraic lattice, and parameters $1 \leqslant r < d$.
Result: A filtration of $\mathcal{L}$

while *progress is done* **do**
  for $j = 1$ **to** k **do**
    Set $\mathcal{F} = (\mathcal{L}_{id}/\mathcal{L}_{(i-1)d})_{i \leqslant d}$
    $(A_i)_{i \leqslant r} \leftarrow$ **DensestSublattice**$(r,\mathcal{F})$
    $(B_i)_{i \leqslant r} \leftarrow$ **Lift**$((A_i)_i, \mathcal{L}_{id})$
    Update $(\mathcal{L}_{di}, (B_i)_i)$
  end for
  for $j = 1$ **to** k **do**
    Set $\mathcal{F} = (\mathcal{L}_{id+r}/\mathcal{L}_{(i-1)d+r})^{\dagger}_{i \leqslant d}$
    $(A_i)_{i \leqslant r} \leftarrow$ **DensestSublattice**$(r,\mathcal{F})$
    $(B_i)_{i \leqslant r} \leftarrow$ **Lift**$((A_i)_i, \mathcal{L}^{\vee}_{id+r})$
    Update $(\mathcal{L}^{\dagger}_{di+r}, (B_i)_i)$
  end for
end while
return $(\{0\}, \mathcal{L}_1, \ldots, \mathcal{L}_n)$

Similarly as in Section 4.1, our basis might not be exactly slide-reduced with respect to the definition. The first element in the filtration will be almost "as if" the filtration was slide-reduced. The analysis also relies on a dynamical system, which is essentially the one used in [32], however we have mildly better convergence speed by using better bounds[9] on the eigenvalues of the operator. For this reason, we defer the analysis to Appendix C.

Nevertheless, the analysis and the result revolve around the following potential vectors after ℓ iterations:

$$\mathcal{P}(\mathcal{L}^{(\ell)}) = (\deg \mathcal{L}_d^{(\ell)}, \deg \mathcal{L}_{2d}^{(\ell)}, \dots, \deg \mathcal{L}_{(k-1)d}^{(\ell)}),$$
$$\mathcal{D}(\mathcal{L}^{(\ell)}) = (\deg \mathcal{L}_r^{(\ell)}, \deg \mathcal{L}_{d+r}^{(\ell)}, \dots, \deg \mathcal{L}_{(k-1)d+r}^{(\ell)}).$$

The fixed point corresponds to the constant $\gamma_{\mathcal{O}}(d,r)$ with suitable exponents and we use the matrices

$$\mathbf{P} = \begin{bmatrix} \frac{r}{d} & & & \\ \frac{d-r}{d} & \frac{r}{d} & & \\ 0 & \frac{d-r}{d} & \frac{r}{d} & \\ & & \frac{d-r}{d} & \frac{r}{d} \\ & & & \frac{d-r}{d} \end{bmatrix} \in \mathbb{R}^{k\times(k-1)}, \text{ and } \mathbf{P}^t\mathbf{P} = \begin{bmatrix} \alpha & \beta & & \\ \beta & \alpha & \beta & \\ & \ddots & \ddots & \beta \\ & & \beta & \alpha \end{bmatrix} \in \mathbb{R}^{(k-1)\times(k-1)},$$

where $\beta = \frac{r(d-r)}{d^2}$ and $\alpha = 1 - 2\beta$. The Gram matrix of $\mathbf{P}$ is a tridiagonal Toeplitz matrix for which eigenvalues can be estimated accurately (see also the proof of Theorem 2).

Theorem 3. *Let $\mathcal{L}$ be a $\mathcal{O}$-lattice of rank kd and $\mathrm{Vol}(\mathcal{L}) = 1$. We also let $\mu = (\frac{i(k-i)d^2}{r(d-r)} \log \sqrt{\gamma_{\mathcal{O}}(d,r)})_{i\leqslant k-1}$. After ℓ iterations of Algorithm 2, we have*

$$\|\mathcal{P}(\mathcal{L}^{(\ell)}) - \mu\|_\infty \leqslant \exp\left(-\ell \frac{\pi^2 r(d-r)}{2n^2}\right) \|\mathcal{P}(\mathcal{L}^{(0)}) - \mu\|.$$

The next corollary makes formal the intuition after enough turns, the filtration computed by Algorithm 2 is essentially slide-reduced.

Corollary 3. *Let $\varepsilon > 0$ and keep the notation of Theorem 3. For an input filtration $(\mathcal{L}_i)_{i\leqslant kd}$ and parameters $1 \leqslant r < d$, let ℓ be such that*

$$\ell \geqslant \frac{2n^2}{\pi^2 r(d-r)} \log\left(\frac{\sqrt{k-1} \cdot \max_{i\leqslant k} |\deg(\mathcal{L}_i) - \mu_i|}{d \log(1+\varepsilon)}\right).$$

Assume that Algorithm 2 is aborted after ℓ turns and outputs its current filtration $(\mathcal{L}'_i)_{i\leqslant nd}$. An additional call to a **DensestSublattice** *oracle in $\mathcal{L}'_d$ gives a lattice $\mathcal{L}'_r \subset \mathcal{L}$ satisfying $\mathrm{Vol}(\mathcal{L}'_r)^{1/r} \leqslant (1+\varepsilon) \cdot (\gamma_{\mathcal{O}}(d,r))^{\frac{n-r}{2r(d-r)}} \mathrm{Vol}(\mathcal{L})^{1/n}$.*

[9] The approach of [32] relies on a transformation of the system, which then incur a loss corresponding to the condition number of the transformation compared to our approach.

Proof. From Theorem 3, the choice of ℓ tells us that $\|\mathcal{P}(\mathcal{L}^{(\ell)}) - \mu\|_\infty \leqslant d\log(1+\varepsilon)$. Using the definition of μ_1, this implies that

$$\mathrm{Vol}(\mathcal{L}'_d)^{1/d} \leqslant (1+\varepsilon)\cdot(\sqrt{\gamma_{\mathcal{O}}(d,r)})^{\frac{n-d}{r(d-r)}}\,\mathrm{Vol}(\mathcal{L})^{1/n}.$$

The last call to the oracle provides $\mathcal{L}'_r$ such that $\mathrm{Vol}(\mathcal{L}'_r) \leqslant \sqrt{\gamma_{\mathcal{O}}(d,r)}\cdot\mathrm{Vol}(\mathcal{L}'_d)^{r/d}$. The claim follows noting that $\frac{1}{r} + \frac{n-d}{r(d-r)} = \frac{n-r}{r(d-r)}$.

Our results are qualitatively equivalent to [32], and differ quantitatively only up to mild improving factors (coming from tighter bounds on the spectral norm). An additional benefit is that it handles algebraic lattices. One can also compare our results to the slide-reduction algorithms of [26], and realize that we are again quantitatively equivalent, which also means that we recover the same reductions as they provided. We also recover their prior estimates on the constant $\gamma_{\mathcal{O}}(n,d)$.

Corollary 4. *For any order $\mathcal{O}$, and integers $n > d \geqslant r \geqslant 2$, we have $\gamma_{\mathcal{O}}(n,r) \leqslant \gamma_{\mathcal{O}}(d,r)^{\frac{n-r}{2r(d-r)}}$.*

4.3 From Hermite to non-Hermite

Local analyses rely on finding shortest or densest element in the "Hermite" regime, where the size is expressed relatively to the volume of the ambient lattice.

Definition 14 ((Hermite-)Densest Sublattice Problem). *Let $\mathcal{L}$ be a $\mathcal{O}$-lattice of rank n and $\gamma \geqslant 1$ a slack factor. The Densest Sublattice Problem $\gamma - \mathrm{DSP}^{\mathcal{O}}_{n,k}$ is to find a sublattice $\mathcal{L}'$ of rank k such that $\mathrm{Vol}\,\mathcal{L}' \leqslant \gamma\cdot\delta_k(\mathcal{L})$.*
The Hermite-Densest Sublattice Problem $\gamma - \mathrm{HDSP}^{\mathcal{O}}_{n,k}$ is to find a sublattice $\mathcal{L}'$ of rank k that achieves $\mathrm{Vol}\,\mathcal{L}' \leqslant \gamma\cdot\mathrm{Vol}(\mathcal{L})^{k/n}$.

By the definition of the Minkowski constant $M_{\mathcal{O}}$, there is an immediate reduction from $(\gamma\cdot M_{\mathcal{O}}^{1/d}) - \mathrm{HDSP}^{\mathcal{O}}_{n,1}$ to $\gamma - \mathrm{DSP}^{\mathcal{O}}_{n,1}$, where $d = [\mathbf{K} : \mathbf{Q}]$. We now propose a (non-uniform) converse reduction from $\gamma^2 - \mathrm{DSP}^{\mathcal{O}}_{n,1}$ to $\gamma - \mathrm{HDSP}^{\mathcal{O}}_{n,1}$. The strategy follows that of Lenstra-Schnorr and Lovàsz [22, (1.2.21)], with an adequate modification to fit the arithmetic of $\mathcal{O}$. It is non-uniform in the sense that when assuming that we have an oracle for $\mathrm{HDSP}^{\mathcal{O}}_{n,1}$, we imply that we also are given oracles for $\mathrm{HDSP}^{\mathcal{O}}_{k,1}$ for any $k \leqslant n$ — a reasonable assumption.

Proposition 8. *Given an oracle for solving $\gamma - \mathrm{HDSP}^{\mathcal{O}}_{n,1}$ over a field $\mathbf{K}$, there exists a polytime $\gamma^2 - \mathrm{DSP}^{\mathcal{O}}_{n,1}$ algorithm making $2n$ calls to the oracle.*

Proof. Let us denote by $\mathcal{A}$ the approximate $\gamma - \mathrm{HDSP}^{\mathcal{O}}_{n,1}$ oracle. Construct $\mathcal{A}'$ as follows. Call at once the oracle on $\mathcal{L}$ and its $\mathcal{O}$-dual $\mathcal{L}^\vee$, getting as respective output $\mathcal{P}$ and $\mathcal{D}$ such that: $\mathrm{Vol}(\mathcal{P})\,\mathrm{Vol}(\mathcal{D}) \leqslant \gamma^2$. Write $\mathcal{D}^\perp_{\mathbf{R}}$ the orthogonal to the space spanned by $\mathcal{D}$, and recurse on $\mathcal{L}\cap\mathcal{D}^\perp_{\mathbf{R}}$ (call the oracle on $\mathcal{L}\cap\mathcal{D}^\perp_{\mathbf{R}}$ and its dual). Return the minimum of all the primal vectors found during these calls.

This algorithm terminates as the rank of the callee lattice is decreasing by one at each recursive step. There are two calls by step, giving the claimed $2n$. The correctness hinges on the following case study, depending on how small the dual submodule $\mathcal{D}$ can be. Let us look at the first step. If we have $\delta_1(\mathcal{L})^{-1} \leqslant \mathrm{Vol}(\mathcal{D}) \leqslant \gamma^2 \mathrm{Vol}(\mathcal{L})^{-1/n}$ ("$\mathcal{D}$ is big"), then from $\mathrm{Vol}(\mathcal{P})\,\mathrm{Vol}(\mathcal{D}) \leqslant \gamma^2$ we obtain directly the claim. Else we have $\mathrm{Vol}(\mathcal{D}) < \delta_1(\mathcal{L})^{-1}$ ("$\mathcal{D}$ is small"). Let Λ be a densest subline of $\mathcal{L}$. Since $\mathcal{D} \subset \mathcal{L}^\vee$, Lemma 10 gives

$$\mathrm{Vol}(g(\Lambda, \mathcal{D})) \leqslant \mathrm{Vol}(\Lambda)\,\mathrm{Vol}(\mathcal{D}) < 1,$$

and since the evaluation ideal is integral in this case, this means $\mathcal{P}$ and $\mathcal{D}$ are orthogonal (that is, their generating vectors are). This means that $\Lambda \subset \mathcal{L} \cap \mathcal{D}_{\mathbf{R}}^{\perp}$, and actually so is any densest subline. We may continue to the next step and proceed as the next $\mathcal{D}$ will be taken in the dual lattice $(\mathcal{L} \cap \mathcal{D}_{\mathbf{R}}^{\perp})^\vee$. Until the last n-th step, it may happen that the found $\mathcal{D}$ is always small. In this case, the last rank 1 sublattice $\mathcal{L}_n$ obtained by intersection is in fact generated by some densest subline Λ. Then $\mathrm{Vol}(\mathcal{L}_n^\vee) = \delta_1(\mathcal{L})^{-1}$, so the oracle necessarily gives us a big $\mathcal{D}_n$ with $\mathrm{Vol}(\mathcal{D}_n) \geqslant \delta_1(\mathcal{L})^{-1}$, and the corresponding $\mathcal{P}_n$ is a solution to $\gamma^2 - \mathrm{DSP}_{n,1}^{\mathcal{O}}$. In any case, we return the densest of all the computed $\mathcal{P}$'s, a solution as well. □

5 On transference for algebraic lattices

This section is dedicated to establishing new bounds for the product of the minima in an algebraic lattice and its dual, building on the concepts introduced in Section 3.2.1. These types of results are commonly referred to as transference inequalities. For $\mathbb{Z}$-lattices, an essentially tight upper bound exists, as detailed by Banaszczyk [3]:

$$1 \leqslant \lambda_i(\mathcal{L})\lambda_{n-i+1}(\mathcal{L}^\vee) \leqslant n. \tag{11}$$

Note that the λ_i here relates to the Euclidean norm over $\mathbf{R}^n$. For algebraic lattices, however, the scenario is more intricate. The analytical methods employed by Banaszczyk, especially those involving the theta functions do not carry comparable information about the height of elements as on $\mathbb{Z}$-lattices, where the Euclidean norm and the height are proportionate.

Nonetheless, we propose pushforward over $\mathbf{Z}$ to salvage Equation (11), at the cost of a loss factor depending only on the geometry of the base order. Our goal in this section is to prove the following novel transference bound relating the *algebraic* norms by mean of volumes. In the statement below, $\mathcal{O}^\circ$ denotes the *codifferent ideal* (see Definition 15).

Theorem 4. *Let $\mathcal{L}$ be an $\mathcal{O}$-lattice of rank n over a number field $\mathbf{K}$ of degree d, where $\mathcal{O}^\circ$ is principal. Then for all $1 \leqslant i \leqslant n$, we have:*

$$1 \leqslant \lambda_i(\mathcal{L})\lambda_{n-i+1}(\mathcal{L}^\vee) \leqslant \nu_i(\mathcal{L})\nu_{n-i+1}(\mathcal{L}^\vee) \leqslant n \cdot \Delta(\mathcal{O})^{\frac{1}{d}}.$$

As mentioned in Section 1, the result is unlikely tight. Already for ideals, we see that $\lambda_1(\mathfrak{a})\lambda_1(\mathfrak{a}^\vee) = 1$ for any line lattice $\mathfrak{a}$.

Descent to Z and preliminary results If $\mathcal{M}$ is a $\mathcal{O}$-module, we let $\pi^{\mathbf{Z}}(\mathcal{M})$ be the $\mathbf{Z}$-module obtained from $\mathcal{M}$ by restriction of scalars — for example, an ideal $\mathfrak{a}$ is also a rank d $\mathbf{Z}$-module $\pi^{\mathbf{Z}}(\mathfrak{a}) = \bigoplus \mathbf{Z}e_i$, for some $e_i \in \mathfrak{a}$, although often the restriction is implicit. If g is hermitian over $\mathbf{K}_{\mathbf{R}}$, the trace map induces a Euclidean form over the space $\pi^{\mathbf{Z}}(\mathcal{M}) \otimes_{\mathbf{Z}} \mathbf{R}$, with norm as $\|x\|^2_{\mathrm{Tr} \circ g} = \mathrm{Tr}(g(x, x))$. This defines the push-forward $\pi^{\mathbf{Z}}(\mathcal{L}) = (\pi^{\mathbf{Z}}(\mathcal{M}), \mathrm{Tr} \circ g)$ of the algebraic lattice $\mathcal{L} = (\mathcal{M}, g)$. As such, any $\mathcal{O}$-lattice of rank n can be seen as a Euclidean lattice of rank nd, and we get $\gamma_{\mathcal{O}}(n, k) \leqslant \gamma_{\mathbf{Z}}(nd, kd)$. The AG inequality can be restated as $\sqrt{d} \cdot H(\mathcal{O}v) = \|v\|_{\pi^{\mathbf{Z}}(\mathcal{L})}$.

As a regular Euclidean lattice, the pushforward over $\mathbf{Z}$ has a volume on its own, which is related to the volume of the original lattice $\mathcal{L}$:

Lemma 13. *Let $\mathcal{L}$ be $\mathcal{O}$-lattice of rank n. Then we have* $\mathrm{Vol}(\pi^{\mathbf{Z}}(\mathcal{L})) = \Delta(\mathcal{O})^{\frac{n}{2}} \mathrm{Vol}(\mathcal{L})$.

This result is sometimes stated without proof; we provide one in Appendix D, relying on the Steinitz form and the Gram-Schmidt orthogonalization. The discriminant appears when identifying $\mathcal{O}$ to its $\mathbf{Z}$-basis via the pushforward.

We first aim to estimate the loss that occurs when doing a pushforward to $\mathbb{Z}$. First, let us prove an elementary result regarding the dimension of pushforward/scalar extension of vector spaces.

Lemma 14. *Let $\mathbf{K}$ be a number field of degree d. For any $\mathbf{Q}$-free family $(v_1, \ldots, v_{id+1})$ of a $\mathbf{K}$-vector space, we have: $i + 1 \leqslant \dim \mathit{Span}_{\mathbf{K}}(v_1, \ldots, v_{id+1}) \leqslant id + 1$.*

The proof is elementary by linear algebra and done in Appendix D. We now show the following result relating minima under scalar restriction, thanks to the AG inequality (see Appendix D). Note that the first deals with a mix of algebraic and Hermitian norms, while the second uses an euclidean norm.

Proposition 9. *Let $\mathcal{O}$ be an order in a number field $\mathbf{K}$ of degree d. For any $\mathcal{O}$-lattice $\mathcal{L}$ of rank n, we have: $\nu_{i+1}(\mathcal{L}) \leqslant \frac{1}{\sqrt{d}} \lambda_{id+1}(\pi^{\mathbf{Z}}(\mathcal{L}))$.*

Duality under scalar restriction We now describe the dual lattice under scalar restriction, noting that this is *not* the dual of the restriction itself. The missing elements are collected in a module called the codifferent.

Definition 15. *Let $\mathfrak{a}$ be a fractional ideal in an order $\mathcal{O}$ of a number field $\mathbf{K}$. The* co-different *of $\mathfrak{a}$ is the fractional ideal $\mathfrak{a}^\circ = \{x \in \mathbf{K} \ : \ \mathrm{Tr}(\overline{x}\mathfrak{a}) \subset \mathbf{Z}\}$. For a $\mathcal{O}$-lattice $\mathcal{L} = (\mathcal{M}, g)$, we call $\mathcal{M}^\circ := \mathcal{O}^\circ \cdot \mathcal{M}^\vee$ its co-different module $\mathcal{L}^\circ := \pi_\star(\mathcal{M}^\circ)$ its co-different lattice.*

One can see that $\mathfrak{a}^\circ$ is the dual of $\mathfrak{a}$ seen as a $\mathbf{Z}$-module (or as a "plain" lattice with hermitian form $(x, y) \mapsto \mathrm{Tr}(\overline{x}y)$). The ideal $\mathcal{O}^\circ$ encodes the gap between $\mathcal{O}$-duality and $\mathbf{Z}$-duality: for all invertible ideal $\mathfrak{a}$, we have $\mathfrak{a}^\circ = \mathfrak{a}^{-*}\mathcal{O}^\circ$, $\mathfrak{a}^{\circ\circ} = \mathfrak{a}$. If we know a pseudo-basis $\mathcal{M} = \bigoplus_i \mathfrak{a}_i b_i$, then we see that $\mathcal{M}^\circ = \bigoplus_i \mathfrak{a}_i^\circ b_i^\vee$. Importantly, we cannot say that $\mathcal{M}^\circ$ is projective anymore, since there is no

reason *a priori* that all $\mathfrak{a}_i^\circ$ are invertible since $\mathcal{O}^\circ$ may not be invertible[10] itself. When $\mathcal{O} = \mathcal{O}_\mathbf{K}$, all ideals are invertible, and thus so is $\mathcal{O}^\circ$.

If $\mathcal{O}$ is non-maximal, $\mathcal{O}^\circ$ may still be invertible. This is the case when $\mathcal{O} = \mathbf{Z}[\alpha]$ is the "equation" order of $\mathbf{K} = \mathbf{Q}[\alpha]$, where it is well-known that $\mathcal{O}^\circ = f'(\alpha)^{-1}\mathcal{O}$, where f is a defining polynomial for $\mathbf{K}$. An important example is that of cyclotomic fields. In both cases, $\mathcal{M}^\circ$ is projective and could be defined as a $\mathcal{O}$-lattice. In any case, to keep coherent definitions, we only define the co-different lattice as a $\mathbf{Z}$-lattice, where this is not a concern anymore. The descent to $\mathbf{Z}$-duality with $\mathcal{O}^\circ$ then extends to $\mathcal{O}$-lattices as follows.

Lemma 15. *Let $\mathcal{L} = (\mathcal{M}, g)$ be a $\mathcal{O}$-lattice. Then we have $\mathcal{L}^\circ = \pi^\mathbf{Z}(\mathcal{L})^\vee = (\pi^\mathbf{Z}(\mathcal{M}^\circ), \mathrm{Tr} \circ g)$.*

The proof can be done by identifying properly defined dual bases, see Appendix D. Invertible ideals are almost principal[11] in a certain sense, so multiplying by an invertible ideal should act essentially as a scaling. This is apparent in the next lemma.

Proposition 10. *Let $\mathfrak{a}$ be an invertible fractional $\mathcal{O}$-ideal and $\mathcal{L}$ be a $\mathcal{O}$-lattice of rank n. For all $1 \leqslant i \leqslant n$, we have $\lambda_i(\mathfrak{a}\mathcal{L}) = \lambda_1(\mathfrak{a})\lambda_i(\mathcal{L})$ and $\nu_i(\mathfrak{a}\mathcal{L}) = \nu_1(\mathfrak{a})\nu_i(\mathcal{L})$. We also have*

$$\lambda_i(\mathfrak{a}\mathcal{L}) \leqslant \min(\lambda_1(\mathfrak{a})\nu_i(\mathcal{L}), \nu_1(\mathfrak{a})\lambda_i(\mathcal{L})) \leqslant \max(\lambda_1(\mathfrak{a})\nu_i(\mathcal{L}), \nu_1(\mathfrak{a})\lambda_i(\mathcal{L})) \leqslant \nu_1(\mathfrak{a}\mathcal{L}).$$

Proof. Let $L_1, \ldots, L_i \subset \mathcal{L}$ such that $H(L_i) = \lambda_i(\mathcal{L})$ and let $L_i = \mathfrak{b}_i x_i$ be a pseudo-basis. Then $\mathfrak{a}L_i \subset \mathfrak{a}\mathcal{L}$, and they still span a $\mathbf{K}$-space of dimension i. We thus have $\lambda_i(\mathfrak{a}\mathcal{L}) \leqslant \mathrm{Vol}(\mathfrak{a}\mathfrak{b}_i x_i)^{1/d} = \mathrm{N}(\mathfrak{a})^{1/d} H(L_i) = \lambda_1(\mathfrak{a})\lambda_i(\mathcal{L})$. For the reverse, assume now $L_1, \ldots, L_i \subset \mathfrak{a}\mathcal{L}$ reach the $\lambda_i(\mathfrak{a}\mathcal{L})$. Since $\mathfrak{a}$ is invertible, we see that $\mathfrak{a}^{-1}L_i \subset \mathcal{L}$, or in other words, we can write $L_i = \mathfrak{a}L_i'$ for some $L_i' \subset \mathcal{L}$. Then we have $\lambda_i(\mathfrak{a}\mathcal{L}) = \lambda_1(\mathfrak{a})H(L_i') \geqslant \lambda_1(\mathfrak{a})\lambda_i(\mathcal{L})$. Now we turn to the ν_i's. Take $\alpha_1 x_1, \ldots, \alpha_i x_i$ reaching the $\nu_i(\mathfrak{a}\mathcal{L})$. We get

$$\nu_i(\mathfrak{a}\mathcal{L}) = H(\mathcal{O}\alpha_i x_i) = \mathrm{N}(g(\alpha_i x_i, \alpha_i x_i))^{\frac{1}{2d}} = \mathrm{N}(\alpha_i)^{1/d} H(\mathcal{O}x_i) \geqslant \nu_1(\mathfrak{a})\nu_i(\mathcal{L}). \tag{12}$$

Now take $a \in \mathfrak{a}$ of minimal algebraic norm, and $x_1, \ldots, x_i$ $\mathbf{K}$-linearly independent reaching the successive minima $\nu_i(\mathcal{L})$. Since $\alpha x_i \in \mathfrak{a}\mathcal{L}$ and these elements are $\mathbf{K}$-linearly independent, we readily compute $H(\mathcal{O}\alpha x_i) = \mathrm{N}(\alpha)^{1/2d}\nu_i(\mathcal{L}) \geqslant \nu_i(\mathfrak{a}\mathcal{L})$. This gives the second equality. For some x giving the i-th minima of $\mathcal{L}$, we have by definition $\nu_i(\mathcal{L}) = H(\mathcal{O}x) \geqslant H(x) \geqslant \lambda_i(\mathcal{L})$. The last claims follow combining the previous inequality with (12), or $\nu_1(\mathfrak{a}) \geqslant \lambda_1(\mathfrak{a})$, then both. □

[10] It is unlikely to be invertible in general, since the potential inverse $\mathcal{D}_\mathcal{O} = \mathcal{O}^{-\circ}$ is contained in the so-called *conductor ideal* $\mathcal{C}_\mathcal{O}$ (see e.g. [6, 30]). Any non-principal ideal which is not coprime to the conductor is not invertible. For $\mathcal{O}^\circ$, we have $\mathcal{O} \subset \mathcal{O}_\mathbf{K} \subset \mathcal{O}_\mathbf{K}^\circ \subset \mathcal{O}^\circ$, so if $x \in \mathcal{D}_\mathcal{O}$, then $x\mathcal{O}^\circ \subset \mathcal{O}$ which implies $x\mathcal{O}_\mathbf{K} \subset \mathcal{O}$ and thus $x \in \mathcal{C}_\mathcal{O}$.

[11] Locally at any prime ideal $\mathfrak{p}$, they are.

Let $(\mathfrak{a}_i, b_i)_{i\leqslant n}$ be a basis of a projective module $\mathcal{M}$. The finitely generated module $\mathcal{M}^\circ$ equipped with the same form as $\mathcal{L}$ is discrete in $\mathbf{K}_\mathbf{R}^n$. However, the resulting object $\mathcal{L}' = (\mathcal{O}^\circ\mathcal{M}^\vee, g)$ is not a $\mathcal{O}$-lattice as we defined it. Nevertheless, it has successive minima (from discreteness) and is given by a basis. The key take of the next result is that pushing duality to $\mathbf{Z}$ expresses as a scaling.

Corollary 5. *Let $\mathcal{O}$ be an order in a number field $\mathbf{K}$ of absolute degree d with $\mathcal{O}^\circ$ invertible. For all $\mathcal{O}$-lattice $\mathcal{L}$ of rank n, we have for $1 \leqslant i \leqslant n$:*

$$\sqrt{d}\cdot\lambda_{i+1}(\mathcal{L}^\vee) \leqslant \nu_{id+1}(\pi^\mathbf{Z}(\mathcal{L})^\vee)\Delta(\mathcal{O})^{\frac{1}{d}},$$
$$\sqrt{d}\cdot\nu_{i+1}(\mathcal{L}^\vee) \leqslant \nu_{id+1}(\pi^\mathbf{Z}(\mathcal{L})^\vee)\Delta(\mathcal{O})^{\frac{1}{d}}.$$

Proof. From Proposition 10 we have $\lambda_{i+1}(\mathcal{L}') = \lambda_1(\mathcal{O}^\circ)\lambda_{i+1}(\mathcal{L}^\vee)$. Using that $\lambda_i \leqslant \nu_i$ for all $\mathcal{O}$-lattices, this yields

$$\lambda_{i+1}(\mathcal{L}^\vee) = \frac{\lambda_{i+1}(\mathcal{L}')}{\lambda_1(\mathcal{O}^\circ)} \leqslant \frac{\nu_{id+1}(\mathcal{L}^\circ)}{\sqrt{d}\lambda_1(\mathcal{O}^\circ)} = \frac{\nu_{id+1}(\pi^\mathbf{Z}(\mathcal{L})^\vee)}{\sqrt{d}\lambda_1(\mathcal{O}^\circ))}, \tag{13}$$

where we also use Proposition 9 and $\pi^\mathbf{Z}(\mathcal{L}') = \mathcal{L}^\circ$, and the second equality is Lemma 15. The first inequality is deduced from $\mathrm{N}(\mathcal{O}^\circ) = \Delta(\mathcal{O})^{-1}$ when $\mathcal{O}^\circ$ is invertible. Proposition 10 also gives $\nu_{i+1}(\mathcal{L}') = \nu_1(\mathcal{O}^\circ)\nu_{i+1}(\mathcal{L}^\vee)$, and we recover the middle inequality in (13) using $\lambda_1(\mathcal{O}^\circ) \leqslant \nu_1(\mathcal{O}^\circ)$ (this is independent of the invertibility of $\mathcal{O}^\circ$). □

We note a dissymmetry in these inequalities, one mixing λ and ν and not the other. Lastly, we conclude with our new transference bound, highlighting again that they relate algebraic norms and not vector lengths. The lower bound can be obtained purely with $\mathcal{O}$-means, but we rely on Corollary 5 and therefore on Banaszczyk's original result for the upper bound.

Proof (of Theorem 4). We start with the lower bound over the λ_i's. Let $\mathcal{P}_j = \mathfrak{a}_j u_j$, resp. $\mathcal{D}_j = \mathfrak{b}_j v_j$ be rank 1 sublattices respectively reaching the i first minima of $\mathcal{L}$, resp. the $n-i+1$ first minima of $\mathcal{L}^\vee$. By definition, $V = \mathrm{span}_\mathbf{K}(v_j)_j$ has rank $n-i+1$ and $U = \mathrm{span}_\mathbf{K}(u_j)_j$ has rank i, so the intersection has rank at least 1. Taking $x = \sum_{j\leqslant i} x_j u_j = \sum_{j\leqslant n-i+1} y_j v_j \neq 0$ in the intersection, we thus have $g(x,x) \neq 0$ as well, implying that there are two indices j,k such that $g(v_k, u_j) \neq 0$. If we let $E = g(\mathcal{P}_j, \mathcal{D}_k)$ be the evaluation lattice of $\mathcal{P}_j$ and $\mathcal{D}_k$, we can write

$$1 \leqslant \mathrm{Vol}(E) \leqslant \mathrm{Vol}(\mathcal{D}_k)\,\mathrm{Vol}(\mathcal{P}_j) \leqslant \lambda_{n-i+1}(\mathcal{L}^\vee)\lambda_i(\mathcal{L}) \leqslant \nu_{n-i+1}(\mathcal{L}^\vee)\nu_i(\mathcal{L}),$$

where the second equality is by integrality of M, the third inequality comes from Lemma 10, and the last one because $\lambda_i \leqslant \nu_i$ for any lattice. The upper bound comes from two applications of Corollary 5, then Banaszczyk's transference bound [3] for $\mathbf{Z}$-lattice of rank nd:

$$\lambda_i(\mathcal{L})\lambda_{n-i+1}(\mathcal{L}^\vee) \leqslant d^{-1}\Delta(\mathcal{O})^{\frac{2}{d}}\cdot\lambda_{id}(\pi^\mathbf{Z}(\mathcal{L}))\cdot\lambda_{nd-id+1}(\pi^\mathbf{Z}(\mathcal{L})^\vee) \leqslant \frac{nd}{d}\Delta(\mathcal{O})^{\frac{2}{d}}.$$

□

6 The densest-sublattice algorithm over number fields

In this final section, we dig into the details of the densestSublattice oracle and show how to reduce this to a line search. This reduction is inspired by the reduction for Euclidean lattices introduced by Dadush and Micciancio in [8]. We denote by enumerator$(\mathcal{L}, T)$ the subline enumerator, which is an oracle giving all the sublines of its input lattice of degree bounded by T.

Algorithm 3: densest-sublattice

Input: An $\mathcal{O}$-lattice $\mathcal{L}$, an integer k
Result: A sublattice $\mathcal{L}' \subset \mathcal{L}$ of rank k of minimal degree

if $k = 0$ **then return** $\{0\}$
$S \leftarrow$ **enumerate**$(\gamma_{\mathcal{O}}(n,1)\deg(\mathcal{L}))$; $S_k \leftarrow$ **enumerate**$(k|\Delta(\mathcal{O})|^{\frac{1}{d}} \cdot \gamma_{\mathcal{O}}(n,1)\deg(\mathcal{L}))$
$W \leftarrow \sum_{\mathcal{V}\in S} \mathcal{V}$
if $\dim W_{\mathbf{R}} < k$ **then**
  $W \leftarrow V +$ **densest-sublattice** $\left(\mathcal{L}/W, k - \mathrm{rk}(W)\right)$
end if
for $T \subset S_k, |T| = k$ **do**
  $W' \leftarrow \sum_{\mathcal{T}\in T} \mathcal{T}$
  if $(\mathrm{rk}(W') = k \wedge \mathrm{rk}(W) < k) \vee (\deg(W') < \deg(W))$ **then** $W \leftarrow W'$
end for
return W

The correctness of this search algorithm relies on the following results, which allows us to only search for a generating family of the densest sublattice into lines of volume only slightly bigger than $k\lambda_1$.

Lemma 16. *Let $\mathcal{L}$ be a rank n $\mathcal{O}$-lattice and $\mathcal{L}_k \subset \mathcal{L}$ be one of its k-dimensional sublattice of minimal degree. Let $\mathcal{V} \subset \mathcal{L}$ be any subline, then either $\mathcal{V} \subset \mathcal{L}_k$ or $\deg(\mathcal{V}) \cdot \lambda_1(\mathcal{L}_k^\vee) \geqslant 1$.*

Proof. Let $\mathcal{D}$ be a subline of minimal degree of the dual sublattice $\mathcal{L}_k^\vee$ and set $H = \left(\mathcal{L}_k^\vee/\mathcal{D}\right)^\vee$, which can be canonically identified with a sublattice of rank $k-1$ in $\mathcal{L}_k$ by Proposition 2. Let $\mathcal{V}$ be any subline *not included in* $\mathcal{L}_k$. Then $H_v = H + \mathcal{V}$ is a sublattice of rank k in $\mathcal{L}$ and we have by minimality of $\mathcal{L}_k$ that it volume $\mathrm{Vol}(\mathcal{L}_k)$ is upper bounded by:

$$\mathrm{Vol}(H_v) \leqslant \mathrm{Vol}(H)\,\mathrm{Vol}(\mathcal{V}) = \left(\frac{\mathrm{Vol}(\mathcal{L}_k^\vee)}{\mathrm{Vol}(\mathcal{D})}\right)^{-1} \mathrm{Vol}(\mathcal{V}) = \mathrm{Vol}(\mathcal{L}_k)\,\mathrm{Vol}(\mathcal{D})\,\mathrm{Vol}(\mathcal{V}).$$

Hence, we have $\mathrm{Vol}(\mathcal{V})\,\mathrm{Vol}(\mathcal{D}) \geqslant 1$, and we conclude by taking the $\frac{1}{[\mathbf{K}:\mathbf{Q}]}$-th power of both side.

Using the transference bound of Lemma 4 , we find that:

Corollary 6. *Let $\mathcal{L}$ be a rank n $\mathcal{O}$-lattice over a field of degree d, then either the densest sublattice of rank k $\mathcal{L}_k \subset \mathcal{L}$ contains all shortest sublines of $\mathcal{L}$ or $\lambda_k(\mathcal{L}_k) \leqslant k|\Delta(\mathcal{O})|^{\frac{1}{d}}\lambda_1(\mathcal{L})$.*

From this point, the algorithm is quite straightforward: either we are in the the first case of the corollary and enumerating over all vectors of height $\lambda_1(\mathcal{L})$ suffices to generate the densest sublattice, either we are in the second case, and we need to enumerate all vectors of height $|\Delta(\mathcal{O})|^{\frac{1}{d}}k\lambda_1(\mathcal{L})$ and find a correct subset of size k which is one of its bases. All in all, this translates into the pseudo code of Algorithm 3.

Proposition 11. *Let $T(\mathcal{O}, n, k) = k|\Delta(\mathcal{O})|^{\frac{1}{d}}\gamma_{\mathcal{O}}(n, 1)$. The densestSublattice algorithm (Algorithm 3) retrieves the densest sublattice in time $(dT(\mathcal{O}, n, k)\deg(\mathcal{L}))^{k\log(dT(\mathcal{O},n,k)\deg(\mathcal{L}))}$ and a linear number of calls to an enumeration oracle with bound $T(\mathcal{O}, n, k)\deg(\mathcal{L})$.*

The correctness follows form what precedes and the complexity from counting argument on ideals over orders. It is detailed in Appendix E.

Remarks.

- The overhead induced by the discriminant in the running time is solely present due to the non-tightness of the transference bound.
- In the case where the order is the maximal order of the field, we can have a finer bound on the number of ideals of bounded norm. One can show that it grows only *linearly* in the norm instead of super polynomially! This gives a far better bound in only $\mathcal{O}(dT(\mathcal{O}, n, k)\deg(\mathcal{L}))^k$!
- By descending over $\mathbf{Z}$, it suffices to enumerate the ball of radius

$$\frac{k}{d}|\Delta(\mathcal{O})|^{\frac{2}{d}}\deg(\mathcal{L})\gamma_{\mathcal{O}}(n, 1)$$

  to complete the enumeration of S_k. Indeed, for each pair of linearly independent vectors (v_1, v_2) in this ball, we can construct the $\mathcal{O}v_1 + \mathcal{O}v_2$ and check if this sublattice is of rank 1. If this is the case, then $v_1, \ldots, v_2$ is a generating family of a subline. By collecting all generating families and sorting them by degree we can perform the full enumeration. This would allow us to fully implement the proposed reductions as we can perform the enumeration over the integers.

Bibliography

[1] Divesh Aggarwal, Jianwei Li, Phong Q. Nguyen, and Noah Stephens-Davidowitz. Slide reduction, revisited - filling the gaps in SVP approximation. In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO 2020, Part II*, volume 12171 of *LNCS*, pages 274–295. Springer, Heidelberg, August 2020.

[2] Miklós Ajtai. Generating hard instances of lattice problems (extended abstract). In *28th ACM STOC*, pages 99–108. ACM Press, May 1996.

[3] W. Banaszczyk. New bounds in some transference theorems in the geometry of numbers. *Mathematische Annalen*, 296(4):625–636, 1993.

[4] Jean-Benoît Bost. Theta invariants of euclidean lattices and infinite-dimensional hermitian vector bundles over arithmetic curves. *arXiv preprint arXiv:1512.08946*, 2015.

[5] Henri Cohen. *Advanced topics in computational number theory*, volume 193. Springer Science & Business Media, 2012.

[6] Keith Conrad. The conductor ideal of an order.

[7] Don Coppersmith. Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *Journal of Cryptology*, 10(4):233–260, September 1997.

[8] Daniel Dadush and Daniele Micciancio. Algorithms for the densest sublattice problem. In Sanjeev Khanna, editor, *24th SODA*, pages 1103–1122. ACM-SIAM, January 2013.

[9] Léo Ducas, Eamonn W. Postlethwaite, Ludo N. Pulles, and Wessel P. J. van Woerden. Hawk: Module LIP makes lattice signatures fast, compact and simple. In Shweta Agrawal and Dongdai Lin, editors, *ASIACRYPT 2022, Part IV*, volume 13794 of *LNCS*, pages 65–94. Springer, Heidelberg, December 2022.

[10] Thomas Espitau, Alexandre Wallet, and Yang Yu. On gaussian sampling, smoothing parameter and application to signatures. In *Advances in Cryptology - ASIACRYPT 2023*, volume 14444 of *Lecture Notes in Computer Science*, pages 65–97. Springer, 2023.

[11] Joël Felderhoff, Alice Pellet-Mary, and Damien Stehlé. On module unique-SVP and NTRU. In Shweta Agrawal and Dongdai Lin, editors, *ASIACRYPT 2022, Part III*, volume 13793 of *LNCS*, pages 709–740. Springer, Heidelberg, December 2022.

[12] Claus Fieker and ME Pohst. On lattices over number fields. In *International Algorithmic Number Theory Symposium*, pages 133–139. Springer, 1996.

[13] Claus Fieker and Damien Stehlé. Short Bases of Lattices over Number Fields. In *Algorithmic Number Theory, 9th International Symposium, ANTS-IX*, pages 157–173, 2010.

[14] Nicolas Gama, Nick Howgrave-Graham, Henrik Koy, and Phong Q. Nguyen. Rankin's constant and blockwise lattice reduction. In Cynthia Dwork, editor, *Advances in Cryptology - CRYPTO 2006, 26th Annual International*

Cryptology Conference, Santa Barbara, California, USA, volume 4117 of *Lecture Notes in Computer Science*, pages 112–130. Springer, 2006.

[15] Nicolas Gama and Phong Q. Nguyen. Finding short lattice vectors within Mordell's inequality. In Richard E. Ladner and Cynthia Dwork, editors, *40th ACM STOC*, pages 207–216. ACM Press, May 2008.

[16] M.J.C. Gover. The eigenproblem of a tridiagonal 2-toeplitz matrix. *Linear Algebra and its Applications*, 197-198:63–78, Jan 1994.

[17] Guillaume Hanrot, Xavier Pujol, and Damien Stehlé. Analyzing blockwise lattice algorithms using dynamical systems. In Phillip Rogaway, editor, *CRYPTO 2011*, volume 6841 of *LNCS*, pages 447–464. Springer, Heidelberg, August 2011.

[18] Paul Kirchner, Thomas Espitau, and Pierre-Alain Fouque. Fast reduction of algebraic lattices over cyclotomic fields. In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO 2020, Part II*, volume 12171 of *LNCS*, pages 155–185. Springer, Heidelberg, August 2020.

[19] Adeline Langlois and Damien Stehlé. Worst-case to average-case reductions for module lattices. *DCC*, 75(3):565–599, 2015.

[20] Changmin Lee, Alice Pellet-Mary, Damien Stehlé, and Alexandre Wallet. An LLL algorithm for module lattices. In Steven D. Galbraith and Shiho Moriai, editors, *ASIACRYPT 2019, Part II*, volume 11922 of *LNCS*, pages 59–90. Springer, Heidelberg, December 2019.

[21] Arjen K. Lenstra, Hendrik W. Jr. Lenstra, and László Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261:515–534, 1982.

[22] László Lovász. *An Algorithmic Theory of Numbers, Graphs and Convexity*. Society for Industrial and Applied Mathematics, 1986.

[23] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. In Henri Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 1–23. Springer, Heidelberg, May / June 2010.

[24] Daniele Micciancio and Michael Walter. Practical, predictable lattice basis reduction. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part I*, volume 9665 of *LNCS*, pages 820–849. Springer, Heidelberg, May 2016.

[25] Gabrielle De Micheli, Daniele Micciancio, Alice Pellet-Mary, and Nam Tran. Reductions from module lattices to free module lattices, and application to dequantizing module-LLL. In Helena Handschuh and Anna Lysyanskaya, editors, *CRYPTO 2023, Part V*, volume 14085 of *LNCS*, pages 836–865. Springer, Heidelberg, August 2023.

[26] Tamalika Mukherjee and Noah Stephens-Davidowitz. Lattice reduction for modules, or how to reduce ModuleSVP to ModuleSVP. In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO 2020, Part II*, volume 12171 of *LNCS*, pages 213–242. Springer, Heidelberg, August 2020.

[27] Alice Pellet-Mary and Damien Stehlé. On the hardness of the NTRU problem. In Mehdi Tibouchi and Huaxiong Wang, editors, *ASIACRYPT 2021, Part I*, volume 13090 of *LNCS*, pages 3–35. Springer, Heidelberg, December 2021.

[28] Humbert Pierre. Théorie de la réduction des formes quadratiques définies positives dans un corps algébrique fini. *Commentarii Mathematici Helvetici*, 12:263, 1939.
[29] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In Harold N. Gabow and Ronald Fagin, editors, *37th ACM STOC*, pages 84–93. ACM Press, May 2005.
[30] Miruna Rosca, Damien Stehlé, and Alexandre Wallet. On the ring-LWE and polynomial-LWE problems. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part I*, volume 10820 of *LNCS*, pages 146–173. Springer, Heidelberg, April / May 2018.
[31] Peter Stevenhagen. *Number rings*. 2020.
[32] Michael Walter. The convergence of slide-type reductions. In Juan Garay, editor, *PKC 2021, Part I*, volume 12710 of *LNCS*, pages 45–67. Springer, Heidelberg, May 2021.

A Proofs of Section 2

Proof (of Lemma 1). Denote by λ_i the successive minima of $\mathcal{O}_{\mathbf{K}}$ over $\mathbf{Z}$ (see infra Section 3.2.1 for a general account on this notion). The only difference with [13] is in the first item, where we notice the slightly stronger inequality $\lambda_i(\mathcal{O}) \geqslant \sqrt{d}$. By Minkowski's second theorem, we have $\lambda_d^2 \leqslant d^d \Delta_K \cdot \prod_{i<d} \lambda_i^{-2}$. Let $v_1, \ldots, v_n \in \mathcal{O}_{\mathbf{K}}$ with T_2-norm reaching λ_i. By the arithmetic-geometric inequality and the integrality of the v_i's, we see that $d \leqslant d\,\mathrm{N}(v_i)^{2/d} \leqslant \lambda_i^2$ for all i. Since the basis is LLL-reduced, we have $\max_i \|\beta_i\|_{T_2} \leqslant 2^{d/2}\lambda_d$, which gives the first item. □

Lemma 17 (Cauchy-Schwarz inequality for $\mathbf{K}_{\mathbf{R}}$). *For $g \in \mathcal{H}_n(\mathbf{K}_{\mathbf{R}})$ and $x, y \in \mathbf{K}_{\mathbf{R}}^n$, we have $\overline{g(x,y)}g(x,y) \leqslant \|x\|_g^2 \cdot \|y\|_g^2$.*

Proof. On each embedding, the standard Cauchy-Schwarz inequality writes as $|g_\sigma(x,y)|^2 \leqslant g_\sigma(x,x) \cdot g_\sigma(y,y)$. These are the embeddings we are looking for. □

B Proofs for Section 3

Another invariant of a projective module of finite rank is its *determinantial ideal* $\det(\mathcal{M}) = \det(B) \cdot \prod_i \mathfrak{a}_i$, where $((\mathfrak{a}_i)_i, B)$ is any pseudo-basis of $\mathcal{M}$. The determinant also helps in characterizing full-rank submodules. The proof of the next result (see Appendix B) essentially follows from examination of where the entries of a module transformation live.

Lemma 18. *If $\mathcal{N} \subset \mathcal{M}$ are projective $\mathcal{O}$-modules of the same finite rank, then we have $\det(\mathcal{N}) \subset \det(\mathcal{M})$, with equality when $\mathcal{N} = \mathcal{M}$.*

Proposition 1 (Multiplicativity of the volume) Let $\mathcal{L} = (\mathcal{M}, g)$ be an $\mathcal{O}$-lattice, and $\mathcal{L}' = (\mathcal{N}, g|_{\mathcal{N}_{\mathbf{R}}})$ be a primitive sublattice. We have

$$\mathrm{Vol}(\mathcal{L}) = \mathrm{Vol}(\mathcal{L}') \cdot \mathrm{Vol}(\pi(\mathcal{L})) = \mathrm{Vol}(\mathcal{L}') \cdot \mathrm{Vol}\left(\mathcal{L}/\mathcal{L}'\right).$$

Proof. Let $(\mathfrak{a}_i, b_i)_{i\leqslant r_n}$ be a pseudo-basis of $\mathcal{L}'$ and complete it as a pseudo-basis $(\mathfrak{a}_i, b_i)_{i\leqslant r_m}$ of $\mathcal{L}$. Since all involved ideals are invertible, the algebraic norm is multiplicative on them, and Lemma 6 shows that we may restrict to the case where $\mathfrak{a}_i = \mathcal{O}$ for all i. Fix a system of coordinates, and write $B_{\mathcal{N}}$ resp. B_0 the column matrix for the b_i's with $i \leqslant r_n$, resp. the column matrix for the b_i's with $i > r_n$. Write also G the matrix representing g. Then we have by block determinant formula

$$\begin{aligned}\mathrm{Vol}(\mathcal{L}) = \det[g(b_i,b_j)]_{i,j\leqslant r_m} &= \det\begin{bmatrix} X & Y \\ Y^* & Z\end{bmatrix} \\ &= \det(X)\cdot\det(Z - Y^*X^{-1}Y),\end{aligned}$$

with $X = B_{\mathcal{N}}^* G B_{\mathcal{N}}$, $Y = B_{\mathcal{N}}^* G B_0$ and $Z = B_0^* G B_0$. Now we readily compute that $Z - Y^*X^{-1}Y = B_0^* G(\mathrm{Id} - P_{\mathcal{N}})B_0$, where $P_{\mathcal{N}} = B_{\mathcal{N}}(B_{\mathcal{N}}^* G B_{\mathcal{N}})^{-1} B_{\mathcal{N}}^* G$ a matrix for the orthogonal projection onto $\mathcal{N}_{\mathbf{R}}$. In other words, this is the matrix of the $g(b_i, \pi(b_i))$'s for $i > r_n$, and by orthogonality, this is the same as the matrix of the $g(\pi(b_i), \pi(b_i))$'s for the same i's. Combined with $\det X = \mathrm{Vol}(\mathcal{L}')$, this gives the first equality, and the second follows using Lemma 7. □

Lemma 18. If $\mathcal{N} \subset \mathcal{M}$ are projective $\mathcal{O}$-modules of the same finite rank, then we have $\det(\mathcal{N}) \subset \det(\mathcal{M})$, with equality when $\mathcal{N} = \mathcal{M}$.

Proof. Let $\mathcal{N} = \bigoplus_{i\leqslant n} \mathfrak{c}_i c_i$ and $\mathcal{M} = \bigoplus_{i\leqslant n} \mathfrak{a}_i b_i$, and also $C = [c_i]_{i\leqslant n}$ and $B = [b_i]_{i\leqslant n}$. Since $\mathcal{M}$ and $\mathcal{N}$ span the same $\mathbf{K}$-space, there exists an invertible matrix $U \in \mathbf{K}^{n\times n}$ such that $C = BU$. Because each $\mathfrak{c}_j c_j$ is a submodule of $\mathcal{M}$, we see that $u_{ij} \in \mathfrak{a}_i \mathfrak{c}_j^{-1}$ for all i, j. By definition, we have $\det(\mathcal{N}) = \left(\prod_i \mathfrak{c}_i \mathfrak{a}_i^{-1} \cdot \det(U)\right)\det(\mathcal{M})$, which gives the result combined to $\det U \subset \prod_i \mathfrak{a}_i \mathfrak{c}_i^{-1}$. When $\mathcal{N} = \mathcal{M}$, then the entries of U^{-1} belong to the ideals $\mathfrak{a}_i^{-1}\mathfrak{c}_j$ which leads to the inverse inclusion[12]. □

Lemma 2. Let $\mathcal{M} = \mathfrak{a}_1 b_1 \oplus \mathfrak{a}_2 b_2$ be a rank 2 projective $\mathcal{O}$-module, and $(\mathfrak{c}_1, d_1)$ be one of its primitive submodules. Let $(u, v) = [b_1, b_2]^{-1} d_1$, then $(u, v) \in \mathfrak{a}_1\mathfrak{c}_1^{-1} \times \mathfrak{a}_2\mathfrak{c}_1^{-1}$, and there exists $(x, y) \in \mathfrak{a}_2^{-1}\mathfrak{c}_1 \times \mathfrak{a}_1^{-1}\mathfrak{c}_1$ such that:

$$uy - vx = 1 \qquad \text{and} \qquad \mathcal{M} = \mathfrak{c}_1 d_1 \oplus \mathfrak{a}_1\mathfrak{a}_2\mathfrak{c}_1^{-1}(xb_1 + yb_2).$$

Moreover there is an algorithm that is polynomial in $\Delta(\mathcal{O})$ and the input bit-size to compute (x, y).

Proof. By definition, $(u\mathfrak{c}_1)b_1 + (v\mathfrak{c}_1)b_2 = \mathfrak{c}_1 d_1 \subset \mathcal{M}$, implying that $u\mathfrak{c}_1 \subseteq \mathfrak{a}_1$ and $v\mathfrak{c}_2 \subseteq \mathfrak{a}_2$, so it is necessary that $(u, v) \in \mathfrak{a}_1\mathfrak{c}_1^{-1} \times \mathfrak{a}_2\mathfrak{c}_1^{-1}$. Primitivity implies that there exists a fractional ideal $\mathfrak{c}$ and a vector d such that $\mathcal{M} = \mathfrak{c}_1 d_1 \oplus \mathfrak{c} d$. Let $(x', y') = [b_1, b_2]^{-1} d$, and similarly as above, observe that $(x', y') \in \mathfrak{a}_1\mathfrak{c}^{-1} \times \mathfrak{a}_2\mathfrak{c}^{-1}$. The primitivity condition also implies that $\mathfrak{a}_1\mathfrak{a}_2 = (uy' - vx')\mathfrak{c}_1\mathfrak{c}$. It now suffices to set $x = x'/(uy' - vx')$, $y = y'/(uy' - vx')$.

[12] In that situation, one also checks that U is an admissible transformation from $((\mathfrak{a}_i)_i, B)$ to $((\mathfrak{c}_i)_i, C)$.

We now turn to Algorithm 4 and its analysis.

Algorithm 4: Completing a primitive submodule of a rank 2 module into a basis

Input: a rank 2 module $\mathcal{M} = \mathfrak{a}_1 b_1 \oplus \mathfrak{a}_2 b_2$ and a primitive submodule $(\mathfrak{c}_1, d_1)$
Result: a module $(\mathfrak{c}_2, d_2) \subset \mathcal{M}$ such that $\mathfrak{c}_1 d_1 \oplus \mathfrak{c}_2 d_2 = \mathcal{M}$ and an admissible transformation matrix U from (b_1, b_2) to (d_1, d_2)

1 Let $d = [\mathbf{K} : \mathbf{Q}]$, $B = [b_1, b_2]$ and $(u, v) \leftarrow B^{-1} d_1$
2 **if** $u = 0$ **then** $x = 0; y = \frac{1}{v}$
3 **if** $v = 0$ **then** $x = \frac{1}{u}; y = 0$
4 $I \leftarrow$ a $\mathbf{Z}$-basis of $u\mathfrak{a}_1^{-1}\mathfrak{c}_1$, $J \leftarrow$ a $\mathbf{Z}$-basis of $v\mathfrak{a}_2^{-1}\mathfrak{c}_1$
5 $C \leftarrow [I|J]$
6 Compute the matrix Z such that $CZ = [\mathrm{Id}\,|0]$, let $(z_I, z_J)^t$ be its first column
7 $x' \leftarrow$ the element in $\mathcal{O}_{\mathbf{K}}$ corresponding to Jz_J
$x \leftarrow x'/v; y \leftarrow -(1 - x')/u$
8 **return** $(\mathfrak{a}_1\mathfrak{a}_2\mathfrak{c}_1^{-1}, xb_1 + yb_2)$ and $U = \begin{pmatrix} u & x \\ v & y \end{pmatrix}$

The running time is dominated by Step 7, which is polynomial time from [5]. From Lemma 2, we have that $u\mathfrak{a}_1^{-1}\mathfrak{c}_1 + v\mathfrak{a}_2^{-1}\mathfrak{c}_1 = \mathcal{O}$: indeed, it contains 1 and both $u\mathfrak{a}_1^{-1}\mathfrak{c}_1$ and $v\mathfrak{a}_2^{-1}\mathfrak{c}_1$ are integral ideals. Since the HNF of the matrix C is the HNF of the ideal $I + J$, it is then $[\mathrm{Id}\,|0]$. It follows that $Iz_I + Jz_J = (1, 0, \ldots, 0)^T$, so that $uy - vx = 1$ with $x \in \mathfrak{a}_2^{-1}\mathfrak{c}_1$ and $y \in \mathfrak{a}_1^{-1}\mathfrak{c}_1$ By choice, we have $\mathfrak{c}_2 = \mathfrak{a}_1\mathfrak{a}_2\mathfrak{c}_1^{-1}$, so that we also have $(x, y) \in \mathfrak{a}_1\mathfrak{c}_2^{-1} \times \mathfrak{a}_2\mathfrak{c}_2^{-1}$. Hence U is an admissible transformation matrix, and the correctness follows. □

Lemma 3. Let $\mathcal{L} = ((\mathfrak{a}_i, b_i), g)$ be a $\mathcal{O}$-lattice of rank n. There exists a hermitian form g' such that $\mathcal{L}$ is isometric to $\big((\mathcal{O}, b_1), \ldots, (\mathcal{O}, b_{n-1}), (\prod_i \mathfrak{a}_i, b_n)), g'\big)$.

Proof. From [5, Lem. 1.2.20], we know that there is a $\mathcal{O}$-module isomorphism φ from $\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n$ to $\mathcal{O}^{n-1} \oplus \mathfrak{s}$, for some ideal $\mathfrak{s}$ in the Steinitz class of the module. Then we can extend $\varphi : \mathcal{L}' \longrightarrow \mathcal{L}_0 := ((\mathcal{O}, b_1), \ldots, (\mathcal{O}, b_{n-1}), (\mathfrak{s}, b_n))$ by letting $\varphi(\sum_i \alpha_i b_i) = \sum_i \varphi(\alpha_1, \ldots, \alpha_n)_i b_i$, where the notation $\varphi(\cdot, \ldots, \cdot)_i$ means the i-th component of the image. Being a $\mathcal{O}$-linear map defined over $\mathcal{O}$, it is also $\mathbf{K}_{\mathbf{R}}$-invertible. For $x, y \in \mathcal{L}_0$ we then let $g'(x, y) = g(\varphi^{-1}(x), \varphi^{-1}(y))$ which turns φ into an isometry of $\mathcal{O}$-lattices. □

Lemma 5. Let $\mathcal{L}$ be an $\mathcal{O}$-lattice. Let $M_{\mathcal{O}}$ be the Minkowski constant of $\mathcal{O}$. Write $d_k(\mathcal{L})$ the volume of the densest free sublattice of $\mathcal{L}$. We have $d_k(\mathcal{L}) \leqslant M_{\mathcal{O}} \cdot \delta_k(\mathcal{L})$. In particular, we have $\nu_1(\mathcal{L}) \leqslant M_{\mathcal{O}} \cdot \lambda_1(\mathcal{L})$.

Proof. If $\mathcal{O}$ is principal, all $\mathcal{O}$-modules are free, and accordingly $M_{\mathcal{O}} = 1$. We now assume $\mathcal{O}$ is not principal. Let $\mathcal{L}' = ((\mathfrak{a}_i, b_i)_{i \leqslant k}, g)$ be the densest sublattice of rank k in $\mathcal{L}$. Writing $\mathfrak{s} = \prod_{i \leqslant k} \mathfrak{a}_i$, by Lemma 3, we can equivalently solve the

problem in $\mathcal{L}_0 = ((\mathcal{O}, b_i)_{i\leqslant k-1}, (\mathfrak{s}, b_k), g')$. Let $\mathcal{M}_0$ be the underlying projective module. By Minkowski's bound for the class group, we know that there exists $\alpha \in \mathfrak{s}$ such that $\mathrm{N}(\alpha\mathcal{O}) \leqslant M_{\mathcal{O}} \mathrm{N}(\mathfrak{s})$. Now the projective module $\mathcal{M} = \mathcal{O}b_1 \oplus \cdots \oplus \mathcal{O}b_{k-1} \oplus \alpha\mathcal{O}b_k$ is a free submodule of rank k in $\mathcal{M}_0$, and the quotient is isomorphic to the finite torsion module $\mathfrak{s}/\alpha\mathcal{O}$. This means the sublattice $\mathcal{L}'' = (\mathcal{M}, g')$ of $\mathcal{L}_0$ has volume at most $M_{\mathcal{O}} \operatorname{Vol}(\mathcal{L}')$. □

Lemma 4. Let $\mathcal{L}' \subsetneq \mathcal{L}$ be $\mathcal{O}$-lattices, and assume that $\mathcal{L}'$ is a densest sublattice of rank $k = \operatorname{rk} \mathcal{L}'$. Then $\mathcal{L}'$ is primitive.

Proof. Let us assume by contradiction that $\mathcal{L}'$ is a densest sublattice, but is not primitive. Equivalently, $\mathcal{L}/\mathcal{L}'$ has torsion elements, that is, there are $x \in \mathcal{L} \setminus \mathcal{L}'$ and $a \in \mathcal{O}$ such that $ax \in \mathcal{L}'$. In other words, x is an element in $(\operatorname{span}_{\mathbf{K}}(\mathcal{L}') \cap \mathcal{L}) \setminus \mathcal{L}'$. If $(\mathfrak{a}_i, b_i)_i$ is a pseudo-basis of $\mathcal{L}'$, its basis vectors are also a basis for the ambient $\mathbf{K}$-space. Writing $x = \sum_i \lambda_i b_i \in \mathcal{L}$, we can assume without loss of generality that $\lambda_1 \notin \mathfrak{a}_1$, and this gives us that $\lambda_1 \mathcal{O} b_1 \subset \mathcal{L}$. If we let $\mathfrak{a}'_1 = \lambda_1\mathcal{O} + \mathfrak{a}_1$, we then have $\mathfrak{a}'_1 b_1 \subset \mathcal{L}$. Now, the submodule $\mathfrak{a}'_1 b_1 \oplus \bigoplus_{i>1} \mathfrak{a}_i b_i$ of $\mathcal{M}$ has the same rank as $\mathcal{L}'$, but since $\mathfrak{a}_1 \subsetneq \mathfrak{a}'_1$, the volume of its corresponding lattice is strictly smaller than $\operatorname{Vol}(\mathcal{L}')$, which contradicts our initial assumption. □

Lemma 6. Let π be the orthogonal projection from $\mathcal{M}_{\mathbf{R}}$ onto $\mathcal{N}_{\mathbf{R}}^{\perp}$. The module $\pi(\mathcal{M})$ is projective of rank $r_m - r_n$ in $\mathcal{N}_{\mathbf{R}}^{\perp}$. If $(\mathfrak{a}_i, b_i)_{r_n < i \leqslant r_m}$ is any pseudo-basis that completes $\mathcal{N}$ into $\mathcal{M}$, then $(\mathfrak{a}_i, \pi(b_i))_{i>r_n}$ is a pseudo-basis for $\pi(\mathcal{M})$.

Proof. Since $\mathcal{N}$ is primitive, we can complete any pseudo-basis $(\mathfrak{a}_i, b_i)_{i\leqslant r_n}$ of $\mathcal{N}$ into a pseudo-basis $(\mathfrak{a}_i, b_i)_{i\leqslant r_m}$ of $\mathcal{M}$. We have by definition $\pi(b_i) = 0$ for $i \leqslant r_n$. Hence for a vector $m = \sum_{i\leqslant r_m} m_i b_i \in \mathcal{M}$ we have $\pi(m) = \sum_{i>r_n} m_i \pi(b_i)$, with $m_i \in \mathfrak{a}_i$. The family $(\pi(b_i))_{i>r_n}$ is also $\mathbf{K}$-free: if a $\mathbf{K}$-linear combination of $b_{r_n+1}, \ldots, b_{r_m}$ belongs to $\mathcal{N}_{\mathbf{R}}$, then a $\mathbf{K}$-linear combination of the b_i's vanishes, so it can only be a trivial combination since the b_i's are in particular a basis of $\mathcal{M}_{\mathbf{R}}$. In other words, $\pi(\mathcal{M})$ has a pseudo-basis $(\mathfrak{a}_i, \pi(b_i))_{i>r_n}$, which shows the projectiveness and gives the rank. □

Lemma 7. We have $\|x + \mathcal{N}\|_{\mathcal{M}/\mathcal{N}} = \|\pi(x)\|_g$ for all $x \in \mathcal{L}$. In particular, $\mathcal{L}/\mathcal{L}' := (\mathcal{M}/\mathcal{N}, \|\cdot\|_{\mathcal{M}/\mathcal{N}})$ is a $\mathcal{O}$-lattice and we have an isometry $\mathcal{L}/\mathcal{L}' \simeq \pi(\mathcal{L})$.

Proof. The candidate isometry maps the pseudo-bases of $\mathcal{L}/\mathcal{L}'$ and $\pi(\mathcal{L})$ one to each other and is extended $\mathcal{O}$-linearly. It remains to show that it is indeed an isometry. Since π is an orthogonal projection, Pythagoras theorem gives on each embedding σ that $g(m,m)_\sigma \geqslant g(\pi(m), \pi(m))_\sigma$ for all $m \in \mathcal{M}$. We have for all $n \in \mathcal{N}_{\mathbf{R}}$ that $\pi(n) = 0$, which implies $\|m + \mathcal{N}\|_{\mathcal{M}/\mathcal{N}} \geqslant \|\pi(m)\|_g$ for all $m \in \mathcal{M}$ — this inequality should be understood embedding-wise. Using that $\pi^2 = \pi$, the inequality is saturated with $m = (m - \pi(m)) + \pi(m)$. □

Lemma 8. Let $\mathcal{L}$ be a $\mathcal{O}$-lattice and $\mathcal{L}_{\mathbf{R}} = \mathcal{L} \otimes_{\mathcal{O}} \mathbf{R}$ its ambient space. The dual lattice is $\mathcal{L}^\vee = \{y \in \mathcal{L}_{\mathbf{R}} \ : \ g(y, \mathcal{L}) \in \mathcal{O}\}$.

Proof. Let $y = \sum_i y_i b_i^\vee$ be in the $\mathcal{O}$-lattice spanned by the candidate pseudo-basis, and $x = \sum_i x_i b_i \in \mathcal{L}$. We readily check that $g(x,y) = \sum_i \overline{y_i} x_i g(b_i^\vee, b_i) \in \mathcal{O}$

since $x_i \in \mathfrak{a}_i$ and $\overline{y_i} \in \mathfrak{a}_i^{-1}$, so the lattice spanned by this pseudo-basis is included in $\mathcal{L}^\vee$. Reciprocally, let $y = \sum_i y_i b_i^\vee \in \mathcal{L}^\vee$, with the y_i *a priori* in $\mathbf{K_R}$ (since the dual basis span the ambient space). Fix an arbitrary i and let $\mathfrak{a} = \mathfrak{a}_i$. By definition of the dual lattice, for all $\alpha \in \mathfrak{a}$, we must have $g(y, \alpha_i b_i) = \overline{y}_i \alpha \in \mathcal{O}$. If $\mathfrak{a}$ is principal, this directly implies $y_i \in \mathfrak{a}^{-*}$. Else, this is in particular true for a set of $\mathcal{O}$-generators u, v for $\mathfrak{a}$, so $y_i \in u^{-1}\mathcal{O} \cap v^{-1}\mathcal{O}$. We are left to show that $\mathfrak{a}^{-1} = u^{-1}\mathcal{O} \cap v^{-1}\mathcal{O}$, which is handled by Lemma 19 below. □

Recall that invertible ideals are always generated by at most two elements.

Lemma 19. *Let $\mathfrak{a} = u\mathcal{O} + v\mathcal{O}$ be an invertible fractional ideal of an order $\mathcal{O}$. Then $\mathfrak{a}^{-1} = u^{-1}\mathcal{O} \cap v^{-1}\mathcal{O}$.*

Proof. Let temporarily $\mathfrak{b} = u^{-1}\mathcal{O} \cap v^{-1}\mathcal{O}$. We proceed by double inclusion. Let $x \in \mathfrak{b}$, so that $xu, xv \in \mathcal{O}$. All element in $\mathfrak{a}$ can be written $e = ue_u + ve_v$ for some $e_u, e_v \in \mathcal{O}$. Then $xe = xue_u + xve_v$ is also in $\mathcal{O}$, so $\mathfrak{b} \subset \mathfrak{a}^{-1}$. If $x \in \mathfrak{a}^{-1}$, then in particular $xu, xv \in \mathcal{O}$ so $x \in \mathfrak{b}$. This gives the reverse inclusion and the result follows. □

Lemma 9. If $\mathcal{L}$ is a $\mathcal{O}$-lattice, then $\det \mathcal{L}^\vee = \det \mathcal{L}^{-*}$ and $\operatorname{Vol}\mathcal{L} \cdot \operatorname{Vol}\mathcal{L}^\vee = 1$.

Proof. Recall that $\mathrm{N}(\mathfrak{a}) = \mathrm{N}(\overline{\mathfrak{a}})$ for all fractional $\mathcal{O}$-ideals. In particular, we have $\mathrm{N}(\mathfrak{a}^{-*}) = \mathrm{N}(\mathfrak{a})^{-1}$ when $\mathfrak{a}$ is invertible. Let B resp $B^\vee$ be matrix representations for the basis vectors of $\mathcal{L}$ and $\mathcal{L}^\vee$, and G be that of the form g. Routine calculations give $\det((B^\vee)^* G B^\vee) = \det(B^* G B)^{-1}$. Hence $(det\mathcal{L})^{-*} = (\prod_i \mathrm{N}(\mathfrak{a}_i^{-*}), 1, \det(B^* G B)^{-1})$ is indeed the conjugate of $(\det \mathcal{L})^{-1}$, and $\operatorname{Vol}(\mathcal{L}) \cdot \operatorname{Vol}(\mathcal{L}^\vee) = 1$ □

.

Proposition 2. Let $\mathcal{L}' \subset \mathcal{L}$ be $\mathcal{O}$-lattices with $\mathcal{L}'$ of rank r_n primitive in $\mathcal{L}$ of rank r_m. Let also $\mathcal{L}'_{\mathbf{R}} = \mathcal{L}' \otimes_{\mathcal{O}} \mathbf{R}$ be the space spanned by $\mathcal{L}'$ and π the orthogonal projection onto ${\mathcal{L}'_{\mathbf{R}}}^{\perp}$. Then we have $\pi(\mathcal{L})^\vee = \mathcal{L}^\vee \cap {\mathcal{L}'_{\mathbf{R}}}^{\perp}$, and a pseudo-basis of this lattice is $\left((\mathfrak{a}_i^{-*}, b_i^\vee)_{r_n < i \leqslant r_m}, g^\perp\right)$.

Proof. Let $x \in \mathcal{L}^\vee \cap {\mathcal{L}'_{\mathbf{R}}}^{\perp}$ and $y \in \pi(\mathcal{L})$. For a $z \in y + \mathcal{L}'_{\mathbf{R}}$, we have $g(x, z-y) = 0$, so if moreover $z \in \mathcal{L}$, we have that $g(x, y) = -g(x, z) \in \mathcal{O}$ by definition of x. This implies that $\mathcal{L}^\vee \cap {\mathcal{L}'_{\mathbf{R}}}^{\perp} \subset \pi(\mathcal{L})^\vee$. For the other inclusion, let $x \in \pi(\mathcal{L})^\vee \subset {\mathcal{L}'_{\mathbf{R}}}^{\perp}$. Take $y \in \mathcal{L}$ and write it as $y = \pi(y) + (y - \pi(y))$. Then we see that $g(x, y) = g(x, y - \pi(y)) + g(x, \pi(y)) = g(x, \pi(y)) \in \mathcal{O}$. Let now $(\mathfrak{a}_i, b_i)_{i \leqslant r_n}$ be a pseudo-basis of $\mathcal{L}'$ and complete it as a pseudo-basis $(\mathfrak{a}_i, b_i)_{i \leqslant r_m}$ of $\mathcal{L}$. We deduce from the definition of the dual basis that ${\mathcal{L}'_{\mathbf{R}}}^{\perp} = \operatorname{span}_{\mathbf{K_R}}(b_i^\vee)_{i > r_n}$, and that $g(b_i^\vee, \pi(b_j)) = g(b_i^\vee, b_j) = 1$ if $i = j$ and 0 otherwise. Hence $(b_i^\vee)_{i > r_n}$ is the dual basis of $(\pi^\perp(b_i))_{i > r_n}$. This completes the proof. □

B.1 Details for Section 3.3

We start with the notion of scaled pseudo-basis, introduced [20] to ensure the size of (the representation of) the coefficient ideals stays bounded during execution of algorithms.

Definition 16. *Let $((\mathfrak{a}_i, b_i)_{i\leqslant n}, g)$ be a pseudo-basis of a $\mathcal{O}$-lattice $\mathcal{L}$. Let $(\widetilde{b_i})$ be the Gram-Schmidt orthogonalization of the b_i's with respect to g, and $r_{ii} = g(\widetilde{b_i}, \widetilde{b_i})$. The pseudo-basis is said* scaled *if we have $\mathcal{O} \subseteq \mathfrak{a}_i$, $\mathrm{N}(\mathfrak{a}_i) \geqslant 2^{-d^2}\Delta(\mathcal{O})^{-1/2}$ and $\|r_{ii}\|_{T_2} \leqslant 2^d\Delta(\mathcal{O})^{1/(2d)}\,\mathrm{N}(r_{ii}\mathfrak{a}_i)^{1/d}$ for all $i \leqslant n$.*

While we have put no restriction on g in defining the objects, it is reasonable to ask that it is rational, that is, that it has can be represented by a matrix with entries in $\mathbf{K}$.

Lemma 20 (Adapted from [20], Le. 3.6). *There is an algorithm that outputs a scaled pseudo-basis of the $\mathcal{O}$-lattice $\mathcal{L}$ generated by an input pseudo-basis, and preserves the $\mathrm{N}(r_{ii}\mathfrak{a}_i)$'s. If $\mathcal{M} \subseteq \mathbf{K}^n$ and g is rational, then it runs in time polynomial in $\log\Delta(\mathcal{O})$ and the input bit-length.*

Algorithm 5: Scaling the ideals

Input: A pseudo-basis $((\mathfrak{a}_i, b_i)_{i\leqslant n}, g)$ of $\mathcal{L}$.
Result: A sclaed pseudo-basis $((\mathfrak{a}'_i, b'_i)_{i\leqslant n}, g)$ of $\mathcal{L}$.

$(\widetilde{b_i}) \leftarrow$ **GSO**$((b_i)_i, g)$ and $r_{ii} \leftarrow g(\widetilde{b_i}, \widetilde{b_i})$ for all $i \leqslant n$
for i *from* 1 *to* n **do**
  Use **LLL$_\mathbf{Z}$** to find $s_i \in r_{ii}\mathfrak{a}_i \setminus \{0\}$ such that $\|s_i\|_{T_2} \leqslant 2^d\Delta_{\mathbf{K}}^{1/(2d)}\,\mathrm{N}(r_{ii}\mathfrak{a}_i)^{1/d}$
  Write $s_i = r_{ii} \cdot x_i$ for some $x_i \in \mathfrak{a}_i$
  $\mathfrak{a}'_i \leftarrow x_i^{-1}\mathfrak{a}_i, b'_i \leftarrow x_i b_i$
end for
return $((\mathfrak{a}'_i, b'_i)_{i\leqslant n}, g)$

Size-reduction of a basis is a common procedure for $\mathbf{Z}$-lattices. We extend this notion of size-reduced pseudo-bases, directly adapting from [12, 20].

Definition 17. *Let $((\mathfrak{a}_i, b_i)_{i\leqslant n}, g)$ be a pseudo-basis of a $\mathcal{O}$-lattice $\mathcal{L}$. Let $(\widetilde{b_i})$ be the Gram-Schmidt orthogonalization of the b_i's, $r_{ii} = g(\widetilde{b_i}, \widetilde{b_i})$ and $r_{ij} = g(\widetilde{b_j}, \widetilde{b_i})$. The pseudo-basis is said* size-reduced *if it is scaled and if we have $\|r_{ij}/r_{ii}\|_{T_2} \leqslant (4d)^d\Delta(\mathcal{O})^{1/2}$ for all $i < j \leqslant n$.*

For $\mathcal{O}$-lattices, we also reuse an algorithm of [12, 20]. It uses a rounding procedure; one could call any (approximate) CVP oracle in $\mathcal{O}$, or even describe the algorithm with an exact CVP-oracle (in the T_2 norm). The interested reader can find it in Appendix B, directly reproduced from [20]. Nevertheless we conclude this section with its associated lemma.

Lemma 21 ([20], Lemma 3.7). *There is an algorithm that outputs a size-reduced pseudo-basis of $\mathcal{L}$ generated by the input pseudo-basis, and preserves the $\mathrm{N}(\mathfrak{a}_i r_{ii})$'s. If $\mathcal{L} \subset \mathbf{K}^n$ and g is rational, it runs in polynomial time in $\log\Delta(\mathcal{O})$ and the input bit-length.*

Namely, let $(\beta_k)_k$ be an LLL-reduced $\mathbf{Z}$-basis of $\mathcal{O}$. Any $x \in \mathbf{K_R}$ can then be written $\sum_k x_k\beta_k$ with $x_k \in \mathbf{R}$, and we define $\lfloor x \rceil = \sum_k \lfloor x_k \rceil_{\mathbf{Z}} \beta_k$, where $\lfloor \cdot \rceil_{\mathbf{Z}}$ denotes the closest integer.

Algorithm 6: Size-reduction

Input: A scaled pseudo-basis $((\mathfrak{a}_i, b_i)_{i\leqslant n}, g)$ of $\mathcal{L}$.
Result: A size-reduced pseudo-basis $((\mathfrak{a}'_i, b'_i)_{i\leqslant n}, g)$ of $\mathcal{L}$.

$(\widetilde{b_i})_i \leftarrow \mathsf{GSO}((b_i)_i, g)$, $r_{ij} = g(\widetilde{b_j}, \widetilde{b_i})$ for $1 \leqslant i < j \leqslant n$
for i *from* 1 *to* n **do**
  for j *from* $i-1$ *to* 1 **do**
    $x \leftarrow \lfloor \frac{r_{ij}}{r_{ii}} \rceil$
    $b_i \leftarrow b_i - x b_j$
  end for
end for
return $((\mathfrak{a}_i, b_i)_i, g)$

Algorithm 7: Scaling the ideals

Input: A pseudo-basis $((\mathfrak{a}_i, b_i)_{i\leqslant n}, g)$ of $\mathcal{L}$.
Result: A sclaed pseudo-basis $((\mathfrak{a}'_i, b'_i)_{i\leqslant n}, g)$ of $\mathcal{L}$.

$(\widetilde{b_i}) \leftarrow$ **GSO**$((b_i)_i, g)$ and $r_{ii} \leftarrow g(\widetilde{b_i}, \widetilde{b_i})$ for all $i \leqslant n$
for i *from* 1 *to* n **do**
  Use **LLL**$_{\mathbf{Z}}$ to find $s_i \in r_{ii}\mathfrak{a}_i \setminus \{0\}$ such that
  $\|s_i\|_{T_2} \leqslant 2^d \Delta_{\mathbf{K}}^{1/(2d)} \mathrm{N}(r_{ii}\mathfrak{a}_i)^{1/d}$
  Write $s_i = r_{ii} \cdot x_i$ for some $x_i \in \mathfrak{a}_i$
  $\mathfrak{a}'_i \leftarrow x_i^{-1}\mathfrak{a}_i$, $b'_i \leftarrow x_i b_i$
end for
return $((\mathfrak{a}'_i, b'_i)_{i\leqslant n}, g)$

Now let $(\beta_k)_k$ be an LLL-reduced $\mathbf{Z}$-basis of $\mathcal{O}$. Any $x \in \mathbf{K_R}$ can then be written $\sum_k x_k\beta_k$ with $x_k \in \mathbf{R}$, and we define $\lfloor x \rceil = \sum_k \lfloor x_k \rceil_{\mathbf{Z}} \beta_k$, where $\lfloor \cdot \rceil_{\mathbf{Z}}$ denotes the closest integer. With this rounding procedure, we can design a size-reduction algorithm for $\mathcal{O}$-lattices.

Algorithm 8: Size-reduction

Input: A scaled pseudo-basis $((\mathfrak{a}_i, b_i)_{i\leqslant n}, g)$ of $\mathcal{L}$.
Result: A size-reduced pseudo-basis $((\mathfrak{a}'_i, b'_i)_{i\leqslant n}, g)$ of $\mathcal{L}$.

$(\widetilde{b}_i)_i \leftarrow \mathsf{GSO}((b_i)_i, g)$, $r_{ij} = g(\widetilde{b}_j, \widetilde{b}_i)$ for $1 \leqslant i < j \leqslant n$
for i *from* 1 *to* n **do**
  for j *from* $i-1$ *to* 1 **do**
    $x \leftarrow \lfloor \frac{r_{ij}}{r_{ii}} \rceil$
    $b_i \leftarrow b_i - x b_j$
  end for
end for
return $((\mathfrak{a}_i, b_i)_i, g)$

C Proofs for Section 4

Proof (of Proposition 4). We start by showing the preservation of the lattice during the execution. From Lemma 20 and Lemma 21, the **SizeReduce** resp. **Scale** steps preserve their input modules, and run in polynomial time in $\log \Delta_{\mathbf{K}}$ and the input bitlength. As we start from a natural filtration, all the quotient module in `Steps` 4 and 5 have rank 2. In any i-th iteration of the for loop, let $V = \mathcal{L}_{i-1} \otimes \mathbf{K}$. Thanks to Lemma 2, Lemma 4 and Lemma 7, we have $\mathcal{L}_{i+1}/\mathcal{L}_{i-1} \simeq \pi_{V^\perp}(\mathcal{L}_{i+1}) = \mathfrak{c}c \oplus \mathfrak{c}'c'$. Moreover, we check that $[c, c'] = \pi_{V^\perp}([b_i, b_{i+1}])U = \pi_{V^\perp}([b_i, b_{i+1}]U)$ and that U is an admissible transformation matrix from $\mathfrak{a}_i b_i \oplus \mathfrak{a}_{i+1} b'_{i+1}$ to $\mathfrak{c} \cdot Ub_i \oplus \mathfrak{c}' \cdot Ub_{i+1}$. In other words, the update of the filtration in `Step` 8 preserves the ambient module, as was claimed. We now turn to the spectral analysis of Δ. By e.g. induction one can show that the matrix is as follow:

$$\Delta = \begin{bmatrix} 0 & \frac{1}{2} & & & 0 \\ 0 & \frac{1}{4} & \frac{1}{2} & & 0 \\ 0 & \frac{1}{8} & \frac{1}{4} & \frac{1}{2} & \\ 0 & \vdots & \ddots & \ddots & 0 \\ \vdots & & & & \frac{1}{2} \\ 0 & 2^{-n} & 2^{1-n} & \cdots & \frac{1}{8} \quad \frac{1}{4} \end{bmatrix}.$$

To analyze it, we split it into two structured submatrices $\Delta = T + P$, where T is the matrix composed of the diagonal and the upper diagonal row of Δ, and P is lower triangular with 0's on the diagonal, and its first lower diagonal being all $1/8$. Calculations show that

$$T^t T = \begin{bmatrix} 0 & 0 & \cdots & & 0 \\ 0 & \frac{5}{16} & \frac{1}{8} & & \\ 0 & \frac{1}{8} & \frac{5}{16} & \frac{1}{8} & \\ 0 & & \frac{1}{8} & \frac{5}{16} & \frac{1}{8} \\ 0 & & \cdots & \frac{1}{8} & \frac{5}{16} \end{bmatrix}.$$

As T^tT is symmetric its spectral norm is deduced from the largest eigenvalues, and thanks to the first row of 0's, we may consider only the tridiagonal Toeplitz sub-block. From [16, Section 2, (2.7)], its largest eigenvalue is $\lambda = \frac{5}{16} - \frac{1}{4}\cos\left(\frac{(n-2)\pi}{n-1}\right) = \frac{1}{16} + \frac{1}{4}(1+\cos(\pi/(n-1))$. With standard bounds using Taylor expansion, we have $1+\cos(\pi/(n-1)) \leqslant 2 - \frac{\pi^2}{(n-1)^2}$, and we obtain

$$\lambda \leqslant \frac{9}{16}\left(1 - \frac{4\pi^2}{9(n-1)^2}\right).$$

Taking square roots and using again a Taylor expansion, this implies

$$\|T\| \leqslant \frac{3}{4}\left(1 - \frac{4\pi^2}{9(n-1)^2}\right)^{1/2} \leqslant \frac{3}{4} - \frac{\pi^2}{6(n-1)^2}. \tag{14}$$

For the case of P, we observe that its second column and its last rows have the same entries, and that these corresponds to the largest vectors among the rows and columns. We then readily compute that $\|P\|_1 = \|P\|_\infty = \sum_{i=3}^{n-1} 2^{-i} \leqslant \frac{1}{4}$, and use the inequality $\|P\| \leqslant (\|P\|_1\|P\|_\infty)^{1/2}$ with Inequality (14) to obtain

$$\|\Delta\| \leqslant \|P\| + \|T\| \leqslant 1 - \frac{\pi^2}{6(n-1)^2}.$$

This finally yields us

$$\|\Pi(\mathcal{L}^{(\ell)}) - \mu\|_2 \leqslant \left(1 - \frac{\pi^2}{6(n-1)^2}\right)^{\ell} \|\Pi(\mathcal{L}^{(0)}) - \mu\|_2,$$

and the claim follows. □

We next give a general lemma for dynamical system defined by a tridiagonal Toeplitz matrix.

Proposition 12. *Let $\tau, \beta > 0$ and $\alpha = 1 - 2\beta$. For $y \in \mathbf{R}^k$, consider the dynamical system $\mathcal{S} = \{\mathbf{T}(\alpha,\beta)y + (\tau,\ldots,\tau)\}$, where $\mathbf{T}$ is the tridiagonal Toeplitz matrix*

$$\mathbf{T}(\alpha,\beta) = \begin{bmatrix} \alpha & \beta & & \\ \beta & \alpha & \beta & \\ & \ddots & \ddots & \beta \\ & & \beta & \alpha \end{bmatrix} \in \mathbb{R}^{k\times k}.$$

Then $\mathcal{S}$ has a unique fixed point x^* with $x_i^* = \frac{i(k-i)\tau}{2\beta}$. Let $\varepsilon > 0$, $x^{(0)}$ be a starting point for $\mathcal{S}$ and $x^{(\ell)}$ be the point obtained after ℓ iterations. We have $\|x^{(\ell)} - x^*\|_\infty \leqslant \varepsilon$ as soon as

$$\ell \geqslant \frac{2k^2}{\beta\pi^2}\log\left(\frac{\|x^{(0)} - x^*\|}{\varepsilon}\right).$$

Proof. Let us first assume a fixed point x^* exists. Such a point must satisfy

$$\begin{aligned}\frac{\tau}{\beta} &= 2x_1^* - x_2^* = 2x_{k-2}^* - x_{k-1}^* \\ &= 2x_i^* - x_{i+1}^* - x_{i-1}^* \text{ for } 2 \leqslant i \leqslant k-2.\end{aligned}$$

By induction, for $2 \leqslant i \leqslant k-2$, these equalities imply

$$x_i^* = ix_1^* - \frac{i(i-1)\tau}{2\beta}, \tag{15}$$

$$x_{k-(i+1)}^* - x_{i+1}^* = 2(x_{k-i}^* - x_i^*) - (x_{k-(i-1)}^* - x_{i-1}^*). \tag{16}$$

Let $\delta = x_{k-1}^* - x_1$ and observe that we have $x_{k-2}^* = x_2^* + 2\delta$. Substituting x_{k-2}^* and x_2^* with Identity (15), we obtain on the one hand $x_1^* = 2\delta + \frac{(k-1)\tau}{2\beta}$. On the other hand we have $x_{k-2}^* = 2x_{k-1}^* - \frac{\tau}{\beta}$, so with Identity (15) we obtain $x_{k-1}^* = (k-2)\delta + \frac{(k-1)\tau}{2\beta}$. This yields $x_{k-1}^* - x_1^* = \delta = (k-4)\delta$ so either $k = 4$ or $\delta = 0$. We readily check that $k = 4$ implies nevertheless that $\delta = 0$, so in any case we obtain $x_1^* = x_{k-1}^* = \frac{(k-1)\tau}{2\beta}$, and also also that $x_{k-2}^* = x_2$. This, by induction on Identity (16), we obtain $x_{k-i}^* = x_i^*$ for the remaning i's. Now that x_1^* is known, the claimed formula for the fixed point follows by substitution in Identity (15).

Now, we can write by induction that $\|x^{(\ell)} - x^*\| \leqslant \|\mathbf{T}(\alpha,\beta)\|^\ell \|x^{(0)} - x^*\|$. From e.g. [16, Section 2, (2.7)], the largest eigenvalue of $\mathbf{T}(\alpha,\beta)$ is $\lambda = 1 - 2\beta(1 - \cos(\pi/k))$, and it gives the spectral norm as $\mathbf{T}(\alpha,\beta)$ is symmetric. By routine calculations , one checks that $1 - \cos(\pi/k) \geqslant \frac{\pi^2}{4k^2}$ and gets

$$\|x^{(\ell)} - x^*\| \leqslant \left(1 - \frac{\beta\pi^2}{2k^2}\right)^\ell \|x^{(0)} - x^*\| \leqslant \exp\left(-\ell \cdot \frac{\beta\pi^2}{2k^2}\right)\|x^{(0)} - x^*\|.$$

The result follows using norm equivalence and taking logarithms. □

Proof (of Theorem 3). To lighten notation, let us write $\gamma = \sqrt{\gamma_{\mathcal{O}}(d,r)}$. First, we describe the filtration after one iteration of the algorithm. Expressing that primal and dual filtrations have been reduced, Inequalities (5) and (12) translate here as:

$$(P_j): \quad \operatorname{Vol} \mathcal{L}_{(j-1)d+r} / \mathcal{L}_{(j-1)d} \leqslant \gamma \cdot \left(\operatorname{Vol} \mathcal{L}_{jd} / \mathcal{L}_{(j-1)d}\right)^{r/d}, \text{ for } 1 \leqslant j \leqslant k,$$

$$(D_j): \quad \gamma^{-1}\left(\operatorname{Vol} \mathcal{L}_{jd+r} / \mathcal{L}'_{r+(j-1)d}\right)^{r/d} \leqslant \operatorname{Vol} \mathcal{L}_{jd+r} / \mathcal{L}_{jd}, \text{ for } 1 \leqslant j \leqslant k-1.$$

These conditions are also verified by the filtration $(\mathcal{L}^{(\ell)})_{j \leqslant kd}$, obtained after ℓ iterations of the loop. Let $\mathbf{x}_i^{(\ell)}$, resp. $\mathbf{y}_i^{(\ell)}$ be the i-th coordinate of $\mathcal{P}(\mathcal{L}^{(\ell)})$, resp.

$\mathcal{D}(\mathcal{L}^{(\ell)})$. The conditions above rewrite as the additive relations

$$(P_1^{(\ell)}): \quad \mathbf{y}_1^{(\ell)} \leqslant \log\gamma + \frac{r}{d}\mathbf{x}_1^{(\ell)}, \quad (P_k^{(\ell)}): \quad \mathbf{y}_k^{(\ell)} \leqslant \log\gamma + \frac{d-r}{d}\mathbf{x}_{k-1}^{(\ell)},$$
$$(P_j^{(\ell)}): \quad \mathbf{y}_j^{(\ell)} \leqslant \log\gamma + \frac{r}{d}\mathbf{x}_{j-1}^{(\ell)} + \frac{d-r}{d}\mathbf{x}_j^{(\ell)}, \text{ for } 2 \leqslant j \leqslant k-1,$$
$$(D_j^{(\ell)}): \quad \mathbf{x}_j^{(\ell)} \leqslant \frac{d-r}{d}\mathbf{y}_{j+1}^{(\ell)} + \frac{r}{d}\mathbf{y}_j^{(\ell)} + \log\gamma, \text{ for } 1 \leqslant j \leqslant k-1.$$

In other words, we have (component-wise) $\mathbf{y}^{(\ell)} \leqslant \mathbf{P}\mathbf{x}^{(\ell)} + \log\gamma \cdot \mathbf{1}_{k-1}$ and $\mathbf{x}^{(\ell)} \leqslant \mathbf{P}^t\mathbf{y}^{(\ell)} + \log\gamma \cdot \mathbf{1}_k$, where $\mathbf{1}$ is the vector with all coordinates equal to one, and

$$\mathbf{P} = \begin{bmatrix} \frac{r}{d} & & \\ \frac{d-r}{d} & \frac{r}{d} & \\ 0 & \frac{d-r}{d} & \frac{r}{d} \\ & & \frac{d-r}{d} \end{bmatrix} \in \mathbb{R}^{k\times(k-1)}.$$

The behaviour of the elements $\mathcal{L}_{id}$ are therefore determined by the dynamical system

$$\mathbf{x}^{(\ell)} \leqslant \mathbf{P}^t\mathbf{P}\mathbf{x}^{(\ell)} + 2\log\gamma \cdot \mathbf{1}_{k-1}. \tag{17}$$

Let $\beta = \frac{r(d-r)}{d^2}$ and $\alpha = 1 - 2\beta$, so that

$$\mathbf{P}^t\mathbf{P} = \begin{bmatrix} \alpha & \beta & & \\ \beta & \alpha & \beta & \\ & \ddots & \ddots & \beta \\ & & \beta & \alpha \end{bmatrix} \in \mathbb{R}^{(k-1)\times(k-1)}.$$

The results follows from Proposition 12. □

Corollary 3. Let $\varepsilon > 0$. For an input filtration $(\mathcal{L}_i)_{i\leqslant kd}$ and parameters $1 \leqslant r < d$, let ℓ be such that

$$\ell \geqslant \frac{2n^2}{\pi^2 r(d-r)} \log\left(\frac{\sqrt{k-1}\cdot \max_{i\leqslant k} |\deg(\mathcal{L}_i) - \mu_i|}{d\log(1+\varepsilon)}\right).$$

Assume that Algorithm 2 is aborted after ℓ turns and outputs its current filtration $(\mathcal{L}'_i)_{i\leqslant nd}$. An additional call to a **DensestSublattice** oracle in $\mathcal{L}'_d$ gives a lattice $\mathcal{L}'_r \subset \mathcal{L}$ satisfying

$$\mathrm{Vol}(\mathcal{L}'_r)^{1/r} \leqslant (1+\varepsilon)\cdot(\gamma_{\mathcal{O}}(d,r))^{\frac{n-r}{2r(d-r)}}\,\mathrm{Vol}(\mathcal{L})^{1/n}.$$

Proof. From Theorem 3, the choice of ℓ tells us that $\|\mathcal{P}(\mathcal{L}^{(\ell)}) - \mu\|_\infty \leqslant d\log(1+\varepsilon)$. Using the definition of μ_1, this implies that

$$\mathrm{Vol}(\mathcal{L}'_d)^{1/d} \leqslant (1+\varepsilon)\cdot(\sqrt{\gamma_{\mathcal{O}}(d,r)})^{\frac{n-d}{r(d-r)}}\,\mathrm{Vol}(\mathcal{L})^{1/n}.$$

The last call to the oracle provides $\mathcal{L}'_r$ such that $\mathrm{Vol}(\mathcal{L}'_r) \leqslant \sqrt{\gamma_{\mathcal{O}}(d,r)}\cdot\mathrm{Vol}(\mathcal{L}'_d)^{r/d}$. The claim follows noting that $\frac{1}{r} + \frac{n-d}{r(d-r)} = \frac{n-r}{r(d-r)}$.

D Proofs of Section 5

Lemma 14. Let $\mathbf{K}$ be a number field of degree d. For any $\mathbf{Q}$-free family $(v_1, \dots, v_{id+1})$ of a $\mathbf{K}$-vector space, we have: $i+1 \leqslant \dim \mathrm{Span}_{\mathbf{K}}(v_1, \dots, v_{id+1}) \leqslant id+1$.

Proof. Let $(v_1, \dots, v_\ell)$ be a $\mathbf{Q}$-free family spanning the $\mathbf{Q}$-linear space V. Define $\overline{V} = \mathrm{Span}_{\mathbf{K}}(v_1, \dots, v_\ell)$, which has a dimension $\bar{\ell} \leqslant \ell$. As $\mathbf{Q}$-linear spaces, V is a subspace of $\overline{V}$. This implies that $\bar{\ell} \leqslant \ell \leqslant d\bar{\ell}$. Applying this with $\ell = id+1$ and using that the dimension is an integer, we get the result.

Proof (of Proposition 9). Take $(e_1, \dots, e_{id+1}) \in \mathcal{L}$, with the uniform bound $\|e_j\|_{\pi^{\mathbf{Z}}(\mathcal{L})} \leqslant A$ for some arbitrary constant A. Then we have by AG inequality that $H(e_j) \leqslant \frac{A}{\sqrt{d}}$. If moreover $(e_1, \dots, e_{id+1})$ is a $\mathbf{Q}$-free family, Lemma 14 implies the existence of $\mathbf{K}$-free elements $e_{j_1}, \dots e_{j_{i+1}}$ in $\mathcal{L}$. This concludes the lemma by the definition of successive minima. □

Proof (of Lemma 13). By Lemma 3, we can assume that $\mathcal{L}$ is given in Steinitz form $\mathcal{L} = \mathcal{O}b_1 \oplus \cdots \oplus \mathcal{O}b_{n-1} \oplus \mathfrak{s}b_n$. There is a $d \in \mathcal{O}$ such that $d\mathfrak{s} \subset \mathcal{O}$, so up to scaling by such a d, we can assume that $\mathcal{L}$ is a full-rank sublattice of $E = \mathcal{O}b_1 \oplus \cdots \oplus \mathcal{O}b_n$. This inclusion pushes forward to their $\mathbf{Z}$-lattice versions, and thus we have $\mathrm{Vol}(\pi^{\mathbf{Z}}(\mathcal{L})) = [\mathcal{O} : \mathfrak{s}] \mathrm{Vol}(\pi^{\mathbf{Z}}(E))$. By definition of the algebraic norm we have $\mathrm{N}(\mathfrak{s}) = [\mathcal{O} : \mathfrak{s}]$ and it remains to compute the volume of E. Consider the lattice $\widetilde{E}$ with basis $(\widetilde{b}_i)_i$, the Gram-Schmidt of the b_i's for the form g and let $\alpha_i = g(\widetilde{b}_i, \widetilde{b}_i)^{1/2}$. Every element $(\mathcal{O}, \widetilde{b}_i, g)$ in its pseudo-basis is isometric to the ideal lattice $E_i = (\mathcal{O}\alpha_i, 1, 1)$. Thanks to orthogonality, this extends to an isometry of lattices from $\widetilde{E}$ to the direct sum $E_1 \oplus \cdots \oplus E_n$, with form given by the identity (the "standard $\mathbf{K}_{\mathbf{R}}$-form"). Hence $\mathrm{Vol}(\pi^{\mathbf{Z}}(\widetilde{E})) = \prod_{i \leqslant n} \mathrm{Vol}(\pi^{\mathbf{Z}}(E_i))$, and so we can conclude by computing the volume of these rank d $\mathbf{Z}$-lattices. By definition of the algebraic norm in term of multiplication matrices, we have $\mathrm{Vol}(\pi^{\mathbf{Z}}(E_i)) = \mathrm{N}(\alpha_i) \mathrm{Vol}(\pi^{\mathbf{Z}}((\mathcal{O}, 1, 1)))$. As $\pi^{\mathbf{Z}}(\mathcal{O})$ is nothing but $\mathcal{O}$ seen through one of its $\mathbf{Z}$-bases, the results follows from the definition of the discriminant. □

Proof (of Lemma 15). Let $(\mathfrak{a}_i, b_i)_{i \leqslant k}$ be a pseudo-basis for $\mathcal{M}$, so that $(\mathfrak{a}_i^\dagger, b_i^\vee)_{i \leqslant k}$ be a pseudo-basis of $\mathcal{M}$ resp. $\mathcal{M}^\dagger$. As $\mathbf{Z}$-modules, the fractional ideals of $\mathcal{O}$ are free of rank $d = [\mathbf{K} : \mathbf{Q}]$. On the one hand, we can thus find bases as $\mathfrak{a}_i = \bigoplus_{j \leqslant d} \mathbf{Z}\alpha_{ij}$, and since the b_i's are $\mathbf{K}$-linearly independent, the family $(\alpha_{ij} b_i)_{i \leqslant k, j \leqslant d}$ is $\mathbf{Z}$-linearly independent. It is therefore a $\mathbf{Z}$-basis of the module $\pi_\star(\mathcal{M})$. On the other hand, since $\mathfrak{a}_i^\dagger$ is the $\mathbf{Z}$-dual of $\mathfrak{a}_i$, it is generated as a $\mathbf{Z}$-module as $\mathfrak{a}_i^\dagger = \bigoplus_{j \leqslant d} \mathbf{Z}\beta_{ij}$, with the condition that $\mathrm{Tr}(\overline{\beta_{ij}}\alpha_{i'j'}) = 1$ if $i = i', j = j'$ and 0 otherwise — this is the dual basis for the trace form. We now identify the family $(\beta_{ij} b_i^\vee)_{i \leqslant k, j \leqslant d}$ to the dual basis of $\pi_\star(\mathcal{M})$ and conclude by unicity of the dual basis. Indeed, we have by bilinearity of g

$$\mathrm{Tr}(g(\beta_{ij} b_i^\vee, \alpha_{i'j'} b_i')) = \mathrm{Tr}(\overline{\beta_{ij}}\alpha_{i'j'} \cdot g(b_i^\vee, b_{i'})),$$

which is 1 if and only if $i = i', j = j'$, and 0 otherwise. □

E Proof of Section 6

Proposition 11. Let $T(\mathcal{O}, n, k) = k|\Delta(\mathcal{O})|^{\frac{1}{d}}\gamma_{\mathcal{O}}(n, 1)$. The densestSublattice algorithm (Algorithm 3) retrieves the densest sublattice in time $(dT(\mathcal{O}, n, k)\deg(\mathcal{L}))^{k\log(dT(\mathcal{O},n,k)\deg(\mathcal{L}))}$ and a linear number of calls to an enumeration oracle with bound $T(\mathcal{O}, n, k)\deg(\mathcal{L})$.

Proof. We first show correctness. By construction, $W_{\mathbf{R}}$ is the $\mathbf{K}$-linear span of all smallest rank 1 sublattice of $\mathcal{L}$. If this candidate is not of rank k we need to complete it first. But remark that for any sublattice D, $\mathrm{Vol}(D \cap \mathcal{L}) = \mathrm{Vol}(W \cap \mathcal{L})\deg\left(D \cap \mathcal{L}/W\right)$, we deduce that $\mathrm{Vol}(D \cap \mathcal{L})$ is minimized for minimal $\mathrm{Vol}\left(D \cap \mathcal{L}/W\right)$, since the quantity $\mathrm{Vol}(W \cap \mathcal{L})$ is independent of D. Hence, it is discovered recursively by the call of line 4, when the rank of W is not k. Then, the algorithm considers all k-subsets of rank 1 sublattices of degree smaller than a fraction k of the densest line lattice, and bookkeep the best solution found. Hence, since the desired solution either contains all shortest rank 1 sublattices and is found before this loop or it contains k-linearly independent rank 1 sublattice of length at most $k|\Delta(\mathcal{O})|^{\frac{1}{d}}$ times the minimal degree, and it is necessarily found during one of the iterations.

Now for the complexity, the number of recursive call in line 4 is bounded by the rank of the lattice. The callee itself starts by enumerating the lines of degree lower than $T(\mathcal{O}, n, k)\deg(\mathcal{L})$. There are at most

$$N = (dT(\mathcal{O}, n, k)\deg(\mathcal{L}))^{\log(T_{\mathcal{O}},n,k)\deg(\mathcal{L}))}$$

such elements (by counting the number of times a prime element can appear in the decomposition of the ideal). We then need to enumerate on the subsets of size k in the main loop, which can be done in $\binom{N}{k}$ time.