Reductions from module lattices to free module lattices

Alice Pellet-Mary, Nam Tran

Reductions from module lattices to free module lattices

Alice Pellet-Mary[1] and Nam Tran[2,3]

[1] Univ. Bordeaux, CNRS, INRIA, Bordeaux INP, IMB, Talence, France, alice.pellet-mary@math.u-bordeaux.fr
[2] Institute of Cybersecurity and Cryptology, School of Computing and Information Technology, Univ. of Wollongong, Australia, ndt141@uowmail.edu.au
[3] CSIRO Data61, Australia

Abstract. In this article, we give evidences that free modules (i.e., modules which admit a basis) are no weaker than arbitrary modules, when it comes to solving cryptographic algorithmic problems (and when the rank of the module is at least 2). More precisely, we show that for three algorithmic problems used in cryptography, namely the shortest vector problem, the Hermite shortest vector problem and a variant of the closest vector problem, there is a reduction from solving the problem in any module of rank $n \geq 2$ to solving the problem in any *free* module of the same rank n.

1 Introduction

Lattice-based algorithmic problems using algebraic lattices, such as the NTRU problem [HPS06], the Ring LWE [SSTX09, LPR13] and Ring SIS [LM06, PR06] problems, or the Module LWE and Module SIS problems [BGV14, LS15], have been used as security foundation for many cryptographic primitives. As an example of the importance of such problems, 3 out of 4 algorithms standardized by the NIST in July 2022 are based on one of these algebraic lattice problems.[4] One of the main advantages of using algebraic lattices compared to standard lattices is that the extra structure added to the lattices allows for less resource for storage and enables faster algorithms for computation, thus improving efficiency. Another advantage of the algebraic structure is that it allows to multiply elements, which can be useful for applications like homomorphic encryption [Gen09a, Gen09b] or obfuscation [GGH+16].

All the five algorithmic problems mentioned above enjoy reductions from (various) worst-case problems over algebraically structured lattices, called module and ideal lattices (see [PS21, FPS22] for the reductions to the NTRU problem, [LM06, PR06] for Ring SIS, [SSTX09, LPR13] for Ring LWE, and [LS15] for module SIS and module LWE). These worst-case algorithmic problems over modules and ideals provide lower bounds on the hardness of the NTRU, Ring/Module SIS and Ring/Module LWE problems, and hence on the security of the schemes

[4] https://csrc.nist.gov/projects/post-quantum-cryptography

based upon them. At a high level, a module can be seen as a lattice, but defined over a ring which is not the ring $\mathbb{Z}$. More formally, let K be a number field of degree d. For simplicity in this introduction, we will focus on $K = \mathbb{Q}[X]/(X^d+1)$ with d a power-of-two, which is a cyclotomic field. This field has a ring of integers $\mathcal{O}_K$, which in our example is equal to $\mathbb{Z}[X]/(X^d+1)$. An $\mathcal{O}_K$-module M in K^m is a subset of K^m generated by a finite set of vectors $\mathbf{v}_1, \ldots, \mathbf{v}_k \in K^m$, i.e.,

$$M := \{\alpha_1\mathbf{v}_1 + \ldots + \alpha_k\mathbf{v}_k : \alpha_1, \ldots, \alpha_k \in \mathcal{O}_K\}.$$

An ideal is a special case of the above definition, corresponding to the case where the generating set is a finite subset of K (i.e., $m = 1$ in the definition above). An important remark in this definition is that the vectors $\mathbf{v}_1, \ldots, \mathbf{v}_k$ are not required to be linearly independent: they generate the module, but they might not be a basis of the module.

This remark actually highlights a key difference between modules over the ring of integers $\mathcal{O}_K$ and lattices over the ring $\mathbb{Z}$. Indeed, the ring $\mathcal{O}_K$ is usually not a principal ideal domain (at least for our running example with K cyclotomic). This means that module lattices do not always have bases over $\mathcal{O}_K$ (contrary to lattices which always have bases over $\mathbb{Z}$). Instead, a module M over $\mathcal{O}_K$ admits pseudo-bases, which consist in n linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$ of K^m and n ideals $I_1, \ldots, I_n$ such that $M = \{\sum_i x_i\mathbf{b}_i \,|\, x_i \in I_i\}$. The integer n is called the rank of the module M.

In some cases, a module M admits a basis, that is, a pseudo-basis where all the coefficient ideals I_i are equal to $\mathcal{O}_K$. In this case, the module M is said to be a *free module*. In the case of ideals (i.e., modules included in K), an ideal admitting a basis is usually called a *principal ideal* (and not a free ideal). We note that, in our example rings, free modules represent a very small portion of the set of all modules.[5] Moreover, even when a module M is free, computing a basis of it from a generating set (or a pseudo-basis) might be challenging. It can be performed in *quantum* polynomial time, but only in subexponential classical time so far (more details can be found in preliminaries). In this article, the main question we try to answer is the following: if we restrict ourselves to free modules represented by a basis (and not any pseudo-basis), do algorithmic problems like the shortest vector problem or the closest vector problem become easier to solve? (When compared to the problems over arbitrary modules, represented by a pseudo-basis.)

So far, the answer to this question is not so clear. There have been some algorithms exploiting the specific structure of free modules or principal ideals, but these algorithms were later extended to all modules or all ideals. For example, [CDPR16] introduced in 2016 an algorithm to compute relatively short elements in *principal ideals* of a cyclotomic field, which was generalized to all ideals one year later in [CDW17]. Another example is the LLL algorithm for module lattices from [LPSW19], which runs in classical polynomial time for free

[5] In the case of ideals for instance, we know that the proportion of principal ideals among all ideals is equal to $1/h_K$, where h_K is a quantity called the class number of the field K. When K is a cyclotomic field, it is known that h_K grows more than exponentially in the degree d of the number field (see, e.g., [Law97, Proposition 11.15]).

modules (represented by a basis) but only in quantum polynomial time for arbitrary modules. Again, it was showed a few years later in [DM22] that one can have a classical algorithm also for arbitrary modules. At the moment, we are not aware of any algorithm that would behave significantly better on free modules (respectively principal ideals) than on arbitrary modules (respectively arbitrary ideals). This might highlight the fact that free modules are not really weaker than arbitrary modules, when it comes to algorithmic problems such as the shortest vector problem.

Contributions. In this article, we give more evidence that free modules already capture all the hardness contained in arbitrary modules, for modules of rank ≥ 2. More formally, we prove that it is possible to reduce three algorithmic problems from their variant over module lattices to their variant over free-module lattices (represented by a basis). The three problems we consider in this work are: the shortest vector problem (SVP), the Hermite shortest vector problem (HSVP) and a variant of the closest vector problem ($\mathrm{CVP}_{\mathrm{cov}}$). In the variant of CVP we consider, we want to find a lattice point $\mathbf{s}$ close to a target $\mathbf{t}$, such that $\|\mathbf{t}-\mathbf{s}\| \leq \gamma \cdot \mathrm{cov}(\mathcal{L})$, where $\gamma \geq 1$ is some approximation factor and $\mathrm{cov}(\mathcal{L})$ is the covering radius of the lattice $\mathcal{L}$ (in the standard CVP problem, we usually asks that $\|\mathbf{t}-\mathbf{s}\| \leq \gamma \cdot \mathrm{dist}(\mathbf{t}, \mathcal{L})$, where $\mathrm{dist}(\mathbf{t}, \mathcal{L})$ is the minimal distance between $\mathbf{t}$ and a point of $\mathcal{L}$).

For an algorithmic problem $\mathcal{P}$, let us write n-module-$\mathcal{P}$ the worst-case problem $\mathcal{P}$ restricted to module lattices of rank n included in K^n, and n-free-module-$\mathcal{P}$ the worst-case problem $\mathcal{P}$ restricted to free-module lattices of rank n included in K^n and represented by a basis. We prove the following theorem.

Theorem 1.1 (Informal, see Theorems 6.1, 6.2 and 6.3). *Let $n \geq 2$ be an integer. Then, there exist probabilistic polynomial time reductions*

- *from n-module-SVP to n-free-module-SVP;*
- *from n-module-HSVP to n-free-module-HSVP;*
- *from n-module-CVP_{cov} to n-free-module-CVP_{cov}.*

The approximation factors achieved by these reductions are polynomial in some quantities depending on the number fields, in n, and in the approximation factor of the oracle solving the problem in free modules (see Theorems 6.1, 6.2, 6.3 for more details). Moreover, one can check that the reductions from the theorem require only two calls to an oracle solving the free-module-$\mathcal{P}$ problem in order to solve one instance of the module-$\mathcal{P}$ problem (where $\mathcal{P} \in \{\mathrm{SVP}, \mathrm{HSVP}, \mathrm{CVP}_{\mathrm{cov}}\}$).

Techniques. The three reductions, for SVP, HSVP and $\mathrm{CVP}_{\mathrm{cov}}$ follow the same framework. Let $\mathcal{P}$ be one of the three problems. We first reduce $\mathcal{P}$ in modules to $\mathcal{P}$ is free modules *and* HSVP in ideals (Section 3). Then, we reduce HSVP in ideals to $\mathcal{P}$ in free modules of rank 2 (Section 4). Finally, we reduce $\mathcal{P}$ in free modules of rank 2 to $\mathcal{P}$ in free modules of rank $n \geq 2$ (Section 5). Combining these three reductions, we obtain a reduction from $\mathcal{P}$ in modules of rank n to $\mathcal{P}$ in free modules of rank n for any $n \geq 2$.

Let us focus a bit more on each of the three subreductions. For the reduction from module-$\mathcal{P}$ to free-module-$\mathcal{P}$ and HSVP in ideal lattices, the main idea is to use an *almost-free representation* of the input module M, that is, a pseudo-basis of M of the form $((\mathbf{b}_i, I_i))_{1\leq i\leq n}$ with $I_i = \mathcal{O}_K$ for all $i \leq n-1$. Such a pseudo-basis can be computed in probabilistic polynomial time from any pseudo-basis of M. Then, we use the oracle solving HSVP in ideals to compute a short element $x \in I_n$, and we consider the free module N given by the basis $(\mathbf{c}_i)_{1\leq i\leq n}$, where $\mathbf{c}_i = \mathbf{b}_i$ for $i \leq n-1$ and $\mathbf{c}_n = x \cdot b_n$. One can check that N is a free module included in M. It can also be checked that N is not much sparser than M. Both properties imply that solving $\mathcal{P}$ in N also provides a solution to $\mathcal{P}$ in M, with some controlled loss in the approximation factor.

In the second step of the reduction, we want to find a short element of an ideal, given access to an oracle solving $\mathcal{P}$ in free modules of rank 2. Here, the main idea is to consider a *two-element representation* of the input ideal, that is, two elements of K that, together, generate the ideal. This two-element representation can be computed in probabilistic polynomial time from any basis of the ideal. We then show that, by solving a free-module-$\mathcal{P}$ instance in a free module of rank 2 constructed from the two elements found before, it is possible to find a short element of the input ideal. Similar techniques were used in [DM22] in order to transform modules of rank 2 into free modules of rank 4.

Finally, the last part of the reduction is to reduce $\mathcal{P}$ from free modules of rank 2 to free modules of rank $n \geq 2$. The strategy here is quite natural: we embed the input module of rank 2 into a larger module of rank n. The naive strategy is, for instance, to consider the direct orthogonal sum of the input module M with the free module $\mathcal{O}_K^{n-1}$ of rank $n-2$ (possibly scaled). This works well for SVP and $\mathrm{CVP}_{\mathrm{cov}}$, but surprisingly, this does not seem to work for HSVP. Instead, for HSVP, we construct a module of rank n from M by gluing $\lfloor n/2 \rfloor$ orthogonal copies of M together, and adding an extra orthogonal copy of $\mathcal{O}_K$ if n is odd. This provides a reduction for HSVP which has some significant loss in the approximation factor when n is odd (whereas we had almost no loss for SVP and $\mathrm{CVP}_{\mathrm{cov}}$). We believe that it would be an interesting open problem to reduce this loss in the HSVP case (or, on the contrary, show that this loss is mandatory).

Discussion. In this introduction, we focused on the special case of cyclotomic number fields. However, our results are not restricted to cyclotomic number fields, but can be used in any number field K. In full generality, number fields might be principal, or have a very small class number. This means that in this case, most of the modules in these number fields are free (the cyclotomic fields are quite the exception, with their very large class number). However, even if all $\mathcal{O}_K$-modules are free, our reduction might still be interesting. Indeed, we have seen that it is in general hard to compute a basis of a free module without a quantum computer. Our reduction provides a way to transform *classically* a problem over a free module represented by a pseudo-basis into two instances of the same problem over free modules represented by a basis.

One of the consequence of our results is that it provides an alternative proof to obtain a fully classical LLL algorithm over any module. Recall that the authors of [LPSW19] described an LLL algorithm for modules, which was by default a quantum algorithm (if given as input a pseudo-basis of a module), but could be run in classical polynomial time in the specific case where the input module was free and represented by a basis. This algorithm was made fully classical (for all modules) in [DM22]. In this work, the authors focused on the quantum steps of the LLL algorithm for modules from [LPSW19], and showed that these steps could actually be run in classical polynomial time, by using some techniques similar to the ones we use in Section 4. Our reductions allow to obtain a similar result in a more straightforward way: one can simply use the reduction from module-SVP to free-module-SVP from Theorem 1.1, and then apply the classical polynomial time LLL algorithm for free modules from [LPSW19], in order to solve classically the two free-module-SVP instances produced by the reduction.

In this article, we restricted ourselves to prove reductions for three lattice problems, namely SVP, HSVP and $\mathrm{CVP}_{\mathrm{cov}}$, which we thought were somewhat standard and representative of the variety of lattice problems. We did not try to see if our reduction framework could be adapted to the large set of other lattice problems (see, e.g., [Ste15, page 1] for a non-exhaustive list of problems). However, we did try to use our framework to prove a reduction for the standard CVP problem,[6] instead of the variant $\mathrm{CVP}_{\mathrm{cov}}$ that we used, but did not succeed. The issue with the standard formulation of CVP stems from the fact that if a target is unexpectedly close to a lattice point, then we may have to find a lattice point whose distance to the target is significantly smaller than the covering radius of the lattice. Interestingly, it seems that our framework can be used in the cases where the target is very close to the lattice (closer than the minimal distance of the lattice) or relatively far away (at a distance of the order of the covering radius of the lattice), but we do not know how to handle the cases in between. We leave it as an open problem to obtain a reduction similar to ours, for the standard CVP problem.

Finally, we remark that another way to obtain reductions from (non free) module problems to free module problems could be to use the reductions from worst-case ideal/module problems to NTRU, Ring/Module LWE or Ring/Module SIS. Indeed, the NTRU, Ring/Module LWE and Ring/Module SIS problems can be reduced to problems over modules (either the shortest vector problem or the bounded distance decoding problem), and the modules that are produced by these reductions are often free and with an easily computable basis. As an example, a Ring LWE instance with good parameters can be reduced to a bounded distance decoding problem in a module M of rank 2 in $\mathcal{O}_K^2$ spanned by three vectors $(a_1, a_2)^T$, $(q, 0)^T$ and $(0, q)^T$. If a_1 is coprime with q (which should happen with relatively high probability), then there exists $u, v \in \mathcal{O}_K$ such that $ua_1 + vq = 1$ and in this case the two vectors $(1, ua_2)^T$ and $(0, q)^T$ form a basis

[6] Recall that the standard CVP problem asks, given as input a target $\mathbf{t}$, to find a point $\mathbf{s}$ of the lattice $\mathcal{L}$ such that $\|\mathbf{t} - \mathbf{s}\| \leq \gamma \cdot \mathrm{dist}(\mathbf{t}, \mathcal{L})$, for some approximation factor γ.

of the module M (which is then free). Even if this approach seems a possible alternative way to obtain reductions from arbitrary modules to free modules, we would like to highlight some advantages of the approach we chose in this article. First of all, the reductions from worst-case ideal/module problems to Ring/Module LWE and Ring/Module SIS do not preserve the rank of the modules, whereas our reductions transform modules into free modules of the same rank (this is also a limitation for the reduction to NTRU from [PS21], but not for the reduction from [FPS22], which preserves the rank). Another limitation of the approach using Ring/Module LWE is that the reductions from worst-case problem to Ring/Module LWE are quantum, whereas our reductions are classical (this is a limitation only for Ring/Module LWE, not for NTRU or Ring/Module SIS which enjoy classical reductions). Finally, one last advantage of our reductions is that the framework is quite simple, and does not require the heavy machinery of the worst-case to average-case reductions of NTRU, Ring/Module LWE and Ring/Module SIS. In particular, our reduction could be easily implemented, and should be quite efficient. Also, we believe that the general framework we describe might be used to derive reductions for other algorithmic problems, in case they are needed.

2 Preliminaries

We let $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ denote the set of integers, rationals, real and complex numbers respectively. For a positive real number x, we let $\log(x)$ denote the logarithm of x in base 2. Throughout this article, we let bold lowercase letters denote vectors. All vectors are column vectors with the coordinates denoted by normal lowercase letter with subsripted index, for example

$$\mathbf{v} = \begin{pmatrix} v_1 \\ \vdots \\ v_d \end{pmatrix} \in \mathbb{R}^d$$

is a column vectors with coordinates $v_1, \ldots, v_d \in \mathbb{R}$. We let $\mathbf{v}^T$ denote the transpose of $\mathbf{v}$. We write $\|\mathbf{v}\|_2 = \sqrt{\sum_i v_i^2}$ and $\|\mathbf{v}\|_\infty = \max_i |v_i|$ to denote the ℓ_2-norm and the ℓ_∞-norm respectively. We mostly work with the ℓ_2-norm and ignore the subscript index when there is no confusion.

2.1 Lattices

A lattice $\mathcal{L}$ is a set of linear combinations with integer coefficients of $\mathbb{R}$-linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^m$

$$\mathcal{L} = \{a_1\mathbf{b}_1 + \ldots + a_n\mathbf{b}_n \ : \ a_1, \ldots, a_n \in \mathbb{Z}\}.$$

The (ordered) set of vectors $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ forms a *basis* of $\mathcal{L}$, and can be represented by a matrix $\mathbf{B} \in \mathbb{R}^{m \times n}$ whose columns are the vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$. The

integer n is the rank of the lattice $\mathcal{L}$. Given a basis $\mathbf{B} \in \mathbb{R}^{m \times n}$ of $\mathcal{L}$, the determinant (or volume) $\det(\mathcal{L})$ is defined as $\det(\mathbf{B}^T\mathbf{B})^{1/2}$. The determinant of a lattice is invariant with respect to any choice of its basis.

For a lattice $\mathcal{L}$ and $i \in \{2, \infty\}$, we let $\lambda_1^{(i)}(\mathcal{L}) = \min\{\|\mathbf{v}\|_i : \mathbf{v} \in \mathcal{L}\backslash\{\mathbf{0}\}\}$ be the length of a shortest non-zero vector of $\mathcal{L}$ with respect to the ℓ_i-norm. We will also use $\lambda_n^{(i)}(\mathcal{L})$, where n is the rank of $\mathcal{L}$, which is the smallest radius $r > 0$ such that there exists n linearly independent vectors in $\mathcal{L}$ of ℓ_i-norm $\leq r$. Again, we mostly work with the ℓ_2-norm and we drop the superscript index when there is no confusion.

Theorem 2.1 (Minkowski's bound). *For a rank-n lattice $\mathcal{L}$, we have*

$$\lambda_1^{(\infty)}(\mathcal{L}) \leq \det(\mathcal{L})^{1/n};$$
$$\lambda_1^{(2)}(\mathcal{L}) \leq \sqrt{n} \cdot \det(\mathcal{L})^{1/n}.$$

We write $\mathrm{Span}_{\mathbb{R}}(\mathcal{L})$ the real span of a lattice $\mathcal{L}$ (not necessarily full rank). The covering radius $\mathrm{cov}(\mathcal{L})$ of a (not necessarily full rank) lattice $\mathcal{L}$ is defined as $\mathrm{cov}(\mathcal{L}) = \max_{\mathbf{t} \in \mathrm{Span}_{\mathbb{R}}(\mathcal{L})} \min_{\mathbf{s} \in \mathcal{L}} \|\mathbf{t} - \mathbf{s}\|$. Equivalently, $\mathrm{cov}(\mathcal{L})$ is the minimal real number $r > 0$ such that for all $\mathbf{t} \in \mathrm{Span}_{\mathbb{R}}(\mathcal{L})$, there exists $\mathbf{s} \in \mathcal{L}$ with $\|\mathbf{t} - \mathbf{s}\| \leq r$. The covering radius of a lattice is a priori hard to compute, but we can show that for any rank-n lattice $\mathcal{L}$, it holds that

$$\mathrm{cov}(\mathcal{L}) \leq n \cdot \lambda_n^{(2)}(\mathcal{L}). \tag{1}$$

Indeed, let $\mathbf{b}_1, \cdots, \mathbf{b}_n$ be linearly independent vectors of $\mathcal{L}$ satisfying $\|\mathbf{b}_i\| \leq \lambda_n^{(2)}(\mathcal{L})$ and let $\mathbf{t} = \sum_i t_i \mathbf{b}_i \in \mathrm{Span}_{\mathbb{R}}(\mathcal{L})$. Then $\mathbf{s} = \sum_i \lfloor t_i \rfloor \mathbf{b}_i \in \mathcal{L}$ and satisfies $\|\mathbf{t} - \mathbf{s}\| \leq \sum_i \|\mathbf{b}_i\| \leq n \cdot \lambda_n^{(2)}(\mathcal{L})$.

On the other hand, we also know that $\mathrm{cov}(\mathcal{L}) \geq 1/2 \cdot \lambda_1^{(2)}(\mathcal{L})$. Indeed, if $\mathbf{s}$ is a shortest nonzero vector of $\mathcal{L}$, then $1/2 \cdot \mathbf{s}$ has to be at distance $\geq \lambda_1^{(2)}(\mathcal{L})/2$ from any lattice point, since otherwise we would have a nonzero vector in $\mathcal{L}$ of euclidean norm $< \lambda_1^{(2)}(\mathcal{L})$.

2.2 Number Fields

Let K be a number field of degree d and $\mathcal{O}_K$ be its ring of integers. The ring $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank d. There exists d embeddings from K to $\mathbb{C}$, denoted by $\sigma_1, \ldots, \sigma_d$. The canonical embedding σ is defined as

$$\forall x \in K, \sigma(x) = (\sigma_1(x), \ldots, \sigma_d(x)) \in \mathbb{C}^d.$$

The number field K, embedded into $\mathbb{C}^d$ via the canonical embedding, has a geometry induced by the geometry of $\mathbb{C}^d$. For $x \in K$, the ℓ_2-norm of x, denoted by $\|x\|$, is defined as the (Hermitian) ℓ_2-norm of the vector $\sigma(x)$ in the space $\mathbb{C}^d$, i.e., $\|x\| := \|\sigma(x)\|$. A similar definition also applies for the ℓ_∞-norm, i.e., $\|x\|_\infty := \|\sigma(x)\|_\infty$ for $x \in K$. For $x, y \in K$, we have the following bound

$$\|xy\| \leq \|x\|_\infty \cdot \|y\| \leq \|x\| \cdot \|y\|.$$

The image $\sigma(\mathcal{O}_K)$ is a rank-d lattice, living in $\mathbb{C}^d \simeq \mathbb{R}^{2d}$ (it is not a full rank lattice in $\mathbb{C}^d$). The volume of $\sigma(\mathcal{O}_K)$ is equal to $\Delta_K^{1/2}$, where Δ_K is the *absolute discriminant* of the number field K and is given by

$$\Delta_K = \left|\det\left(\sigma_i(r_j)\right)_{1\leq i,j\leq d}\right|^2,$$

where $r_1, \ldots, r_d$ is a $\mathbb{Z}$-basis of $\mathcal{O}_K$. The value of Δ_K is invariant from the choice of the basis $r_1, \ldots, r_d$ of $\mathcal{O}_K$. We will also consider the quantity $\lambda_d^\infty(\sigma(\mathcal{O}_K))$, which we will write $\lambda_d^{(\infty)}(\mathcal{O}_K)$ to simplify notations. In the case of cyclotomic fields, we know that $\lambda_d^{(\infty)}(\mathcal{O}_K) = 1$ (since there is a basis of $\mathcal{O}_K$ made of roots of unity). For general number fields, the quantity $\lambda_d^{(\infty)}(\mathcal{O}_K)$ can be larger, but it cannot be too large, as stated in the following lemma from [BST+20] (the original result from [BST+20] only states that $\lambda_d^\infty(\mathcal{O}_K) = O(\Delta_K^{1/d})$, but the constant in the big O can be worked out).

Lemma 2.1 (Adapted from [BST+20, Theorem 3.1]). *For any number field K, it holds that $\lambda_d^\infty(\mathcal{O}_K) \leq \Delta_K^{1/d}$.*

Algorithms. In this article, when we say that an algorithm is *probabilistic polynomial time*, we mean that the algorithm is a Las Vegas type algorithm,[7] whose expected running time is polynomial in the input size of the algorithm and in $\log \Delta_K$. We emphasize that even when Δ_K is not part of the input of the algorithm, we consider that $\log \Delta_K$ is a polynomial quantity.

2.3 Ideals

A fractional ideal I of K is an $\mathcal{O}_K$-submodule of K for which there exists $a \in \mathcal{O}_K \backslash \{0\}$ such that $aI \subset \mathcal{O}_K$. When $I \subset \mathcal{O}_K$, we say that I is an *integral* ideal. The sum and product of two fractional ideals I and I', defined as,

$$I + I' := \{x + y : x \in I, y \in I'\}$$
$$II' := \left\{\sum_{i=1}^{n} x_i y_i : n \in \mathbb{Z}_{>0}, x_i \in I, y_i \in I'\right\}$$

are also fractional ideals. Any non-zero fractional ideal I of K is invertible, meaning that there exists some fractional ideal I^{-1} such that $I \cdot I^{-1} = \mathcal{O}_K$. An ideal $\mathfrak{p}$ is said to be prime if the quotient ring $\mathcal{O}_K/\mathfrak{p}$ is an integral domain. For $x \in K$, we write $\langle x \rangle = x\mathcal{O}_K$ to denote the principal ideal generated by x. We remark that $\mathcal{O}_K$ is a Dedekind domain, in which nonzero proper ideals are uniquely factorized into product of power of prime ideals (the uniqueness is up to the order of the prime factors).

[7] That is, an algorithm whose output is always correct, but whose running time is a random variable.

Ideal lattices and algebraic norm. The image $\sigma(I)$ of a fractional ideal I is a rank-d lattice of $\mathbb{C}^d$. We also refer to such lattices as *ideal lattices*. The algebraic norm of a fractional ideal I, denoted by $\mathcal{N}(I)$, is defined to be the determinant of the lattice $\sigma(I)$ divided by $\Delta_K^{1/2}$. Note that if I is integral, then $\mathcal{N}(I)$ is the index $[\mathcal{O}_K : I]$. Ideals norm is multiplicative, i.e. $\mathcal{N}(IJ) = \mathcal{N}(I) \cdot \mathcal{N}(J)$ for fractional ideals I, J. For a principal ideal $\langle x \rangle$, we write $\mathcal{N}(x)$ to denote the algebraic norm of $\langle x \rangle$. This corresponds to the absolute value of the usual definition of the algebraic norm of an element, i.e., $\mathcal{N}(x) = \left| \prod_{i=1}^{d} \sigma_i(x) \right|$.

For any non-zero element $x \in K$, we have the following relation between the algebraic norm and euclidean norm of x, which is obtained from the inequality of arithmetic and geometric means applied to $(|\sigma_i(x)|^2)_i$.

$$\sqrt{d} \cdot \mathcal{N}(x)^{1/d} \leq \|x\|. \tag{2}$$

This implies in particular that for any element $x \in \mathcal{O}_K$, we have $\|x\| \geq \sqrt{d}$.

For any fractional ideal I, it holds that $\lambda_d(I) \leq \lambda_1(I) \cdot \lambda_d^{(\infty)}(\mathcal{O}_K)$. Indeed, if $s \in I$ is a shortest nonzero element of I for the euclidean norm, and $r_1, \ldots, r_d$ are d linearly independent elements of $\mathcal{O}_K$ satisfying $\|r_i\|_\infty \leq \lambda_d^{(\infty)}(\mathcal{O}_K)$ for all i's, then the elements $r_i \cdot s$ are d linearly independent elements of I and satisfy $\|r_i \cdot s\| \leq \|r_i\|_\infty \cdot \|s\| \leq \lambda_1(I) \cdot \lambda_d^{(\infty)}(\mathcal{O}_K)$. Combining this with Minkowski's inequality and Equation (1) yields

$$\mathrm{cov}(I) \leq d^{3/2} \cdot \lambda_d^{(\infty)}(\mathcal{O}_K) \det(I)^{1/d}. \tag{3}$$

If $I = x\mathcal{O}_K$ is principal, using (2) this can be rewritten

$$\mathrm{cov}(x\mathcal{O}_K) \leq d \cdot \lambda_d^{(\infty)}(\mathcal{O}_K) \cdot \Delta_K^{1/2d} \cdot \|x\|. \tag{4}$$

Two elements representation. Every fractional ideal I in K admits a *two-element representation*, which is a way to write I as a sum of two principal ideals $\langle x \rangle$ and $\langle y \rangle$. The following result states that the two-element representation of an ideal can be computed in expected polynomial time.

Theorem 2.2 (Adapted from Lemma 2.6 of [PS21]). *There exists a probabilistic polynomial time algorithm taking a fractional ideal $I \subset K$ and a nonzero $x \in I$ as inputs, and computing $y \in I$ such that $I = \langle x \rangle + \langle y \rangle$.*

Proof. The proof is nearly identical to that in [PS21], except that we repeat the algorithm until it outputs a valid pair (x, y), instead of allowing the algorithm to fail with small probability. Unwrapping the proof, one can see that the algorithm in [PS21] is obtained by taking the algorithm from [FS10, Fig.1], and setting the element x_1 to be the input x in Step 1. In [FS10], it is proven that the probability p that the algorithm does not fail is at least $1/\mathrm{e}$. Hence, the expected number of iterations of our algorithm is $1/p \leq \mathrm{e}$. □

2.4 Modules

Below, we recall the main results about modules that we will need in this article. For more detailed references about the theoretical and computational aspects of modules over Dedekind domain, we refer the reader to [Hop98, Chapter 4] and [Coh12, Chapter 1].

Let $M \subset K^m$ be a finitely generated $\mathcal{O}_K$-module, then there exists K-linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$ of K^m and fractional ideals $I_1, \ldots, I_n$ such that

$$M = I_1\mathbf{b}_1 + \ldots + I_n\mathbf{b}_n.$$

The set of tuples $((I_i, \mathbf{b}_i))_{i \leq n}$ is called a *pseudo-basis* of M, the positive integer n is called the *rank* of M. In particular, fractional ideals of K are rank-1 $\mathcal{O}_K$-modules. For any rank-n module M in K^m, there exists a canonical pseudo-basis, called the HNF basis of M, which can be computed in polynomial time from any pseudo-basis of M (see, e.g., [Coh12]).

Free modules. A free module is a module M which has a pseudo basis $((I_i, \mathbf{b}_i))_{i \leq n}$ with all the ideals I_i equal to $\mathcal{O}_K$. When this is the case, we say that $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ is a *free basis* of M.[8] We emphasize here that even if the module M is free, not all pseudo-bases of M are free bases. In particular, the HNF basis of a free module has no reason to be a free basis. Moreover, computing a free basis of a free module given as input an arbitrary pseudo-basis is not known to be doable in classical polynomial time. Indeed, computing a free basis of a free module amounts to computing generators of principal ideals, given as input an arbitrary $\mathbb{Z}$-basis of the ideals (since one can efficiently transform any pseudo-basis of a free module into a new pseudo-basis where all the coefficient ideals are principal, using, e.g., the almost free representation discussed in the next section). This can be done in quantum polynomial time [BS16] but only in sub-exponential classical time [BF14] so far.

Almost free representations. For any rank-n module M, there exist pseudo-bases of the form $((\mathbf{b}_i, I_i))_i$, with $I_i = \mathcal{O}_K$ for all $i = 1$ to $n-1$ (i.e., only the last ideal is non-trivial). Such pseudo-bases are called *almost-free representations* of M (or *Steinitz form*). We denote this representation by $(\mathbf{b}_1, \ldots, \mathbf{b}_n, I)$, where I is the coefficient ideal corresponding to $\mathbf{b}_n$. Note that, contrary to the HNF basis, the almost-free representation is not unique: for a given module M, there are many pseudo-bases satisfying $I_i = \mathcal{O}_K$ for all $i = 1$ to $n-1$. Still, it is efficiently computable, as stated in the following lemma.

Lemma 2.2 ([BHJ22, Corollary A.3]). *There is a probabilistic polynomial time algorithm that takes as input any pseudo-basis of a rank-n module M in K^n for some $n \geq 1$, and returns an almost-free representation of M.*

[8] Those are usually simply called "bases", by opposition to the pseudo-bases. But we prefer to add the adjective "free" in this work, to make the distinction even clearer.

Module lattices. The canonical embedding can be extended to K^m, by defining $\sigma(\mathbf{v})$ for $\mathbf{v} = (v_1, \ldots, v_m)^T \in K^m$ to be the concatenation of $\sigma(v_i)$. Then $\sigma(\mathbf{v})$ is a vector of $\mathbb{C}^{md}$ and $\sigma(M)$ is a lattice of rank nd (i.e., non full rank). We refer to such lattices as *module lattices*. We will again abuse notations and write $\|\mathbf{v}\|_2 := \|\sigma(\mathbf{v})\|_2$ and $\|\mathbf{v}\|_\infty := \|\sigma(\mathbf{v})\|_\infty$ for vectors $\mathbf{v} \in K^m$. Similarly, we use M instead of $\sigma(M)$ when we view M as a lattice (e.g., $\lambda_1(M)$, $\det(M)$, ...). In the rest of the article, we will use the observation that $\mathrm{Span}_{\mathbb{Q}}(\sigma(M)) = \sigma(\mathrm{Span}_K(M))$, and we will again abuse notation and write $\mathrm{Span}_K(M)$ for both.

For a rank-n module M in K^n (i.e., a full rank module), we define the norm of M to be

$$\mathcal{N}(M) = \mathcal{N}(\det \mathbf{B}) \cdot \prod_i \mathcal{N}(I_i),$$

where $((\mathbf{b}_i, I_i))_i$ is a pseudo-basis of M and $\mathbf{B}$ is the $n \times n$ matrix with columns $\mathbf{b}_i$'s (so $\det(\mathbf{B})$ is an element of K). This quantity does not depend on the choice of the pseudo-basis. It is related to the volume of the lattice $\sigma(M)$ by the formula $\det(\sigma(M)) = \Delta_K^{n/2} \cdot \mathcal{N}(M)$.

2.5 Algorithmic problems over module and ideal lattices

We will consider the following algorithmic problems over module and ideal lattices. These problems are worst-case, which means that we want an algorithm that succeeds on any possible input.

Definition 2.1 (Module-SVP). *For $\gamma \geq 1$ and a positive integer n, the module shortest vector problem ((γ, n)-module-SVP) asks, given as input any pseudo-basis of any rank-n module M in K^n, to find a nonzero vector $\boldsymbol{s}$ of M such that $\|\boldsymbol{s}\| \leq \gamma \cdot \lambda_1(M)$.*

Definition 2.2 (Free-module-SVP). *For $\gamma \geq 1$ and a positive integer n, the free module shortest vector problem ((γ, n)-free-module-SVP) asks, given as input any free basis of any rank-n free module M in K^n, to find a nonzero vector $\boldsymbol{s}$ of M such that $\|\boldsymbol{s}\| \leq \gamma \cdot \lambda_1(M)$.*

Note that, for simplicity, we restricted our problems to full ranks modules, i.e., to modules of rank n living in K^n. Regarding the choice of the input pseudo-basis, we note that for the module-SVP problem, we can always assume that the module is represented by its HNF pseudo-basis, since it can be computed efficiently from any pseudo-basis. Doing so, we could define the problem as being worst-case only on the choice of the module. In the case of free-module-SVP however, we cannot do the same, since the module has to be represented by a *free basis* (recall that HNF bases are in general not free, even for free modules). In this definition, it is important that the algorithm succeeds for any free basis of a module.

We also define Hermite analogues of these two problems, named (γ, n)-module-HSVP and (γ, n)-free-module-HSVP respectively, by replacing $\lambda_1(M)$ by $\sqrt{nd} \cdot \det(M)^{1/(nd)}$ in the definitions above. Note that by Minkowski's bound,

we have immediate reductions from module-HSVP to module-SVP, and from free-module-HSVP to free-module-SVP, which preserve the rank of the module and the approximation factor.

Finally, we define a variant of the CVP problem over modules, which we call $\mathrm{CVP}_{\mathrm{cov}}$. In the CVP problem, the approximation factor is usually defined by comparing the distance between the target and the solution with the minimal distance from the target to the lattice. In the variant of CVP we consider, we instead compare this with the covering radius of the lattice. We believe that this variant is quite natural: this covers the "standard situation", where the target vector $\mathbf{t}$ has no reason to be particularly close to a lattice vector. This is in a sense similar to the Hermite variant of the shortest vector problem: we consider the expected distance from the target to the lattice (or the expected length of a shortest nonzero vector) instead of the actual distance to the lattice (or the actual length of a shortest vector).

Definition 2.3 (Module-$\mathrm{CVP}_{\mathrm{cov}}$). *For $\gamma \geq 1$ and a positive integer n, the module closest vector problem with respect to the covering radius ((γ, n)-module-CVP_{cov}) asks, given as input any pseudo-basis of any rank-n module M in K^n and any target vector $\mathbf{t} \in \mathrm{Span}_K(M)$, to find a vector $\boldsymbol{s}$ of M such that $\|\mathbf{t} - \mathbf{s}\| \leq \gamma \cdot \mathrm{cov}(M)$.*

The free-module closest vector problem with respect to the covering radius ((γ, n)-free-module-$\mathrm{CVP}_{\mathrm{cov}}$) is defined analogously, by restricting the input module to being free and represented by (any) free basis.

When $n = 1$, the modules are ideals and we use the terminology γ-ideal-HSVP instead of $(\gamma, 1)$-module-HSVP.[9]

3 From module problems to free-module problems and ideal-HSVP

In this section, we show that solving SVP (respectively HSVP, $\mathrm{CVP}_{\mathrm{cov}}$) in module lattices can be reduced to solving SVP (respectively HSVP, $\mathrm{CVP}_{\mathrm{cov}}$) in free module lattices *and* solving HSVP in ideal lattices. The three reductions have exactly the same structure, hence we present the reductions in a unique algorithm, namely Algorithm 3.1 below, making queries to an oracle that solves either SVP, HSVP or $\mathrm{CVP}_{\mathrm{cov}}$ in free modules. We then present the analysis of the three different cases in separate subsections, since these analyses differ.

The high level idea of the reductions is as follows. First, we compute an almost free basis of our input module, let's say $(\mathbf{b}_1, \ldots, \mathbf{b}_n, I)$. Then, we solve HSVP in the ideal I to obtain a short element $\alpha \in I$. The reduction finally calls the oracle solving SVP (respectively HSVP, $\mathrm{CVP}_{\mathrm{cov}}$) in free modules on the free module N with basis $(\mathbf{b}_1, \ldots, \alpha\mathbf{b}_n)$. This free module a submodule of M, and so a solution to SVP (respectively HSVP, $\mathrm{CVP}_{\mathrm{cov}}$) in N is in particular also a

[9] The other problems will not be used for ideal lattices, so we do not give them a special name.

solution in M. Analysing how much one looses during this reduction depends on the choice of the problem (SVP, HSVP, CVP_{cov}), and will be done in separate propositions.

Let us first describe the reduction algorithm formally.

Algorithm 3.1: Reduction from module-SVP/HSVP/CVP_{cov} to free-module-SVP/HSVP/CVP_{cov}

Oracles: $\mathcal{O}_{id}$ an oracle solving γ_{id}-ideal-HSVP and $\mathcal{O}$ an oracle solving (γ, n)-free-module-SVP (or HSVP, or CVP_{cov})

Input: A pseudo-basis $(\mathbf{b}_i, I_i)_{1 \leq i \leq n}$ of a rank-n module $M \subset K^n$; optionally a target vector $\mathbf{t} \in \text{Span}_K(M)$ if $\mathcal{O}$ solves free-module-CVP_{cov}

Output: A vector $\mathbf{s} \in M$

1 Compute an almost-free representation $(\mathbf{c}_1, \cdots, \mathbf{c}_n, I)$ of M;
2 Run $\mathcal{O}_{id}$ on I to obtain $\alpha \in I \setminus \{0\}$;
3 Let N be the free module spanned by $\mathbf{b}_1, \ldots, \mathbf{b}_{n-1}, \alpha \mathbf{b}_n$;
4 Run $\mathcal{O}$ on N (and optionally $\mathbf{t}$ in the case of CVP_{cov}) to obtain $\mathbf{s} \in N$;
5 **return** $\mathbf{s}$.

Let us first observe that this reduction runs in polynomial time.

Proposition 3.1. *Let $n \geq 1$ be an integer and $\gamma_{id}, \gamma \geq 1$ be real numbers. Let $\mathcal{O}_{id}$ be an oracle solving γ_{id}-ideal-HSVP and $\mathcal{O}$ be an oracle solving (γ, n)-free-module-SVP (respectively (γ, n)-free-module-HSVP, (γ, n)-free-module-CVP_{cov}). Then given access to $\mathcal{O}_{id}$ and $\mathcal{O}$, Algorithm 3.1 runs in probabilistic polynomial time, and makes one call to $\mathcal{O}_{id}$ and one call to $\mathcal{O}$.*

Proof. The only step of the algorithm which does not consist in calling an oracle is the computation of the almost-free pseudo-basis in the first step. This can be done in expected polynomial time thanks to Lemma 2.2. □

We will now analyze the correctness and the loss of the reductions.

3.1 The case of SVP

We start by an auxiliary lemma.

Lemma 3.1. *Using the same notations as in Algorithm 3.1, we have $\lambda_1(N) \leq \gamma_{id} \cdot \Delta_K^{1/d} \cdot \lambda_1(M)$.*

Proof. Take $\mathbf{v} \in M \setminus \{\mathbf{0}\}$ reaching $\lambda_1(M)$. We have $\mathbf{v} = \alpha_1 \mathbf{b}_1 + \ldots + \alpha_n \mathbf{b}_n$, where $\alpha_1, \ldots, \alpha_{n-1} \in \mathcal{O}_K$ and $\alpha_n \in I$. Note that since $\alpha \in I$, there exists some integral ideal J such that $\langle \alpha \rangle = IJ$. Since α is a solution to γ_{id}-HSVP in I, we have $\|\alpha\| \leq \gamma_{id} \cdot \sqrt{d} \cdot \Delta_K^{1/(2d)} \cdot \mathcal{N}(I)^{1/d}$, which implies

$$\mathcal{N}(J) = \frac{\mathcal{N}(\alpha)}{\mathcal{N}(I)} \leq \frac{\|\alpha\|^d}{\sqrt{d}^d \cdot \mathcal{N}(I)^d} \leq \gamma_{id}^d \cdot \Delta_K^{1/2},$$

where the first inequality is obtained from Equation (2).

Let $u \in J \backslash \{0\}$ reaching $\lambda_1^{(\infty)}(J)$, then $u \in \mathcal{O}_K$ (recall that J is integral) and $\alpha_n u \in \langle \alpha \rangle$. This implies that

$$u\mathbf{v} = \alpha_1 u\mathbf{b}_1 + \ldots + \alpha_n u\mathbf{b}_n \in N.$$

From this, we finally obtain that

$$\begin{aligned}\lambda_1(N) \leq \|u\mathbf{v}\| \leq \|u\|_\infty \cdot \|\mathbf{v}\| &\leq \lambda_1^{(\infty)}(J) \cdot \lambda_1(M) \\ &\leq \Delta_K^{1/2d} \cdot \mathcal{N}(J)^{1/d} \cdot \lambda_1(M) \\ &\leq \gamma_{id} \cdot \Delta_K^{1/d} \cdot \lambda_1(M).\end{aligned}$$

□

Proposition 3.2. *If $\mathcal{O}$ solves (γ, n)-free-module-SVP, then on input a pseudo-basis of a rank-n module M in K^n, Algorithm 3.1 outputs $\mathbf{s} \in M \setminus \{0\}$ such that $\|\mathbf{s}\| \leq \gamma \cdot \gamma_{id} \cdot \Delta_K^{1/d} \cdot \lambda_1(M)$.*

Proof. Observe first that N is a submodule of M, hence a non-zero vector of N is also a non-zero vector of M, and $\mathbf{s} \in M \setminus \{0\}$ as desired. The upper bound on $\|\mathbf{s}\|$ comes from the fact that $\mathbf{s}$ is a solution to (γ, n)-free-module-SVP in N, i.e., $\|\mathbf{s}\| \leq \gamma \cdot \lambda_1(N)$, and the upper bound on $\lambda_1(N)$ from Lemma 3.1. □

Combining Proposition 3.2 with Proposition 3.1, we obtain the following corollary.

Corollary 3.1. *Let $\gamma, \gamma_{id} \geq 1$ and $n \geq 1$ be an integer. For any $\gamma' \geq \gamma \cdot \gamma_{id} \cdot \Delta_K^{1/d}$, there is a probabilistic, polynomial-time reduction from solving (γ', n)-module-SVP in K^n to solving (γ, n)-free-module-SVP in K^n and γ_{id}-ideal-HSVP.*

3.2 The case of HSVP

As in the SVP case, we start by an auxiliary lemma.

Lemma 3.2. *Using the same notations as in Algorithm 3.1, we have* $\det(N) \leq \gamma_{id}^d \cdot \Delta_K^{1/2} \cdot \det(M)$.

Proof. We know from preliminaries that

$$\frac{\det N}{\det M} = \frac{\mathcal{N}(N)}{\mathcal{N}(M)} = \frac{\mathcal{N}(\alpha)}{\mathcal{N}(I)} \leq \gamma_{id}^d \cdot \Delta_K^{1/2},$$

where the last inequality was proven in the proof of Lemma 3.1. □

Proposition 3.3. *If $\mathcal{O}$ solves (γ, n)-free-module-HSVP, then on input a pseudo-basis of a rank-n module M, Algorithm 3.1 outputs $\mathbf{s} \in M \setminus \{0\}$ such that $\|\mathbf{s}\| \leq \gamma_{id}^{1/n} \cdot \gamma \cdot \Delta_K^{1/2nd} \cdot \sqrt{nd} \cdot (\det M)^{1/nd}$.*

Proof. Let N be as in Algorithm 3.1. Observe that N is a submodule of M, hence a non-zero vector of N is also a non-zero vector of M, and $\mathbf{s} \in M \setminus \{0\}$ as desired. From Lemma 3.2, we know that $\det(N) \leq \gamma_{id}^{d} \cdot \Delta_K^{1/2} \cdot \det(M)$, hence it follows that

$$\begin{aligned}\|\mathbf{s}\| &\leq \gamma \cdot \sqrt{nd} \cdot (\det N)^{1/nd} \\ &\leq \gamma_{id}^{1/n} \cdot \gamma \cdot \Delta_K^{1/2nd} \cdot \sqrt{nd} \cdot (\det M)^{1/nd}\end{aligned}$$

as desired. □

Combining Propositions 3.3 and 3.1, we obtain the following corollary.

Corollary 3.2. *Let $\gamma, \gamma_{id} \geq 1$ and $n \geq 1$ be an integer. For any $\gamma' \geq \gamma_{id}^{1/n} \cdot \gamma \cdot \Delta_K^{1/2nd}$, there is a probabilistic, polynomial-time reduction from solving (γ', n)-module-HSVP in K^n to solving (γ, n)-free-module-HSVP in K^n and γ_{id}-ideal-HSVP.*

3.3 The case of $\mathbf{CVP}_{\mathbf{cov}}$

Similarly to the two previous cases, we start by an auxiliary lemma.

Lemma 3.3. *Using the same notations as in Algorithm 3.1, we have* $\mathrm{cov}(N) \leq \gamma_{id} \cdot \Delta_K^{1/d} \cdot \mathrm{cov}(M)$.

Proof. Let $\mathbf{t} \in \mathrm{Span}_K(N)$. We cant to prove the existence of a vector $\mathbf{s} \in N$ with $\|\mathbf{t} - \mathbf{s}\| \leq \gamma_{id} \cdot \Delta_K^{1/d} \cdot \mathrm{cov}(M)$.

Let $u \in \alpha \cdot I^{-1}$ be a shortest nonzero vector of $\alpha \cdot I^{-1}$ for the infinity norm. By Minkowski's theorem, we know that

$$\|u\|_\infty \leq \det(\alpha \cdot I^{-1})^{1/d} = \Delta_K^{1/2d} \cdot \mathcal{N}(\alpha \cdot I^{-1})^{1/d} \leq \gamma_{id} \cdot \Delta_K^{1/d},$$

where the last inequality was proven in the proof of Lemma 3.1. Note that since $\alpha \in I$, then the ideal $\alpha \cdot I^{-1}$ is integral and so in particular $u \in \mathcal{O}_K$. This, in turns, implies that for any $\mathbf{x} \in M$, we have $u \cdot \mathbf{x} \in N$.

Now, let us define $\mathbf{t}' = u^{-1} \cdot \mathbf{t}$. It holds that $\mathbf{t}' \in \mathrm{Span}_K(N) = \mathrm{Span}_K(M)$, so by definition of the covering radius, there exists $\mathbf{s}' \in M$ such that $\|\mathbf{t}' - \mathbf{s}'\| \leq \mathrm{cov}(M)$. From what we have seen above, $\mathbf{s} = u \cdot \mathbf{s}'$ is then a vector of N, and from the bound on $\|u\|_\infty$ we finally obtain

$$\|\mathbf{t} - \mathbf{s}\| \leq \|u\|_\infty \cdot \|\mathbf{t}' - \mathbf{s}'\| \leq \gamma_{id} \cdot \Delta_K^{1/d} \cdot \mathrm{cov}(M),$$

as desired. □

Proposition 3.4. *If $\mathcal{O}$ solves (γ, n)-free-module-CVP$_{cov}$, then on input a pseudo-basis of a rank-n module M and a target vector $\mathbf{t} \in \mathrm{Span}_K(M)$, Algorithm 3.1 outputs $\mathbf{s} \in M$ such that $\|\mathbf{t} - \mathbf{s}\| \leq \gamma \cdot \gamma_{id} \cdot \Delta_K^{1/d} \cdot \mathrm{cov}(M)$.*

Proof. Let N be as in Algorithm 3.1. Since N is a submodule of M, and $\mathbf{s} \in N$, then in particular we have $\mathbf{s} \in M$. Moreover, from Lemma 3.3, we know that $\mathrm{cov}(N) \leq \gamma_{id} \cdot \Delta_K^{1/d} \cdot \mathrm{cov}(M)$, hence it follows that

$$\begin{aligned} \|\mathbf{t} - \mathbf{s}\| &\leq \gamma \cdot \mathrm{cov}(N) \\ &\leq \gamma \cdot \gamma_{id} \cdot \Delta_K^{1/d} \cdot \mathrm{cov}(N), \end{aligned}$$

as desired. □

Combining Propositions 3.4 and 3.1, we obtain the following corollary.

Corollary 3.3. *Let $\gamma, \gamma_{id} \geq 1$ and $n \geq 1$ be an integer. For any $\gamma' \geq \gamma \cdot \gamma_{id} \cdot \Delta_K^{1/d}$, there is a probabilistic, polynomial-time reduction from solving (γ', n)-module-CVP$_{cov}$ in K^n to solving (γ, n)-free-module-CVP$_{cov}$ in K^n and γ_{id}-ideal-HSVP.*

4 From ideal-HSVP to rank-2 free-module problems

In this section, we show that solving ideal-HSVP can be reduced to solving free-module-SVP (respectively free-module-HSVP, free-module-CVP$_{\mathrm{cov}}$) in modules of rank 2. Since HSVP reduces to SVP in the same lattice by Minkowski's theorem, we actually only need to prove two reductions, one to free-module-HSVP and one to free-module-CVP$_{\mathrm{cov}}$. We do so in the two subsections below.

4.1 The case of HSVP (and SVP)

In this subsection, we reduce ideal-HSVP to free-module-HSVP in modules of rank 2. The high level idea is to use a two-element representation of the input ideal to transform it into a free rank-2 module, such that any short vector of this free rank-2 module can be transformed back into a short vector of the input ideal. Similar ideas were used in [DM22] in order to transform a rank-2 module into a free rank-4 module.

More precisely, given an ideal I, we compute a two-element representation $I = \langle a \rangle + \langle b \rangle$ and construct the free module M with a basis consisting of the columns of the following matrix

$$\begin{pmatrix} a & b \\ 0 & \varepsilon \end{pmatrix},$$

where $\varepsilon > 0$ is a rational number to be specified later. Observe that every $\mathbf{s} \in M$ is of the form $\begin{pmatrix} x & y \end{pmatrix}^T$ for $x \in I$ and $y \in \langle \epsilon \rangle$. Hence, if $\mathbf{s}$ is small, then its first coordinate x is a small element of I. Here, since the size of $\mathbf{s}$ is related to the determinant of M, which depends on the choice of ε, we want to take ε as small as possible. However, M also contains vectors of the form $\begin{pmatrix} 0 & v\varepsilon \end{pmatrix}^T$ for $v \in \mathcal{O}_K$, so if ε is too small then the short vectors of M are of this form and result in $x = 0$. To avoid this case, we observe that when $\begin{pmatrix} 0 & v\varepsilon \end{pmatrix}^T$ is a short vector of M then ε can be upper bounded by a quantity depending only on K, I and a. Thus by choosing ε greater than this quantity, we avoid the case where short vectors of M have their first coordinate equal to 0.

Proposition 4.1. *For any $\gamma \geq 1$ and $\gamma' > 2\gamma^2 \cdot \Delta_K^{1/2d}$, there exists a probabilistic polynomial-time reduction from solving γ'-ideal-HSVP to solving $(\gamma, 2)$-free-module-HSVP in K^2.*

Proof. Let I be a non-zero ideal of K, without loss of generality we can assume that I is integral (otherwise we scale it to an integral ideal, which does not change its geometry). Compute a two-element representation $I = \langle a \rangle + \langle b \rangle$ with $a \neq 0$ using the algorithm of Theorem 2.2 and consider the free module $M \subset K^2$ generated by the free basis (in columns)

$$\begin{pmatrix} a & b \\ 0 & \varepsilon \end{pmatrix},$$

for some $\varepsilon > 0$, rational, to be determined. We want to prove that any solution to γ-HSVP in M is of the form $\begin{pmatrix} x & y \end{pmatrix}^T$, with x a solution to γ'-ideal-HSVP in I. Since a free basis of M is efficiently computable from I (in probabilistic polynomial time), this will give us a probabilistic polynomial time reduction from γ'-ideal-HSVP to $(\gamma, 2)$-free-module-HSVP as desired.

Let us first prove that if ε is large enough, then all solutions to γ-HSVP in M are of the form $\begin{pmatrix} x & y \end{pmatrix}^T$ with x non-zero. To do so, assume by contradiction that $\begin{pmatrix} 0 & v\varepsilon \end{pmatrix}^T$ is a solution to γ-HSVP in M, then $v \in \mathcal{O}_K \backslash \{0\}$ and there exists $u \in \mathcal{O}_K$ such that $ua + vb = 0$. By definition of γ-HSVP, we have

$$\varepsilon \cdot \|v\| \leq \gamma \cdot \sqrt{2d} \cdot \Delta_K^{1/2d} \cdot \mathcal{N}(M)^{1/2d} = \gamma \cdot \sqrt{2d} \cdot \Delta_K^{1/2d} \cdot \varepsilon^{1/2} \cdot \mathcal{N}(a)^{1/2d}.$$

Next, we want to show that because of the equality $ua + vb = 0$, then v has to be quite large, and the inequality above cannot be satisfied. The equality $ua + vb = 0$ implies that $\langle u \rangle \langle a \rangle = \langle v \rangle \langle b \rangle$. Assume for the moment that $b \neq 0$. Then, all ideals in the equation above are nonzero (since both a and b are nonzero, and v should also be nonzero). Since $I = \langle a \rangle + \langle b \rangle$, there exists nonzero integral ideals J_1, J_2 such that $\langle a \rangle = IJ_1, \langle b \rangle = IJ_2$ and J_1, J_2 do not have any common factor in their factorization into prime ideals. Since I is invertible (because it is non-zero), the equality $\langle u \rangle \langle a \rangle = \langle v \rangle \langle b \rangle$ can be rewritten as $\langle u \rangle J_1 = \langle v \rangle J_2$. Note that all ideals involved in this equality are integral (because u and v are in $\mathcal{O}_K$). Since J_1 and J_2 are coprime, it must be that J_1 divides $\langle v \rangle$, which implies in particular that $\mathcal{N}(v) \geq \mathcal{N}(J_1) = \mathcal{N}(a)/\mathcal{N}(I)$, where the last equality comes from the definition of J_1. Finally, recall from Equation (2) that $\|v\| \geq \sqrt{d} \cdot \mathcal{N}(v)^{1/d}$, which gives us

$$\|v\| \geq \sqrt{d} \cdot \left(\frac{\mathcal{N}(a)}{\mathcal{N}(I)} \right)^{1/d}.$$

In the case $b = 0$, then $\mathcal{N}(a) = \mathcal{N}(I)$ and thus the inequality still holds, since $v \in \mathcal{O}_K$. Combining this inequality with the one above we obtain

$$\sqrt{d} \cdot \left(\frac{\mathcal{N}(a)}{\mathcal{N}(I)} \right)^{1/d} \leq \|v\| \leq \frac{\gamma \cdot \sqrt{2d} \cdot \Delta_K^{1/2d} \cdot \mathcal{N}(a)^{1/2d}}{\varepsilon^{1/2}},$$

which results in

$$\varepsilon \leq 2\gamma^2 \Delta_K^{1/d} \cdot \frac{\mathcal{N}(I)^{2/d}}{\mathcal{N}(a)^{1/d}}.$$

Therefore choosing $\varepsilon > 2\gamma^2 \Delta_K^{1/d} \mathcal{N}(I)^{2/d} / \mathcal{N}(a)^{1/d}$ guarantees that the solution $\mathbf{s} = \begin{pmatrix} x & y \end{pmatrix}^T$ to γ-SVP over M satisfies $x \neq 0$.

Now, we also choose ε such that

$$\varepsilon \leq \frac{\gamma'^2}{2\gamma^2} \cdot \frac{\mathcal{N}(I)^{2/d}}{\mathcal{N}(a)^{1/d}}.$$

Note that $\gamma' > 2\gamma^2 \cdot \Delta_K^{1/2d}$ implies the existence of such ε. Calling the free-module-HSVP oracle on input M, let $\mathbf{s}$ be the output and x be the first coordinate of $\mathbf{s}$. The choice of ε guarantees that $x \in I \backslash \{0\}$ and

$$\begin{aligned} \|x\| \leq \|\mathbf{s}\| &\leq \gamma \cdot \sqrt{2d} \cdot \Delta_K^{1/2d} \cdot \varepsilon^{1/2} \cdot \mathcal{N}(a)^{1/2d} \\ &\leq \gamma' \cdot \sqrt{d} \cdot \Delta_K^{1/2d} \cdot \mathcal{N}(I)^{1/d} = \gamma' \cdot \sqrt{d} \cdot \det(I)^{1/d}. \end{aligned}$$

Hence x is a solution to γ'-ideal-HSVP over I. □

Since $(\gamma, 2)$-free-module-HSVP reduces to $(\gamma, 2)$-free-module-SVP (by definition and by Minkowski's bound), Proposition 4.1 implies the following proposition.

Proposition 4.2. *For any $\gamma \geq 1$ and $\gamma' > 2\gamma^2 \cdot \Delta_K^{1/2d}$, there exists a probabilistic polynomial-time reduction from solving γ'-ideal-HSVP to solving $(\gamma, 2)$-free-module-SVP in K^2.*

4.2 The case of $\mathrm{CVP}_{\mathrm{cov}}$

Let us now consider the reduction to $\mathrm{CVP}_{\mathrm{cov}}$ in free-modules of rank 2. The main ideas of the reduction are similar to the SVP/HSVP case, but the analysis is a bit different.

The idea is again to consider the free rank-2 module M spanned by the columns of the matrix $\begin{pmatrix} a & b \\ 0 & \varepsilon \end{pmatrix}$, where $I = \langle a \rangle + \langle b \rangle$ and ε is small. We show that if ε is sufficiently small, then the covering radius of this lattice is roughly equal to $\det(I)^{1/d}$ (up to polynomial factors). Note that, contrary to the SVP/HSVP case, we have no lower bound on ε here. The ideal case would be $\varepsilon = 0$, but this would lead to a (non free) module of rank 1. Ensuring that the module has rank 2 is the only reason we take $\varepsilon \neq 0$.

Then, in order to find a short vector in I, we simply solve $\mathrm{CVP}_{\mathrm{cov}}$ in M with a target vector of the form $\mathbf{t} = (t_0, 0)^T$, where we choose t_0 just slightly above the covering radius of M, so that any solution $\mathbf{s} = (s_0, s_1)^T$ has $s_0 \neq 0$, and $s_0 \in I$ is somewhat short.

Proposition 4.3. *For any $\gamma \geq 1$ and $\gamma' \geq 5 \cdot \gamma \cdot d \cdot \lambda_d^{(\infty)}(\mathcal{O}_K)$, there exists a probabilistic polynomial-time reduction from solving γ'-ideal-HSVP to solving $(\gamma, 2)$-free-module-CVP$_{cov}$ in K^2.*

Proof. Let I be an integral ideal in $\mathcal{O}_K$ (we can assume that I is integral without loss of generality, if it is not we scale it). Let $a, b \in \mathcal{O}_K$ be such that $I = \langle a \rangle + \langle b \rangle$ (with $a \neq 0$), and $\varepsilon > 0$ be some rational number. Let M be the rank-2 free module spanned by the basis $\begin{pmatrix} a & b \\ 0 & \varepsilon \end{pmatrix}$. First, let us prove that

$$\mathrm{cov}(M) \leq \varepsilon \cdot \left(d \cdot \lambda_d^{(\infty)}(\mathcal{O}_K) \cdot \Delta_K^{1/2d} \cdot (\sqrt{d} + \|a\|) \right) + d^{3/2} \cdot \lambda_d^{(\infty)}(\mathcal{O}_K) \cdot \det(I)^{1/d}.$$

Let $\mathbf{t} = (t_0, t_1)^T \in \mathrm{Span}_K(M) = K^2$. Let $w \in \mathcal{O}_K$ be such that $\|w\varepsilon - t_1\| \leq \mathrm{cov}(\varepsilon\mathcal{O}_K)$ (i.e., $w\varepsilon$ is a closest point to t_1 in the ideal $\varepsilon\mathcal{O}_K$). If we subtract $w \cdot (b, \varepsilon)^T$ to $\mathbf{t}$, we obtain a new vector $\mathbf{t}' = (t_0', t_1')^T$, which is at the same distance to M than $\mathbf{t}$ (since $w \cdot (b, \varepsilon)^T \in M$), but whose second coordinates is small, namely $\|t_1'\| \leq \mathrm{cov}(\varepsilon\mathcal{O}_K)$.

Let us now reduce the first coordinate. Let $\alpha \in I$ be a closest vector to t_0', that is, $\|\alpha - t_0'\| \leq \mathrm{cov}(I)$. Since I is generated by a and b, there exists u_0 and v_0 in O_K such that $\alpha = u_0 a + v_0 b$. We would like to take v_0 as small as possible (since adding v_0 times the second basis vector will make the second coordinate of our vector increase again). We know that any $(u, v) = (u_0 + kb, v_0 - ka)$ with $k \in \mathcal{O}_K$ also satisfies $\alpha = ua + vb$. Hence, we can always reduce v modulo a and ensure that $\|v\| = \|v_0 - ka\| \leq \mathrm{cov}(a\mathcal{O}_K)$.

Overall, we obtain $(u, v) \in \mathcal{O}_K^2$ with $\|v\| \leq \mathrm{cov}(a\mathcal{O}_K)$ such that $\|ua + vb - t_0'\| \leq \mathrm{cov}(I)$. Taking $\mathbf{s} = u(a, 0)^T + (v + w)(b, \varepsilon)^T \in M$ finally gives us

$$\begin{aligned} \|\mathbf{t} - \mathbf{s}\| &= \|\mathbf{t}' - u(a, 0)^T - v(b, \varepsilon)^T\| \\ &= \|(t_0' - \alpha, t_1' - \varepsilon v)^T\| \\ &\leq \|t_0' - \alpha\| + \|t_1'\| + \varepsilon\|v\| \\ &\leq \mathrm{cov}(I) + \mathrm{cov}(\varepsilon\mathcal{O}_K) + \varepsilon \cdot \mathrm{cov}(a\mathcal{O}_K). \end{aligned}$$

To conclude, recall from preliminaries (Equations (3) and (4)) that

$$\begin{aligned} \mathrm{cov}(I) &\leq d^{3/2} \cdot \lambda_d^{(\infty)}(\mathcal{O}_K) \cdot \det(I)^{1/d}, \\ \mathrm{cov}(a\mathcal{O}_K) &\leq d \cdot \lambda_d^{(\infty)}(\mathcal{O}_K) \cdot \Delta_K^{1/2d} \cdot \|a\|, \\ \mathrm{cov}(\varepsilon\mathcal{O}_K) &\leq \varepsilon \cdot d^{3/2} \cdot \lambda_d^{(\infty)}(\mathcal{O}_K) \cdot \Delta_K^{1/2d}, \end{aligned}$$

where in the last inequality we used the fact that ε is rational and so $\|\varepsilon\| = \varepsilon\sqrt{d}$. Combining everything, we obtain the desired upper bound on $\mathrm{cov}(M)$.

We can now describe our reduction from ideal-HSVP to free-module-CVP$_{\mathrm{cov}}$ in modules of rank 2. Our algorithm takes as input some integral ideal I. It computes in probabilistic polynomial time a and b in $\mathcal{O}_K$ such that $I = \langle a \rangle + \langle b \rangle$, with $a \neq 0$ (see Lemma 2.2). Then, it sets $\varepsilon > 0$ rational such that $\varepsilon \leq$

$\left(\Delta_K^{1/(2d)} \cdot (\sqrt{d} + \|a\|)\right)^{-1} \cdot \det(I)^{1/d}$, and compute the free basis $\begin{pmatrix} a & b \\ 0 & \varepsilon \end{pmatrix}$, spanning some rank-2 module M.

The reduction also creates the target vector $\mathbf{t} = (\delta, 0)^T$, with $\delta \in \mathbb{Q}$ such that $\delta \in (2, 3] \cdot \gamma \cdot d\lambda_d^{(\infty)}(\mathcal{O}_K) \cdot \det(I)^{1/d}$. The reduction then runs the $(\gamma, 2)$-free-module-$\mathrm{CVP}_{\mathrm{cov}}$ oracle on input M and $\mathbf{t}$, to obtain a vector $\mathbf{s} = (s_0, s_1)^T$, and it outputs s_0.

One can check that the reduction in probabilistic polynomial time. Let us now prove that s_0 is a solution to γ'-HSVP in I with γ' as in the theorem statement.

First, $s_0 \in I$ since a and b are both in I. Also, by choice of ε and using what we have proven above, we know that $\mathrm{cov}(M) \leq 2d^{3/2} \cdot \lambda_d^{(\infty)}(\mathcal{O}_K) \cdot \det(I)^{1/d}$. This implies that

$$\|s_0 - \delta\| \leq \|\mathbf{s} - \mathbf{t}\| \leq \gamma \cdot \mathrm{cov}(M) < \|\delta\|,$$

using the fact that $\|\delta\| = \sqrt{d}\delta$ since $\delta \in \mathbb{Q} \subseteq K$. This means that s_0 is nonzero, and $\|s_0\| \leq \|\delta\| + \gamma \cdot \mathrm{cov}(M) \leq 5\gamma \cdot d \cdot \lambda_d^{(\infty)}(\mathcal{O}_K) \cdot \sqrt{d} \cdot \det(I)^{1/d}$, as desired. □

5 From rank-2 free-module problems to rank-n free-module problems

We conclude the reductions by proving a reduction from free-module-SVP (respectively HSVP, $\mathrm{CVP}_{\mathrm{cov}}$) in modules of rank 2 to free-module-SVP (respectively HSVP, $\mathrm{CVP}_{\mathrm{cov}}$) in modules of rank $n \geq 2$. These reductions are not surprising, since they follow the intuition that the hardness of module problems increase when the rank of the module increase (for a fixed underlying field). Following this intuition, the reductions for SVP and $\mathrm{CVP}_{\mathrm{cov}}$ are easily obtained by embedding the rank 2 input module into a larger rank module, and padding the extra dimensions with dummy vectors. Surprisingly however, the reduction for HSVP is not as easy as the other two, and we even have some significant loss in the approximation factor when reducing to modules of rank n with n odd. The proof of Proposition 5.2 (the HSVP reduction) is the most interesting one of this section. We believe that improving the reduction for HSVP to obtain a smaller loss is an interesting open problem.

5.1 The case of SVP

In this subsection, we reduce SVP in rank-2 free modules in K^2 to SVP in rank-n free module, where $n \geq 2$. This is naturally done by embedding the rank 2 free module into a larger rank free module.

Let $M_1 \subset K^2$ be a rank-2 free modules with a free basis $\mathbf{B}' \in K^{2\times 2}$. We construct a rank-$n$ free module $M \subset K^n$ generated by the columns of the following block matrix

$$\mathbf{B} = \left(\begin{array}{c|c} \mathbf{B}' & 0 \\ \hline 0 & \delta I_{n-2} \end{array}\right) \in K^{n\times n}$$

where δ is a positive, rational number, to be determined later. Note that M_1 is the rank-2 free module generated by the first two columns of $\mathbf{B}$. If we let M_2 be the rank-$(n-2)$ free module generated by the remaining $n-2$ columns of B, then we see that $M = M_1 \oplus M_2$, and the sum is orthogonal.

Lemma 5.1. *With the above notations,* $\lambda_1(M) = \min\{\lambda_1(M_1), \lambda_1(M_2)\}$.

Proof. Let $\mathbf{s} \in M \backslash \{\mathbf{0}\}$ be a shortest vector, we have $\mathbf{s} = \mathbf{s}_1 + \mathbf{s}_2$, where $\mathbf{s}_1 \in M_1$, $\mathbf{s}_2$ in M_2 and $\mathbf{s}_1, \mathbf{s}_2$ are orthogonal (when viewed as vectors in $\mathbb{C}^{nd}$). If both $\mathbf{s}_1$ and $\mathbf{s}_2$ are nonzero vectors, then $\lambda_1(M) = \|\mathbf{s}\| > \min\{\|\mathbf{s}_1\|, \|\mathbf{s}_2\|\}$, which is absurd. Thus one of $\mathbf{s}_1$ and $\mathbf{s}_2$ is zero vector, and the conclusion follows. □

Suppose that we have access to an oracle solving (γ, n)-free-module-SVP on input any free basis of any rank-n module in K^n. Calling this oracle on input $\mathbf{B}$ will give a short vector $\mathbf{s}$ of M. The idea is to choose δ large enough such that M_2 does not contain any relatively short vector of M and thus the short vectors of M should be the short vectors of M_1. In particular, if we choose δ such that $\lambda_1(M_2) \geq \gamma\lambda_1(M_1)$, then a solution $\mathbf{s}$ to γ-SVP in M is also a solution to γ-SVP in M_1 (when projecting on the first two coordinates).

Lemma 5.2. *If* $\delta > \gamma \cdot \sqrt{2} \cdot \det(M_1)^{1/(2d)}$, *then* $\lambda_1(M_2) > \gamma \cdot \lambda_1(M_1)$.

Proof. Let $\mathbf{s} = (0, 0, s_1\delta, \ldots, s_{n-2}\delta)^T \in M_2$ be a shortest nonzero vector of M_2, where $s_i \in \mathcal{O}_K$. Observe that there exists some $i \in \{1, \ldots, n-2\}$ such that $s_i \neq 0$, then

$$\lambda_1(M_2) = \|\mathbf{s}\| \geq \delta \cdot \|s_i\| \geq \delta \cdot \sqrt{d} > \gamma \cdot \sqrt{2d} \cdot \det(M_1)^{1/(2d)}.$$

By Minkowski's bound, it follows that $\lambda_1(M_2) > \gamma\lambda_1(M_1)$. □

We can now prove our reduction from rank 2 to rank n free modules.

Proposition 5.1. *Let* $\gamma \geq 1$ *be a reaul number and* $n \geq 2$ *be an integer. There is a polynomial-time (deterministic) reduction from solving* $(\gamma, 2)$*-free-module-SVP in* K^2 *to* (γ, n)*-free-module-SVP in* K^n.

Proof. Consider a rank-2 free module M_1 given by a basis $\mathbf{B}' \in K^{2\times 2}$. We set $\delta = \lceil \gamma \cdot 2 \cdot \det(M_1)^{1/(2d)} \rceil$ and construct the block matrix

$$\mathbf{B} = \left(\begin{array}{c|c} \mathbf{B}' & 0 \\ \hline 0 & \delta I_{n-2} \end{array}\right) \in K^{n\times n}$$

as above. Note that computing δ and constructing $\mathbf{B}$ can be performed in time polynomial in the size of $\mathbf{B}'$ and in $\log \Delta_K$ (and the size of $\mathbf{B}$ is polynomial in these two quantities). We observe also that $\mathbf{B}$ is a free basis of a rank n module in K^n. Calling the (γ, n)-free-module-SVP oracle on this module produces $\mathbf{s} = (s_1, s_2, \ldots, s_n) \in K^n$. Our reduction algorithm then outputs the vector formed by the first two coordinates of $\mathbf{s}$.

We have seen that this procedure is polynomial time. Let us now show that the output vector is a solution to γ-SVP in M_1. Since δ satisfies the condition of Lemma 5.2, we have $\lambda_1(M_2) > \gamma\lambda_1(M_1) \geq \lambda_1(M_1)$. By Lemma 5.1, it follows that $\lambda_1(M) = \lambda(M_1)$. The output $\mathbf{s}$ of the oracle then satisfies $\|\mathbf{s}\| \leq \gamma \cdot \lambda_1(M_1) < \lambda_1(M_2)$. This implies that $\mathbf{s}' = (s_1, s_2)^T$ is nonzero, in M_1 and of euclidean norm $\leq \gamma \cdot \lambda_1(M_1)$ as desired. □

5.2 The case of HSVP

In this section, we reduce HSVP in free modules of rank 2 to HSVP in free modules of rank $n \geq 2$. The strategy is somewhat similar to the SVP case: we embed our rank-2 module into a rank-n module and use the oracle in this rank-n module. However, in the HSVP case, padding the extra dimensions of the modules with (scaled) identity vectors does not seem to work. Hence, we instead copy our rank-2 modules into $n/2$ orthogonal copies of itself. For this reason, the case with n odd behaves differently from the case with n even, and we obtain a worse approximation factor in this case of n odd (this is the only reduction in this section, where the new approximation factor is more than linear in the original approximation factor).

Proposition 5.2. *Let $n \geq 2$ be an integer and define $\varepsilon_n = 0$ if n is even and $\varepsilon_n = 1/(n-1)$ if n is odd. For any real numbers $\gamma \geq 1$ and $\gamma' \geq \gamma^{1+\varepsilon_n} \cdot \sqrt{n}^{1+\varepsilon_n} \cdot \Delta_K^{\varepsilon_n/2d}$, there exists a (deterministic) polynomial time reduction from solving $(\gamma', 2)$-free-module-HSVP to solving (γ, n)-free-module-HSVP.*

Note that the quantity ε_n in the theorem is always $\leq 1/2$, so by taking $\gamma' \geq \gamma^{3/2} \cdot n^{3/4} \cdot \Delta_K^{1/4d}$, the theorem's requirement is fulfilled.

Proof. Consider a rank-2 free module M_1 given by a basis $\mathbf{B}' \in K^{2\times 2}$. Consider the case when n is even, we construct the block matrix

$$\mathbf{B} = \begin{pmatrix} \mathbf{B}' & 0 & \cdots & 0 \\ 0 & \mathbf{B}' & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \mathbf{B}' \end{pmatrix} \in K^{n\times n},$$

which is a block diagonal matrix with diagonal elements consisting of $n/2$ blocks of $\mathbf{B}'$. Observe the cost of constructing $\mathbf{B}$ and the size of $\mathbf{B}$ is polynomial in the size of $\mathbf{B}'$. We observe also that $\mathbf{B}$ is a free basis of a rank n module in K^n. Calling the (γ, n)-free-module-HSVP oracle on this module produces $\mathbf{s} = (s_1, s_2, \ldots, s_n) \in K^n$ satisfying $\|\mathbf{s}\| \leq \gamma \cdot \sqrt{nd} \cdot \det(M)^{1/nd}$. Our reduction algorithm then selects an odd index i such that (s_i, s_{i+1}) is nonzero and outputs

$\mathbf{s}' = (s_i, s_{i+1})$. Such i always exists since $\mathbf{s}$ is nonzero, and $\mathbf{s}' \in M_1$ and satisfies

$$\begin{aligned}\|\mathbf{s}'\| \leq \|\mathbf{s}\| &\leq \gamma \cdot \sqrt{nd} \cdot \det(M)^{1/nd} \\ &= \gamma \cdot \sqrt{nd} \cdot \left(\Delta_K^{n/2} \cdot \mathcal{N}(\det \mathbf{B})\right)^{1/nd} \\ &= \gamma \cdot \sqrt{nd} \cdot \Delta_K^{1/2d} \cdot \left(\mathcal{N}\left(\det \mathbf{B}'\right)^{n/2}\right)^{1/nd} \\ &= \gamma \cdot \sqrt{nd} \cdot \det(M_1)^{1/2d} \leq \gamma' \cdot \sqrt{2d} \cdot \det(M_1)^{1/2d},\end{aligned}$$

the last inequality is obtained by the fact that $\gamma' = \gamma\sqrt{n} \geq \gamma \cdot \sqrt{n/2}$ when n is even. Hence, $\mathbf{s}'$ is a solution to γ'-HSVP in M_1 as desired. Now consider the case when n is odd, we construct the block matrix

$$\mathbf{B} = \begin{pmatrix} \mathbf{B}' & 0 & 0 & \cdots & 0 & 0 \\ 0 & \mathbf{B}' & 0 & \cdots & 0 & 0 \\ 0 & 0 & \mathbf{B}' & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \\ 0 & 0 & 0 & \cdots & \mathbf{B}' & 0 \\ 0 & 0 & 0 & \cdots & 0 & \delta \end{pmatrix} \in K^{n \times n},$$

where δ is a rational number satisfying $\delta_0 < \delta \leq 2\delta_0$, for

$$\delta_0 = \gamma^{n/(n-1)} \cdot \Delta_K^{n/2d(n-1)} \cdot (\sqrt{n})^{n/(n-1)} \cdot \mathcal{N}\left(\det \mathbf{B}'\right)^{1/2d}.$$

Note that $\mathbf{B}$ is a block diagonal matrix with diagonal elements consisting of $(n-1)/2$ blocks of $\mathbf{B}'$ and δ. Similarly to the case where n is even, $\mathbf{B}$ is a free basis of a rank n module in K^n; the cost of constructing $\mathbf{B}$ and the size of $\mathbf{B}$ is polynomial in the size of $\mathbf{B}'$ and $\log \Delta_K$. Calling the (γ, n)-free-module-HSVP oracle on this module produces $\mathbf{s} = (s_1, s_2, \ldots, s_n) \in K^n$ satisfying $\|\mathbf{s}\| \leq \gamma \cdot \sqrt{nd} \cdot \det(M)^{1/nd}$. Our reduction algorithm now select an odd index $i < n$ such that (s_i, s_{i+1}) is nonzero and outputs $\mathbf{s}' = (s_i, s_{i+1})$.

Now we show that such choice of i can always be made. Suppose by contradiction that the (γ, n)-free-module-SVP outputs $\mathbf{s} = (0, \ldots, 0, \delta u) \in K^n$, where $u \in \mathcal{O}_K \backslash \{0\}$. Note that we have

$$\delta \cdot \|u\| \leq \gamma \cdot \sqrt{nd} \cdot (\det M)^{1/nd} = \gamma \cdot \sqrt{nd} \cdot \Delta_K^{1/2d} \cdot \mathcal{N}(\det \mathbf{B}')^{(n-1)/2nd} \cdot \delta^{1/n}.$$

Since $u \in \mathcal{O}_K \setminus \{0\}$, we have $\|u\| \geq \sqrt{d}$, which implies

$$\delta \leq \gamma^{n/(n-1)} \cdot \Delta_K^{n/2d(n-1)} \cdot (\sqrt{n})^{n/(n-1)} \cdot \mathcal{N}\left(\det \mathbf{B}'\right)^{1/2d} = \delta_0.$$

This contradicts the choice of δ. Thus the reduction algorithm in case n is odd can always outputs $\mathbf{s}'$ which is a nonzero vector of M_1 and satisfies

$$\begin{aligned}\|\mathbf{s}'\| \leq \|\mathbf{s}\| &\leq \gamma \cdot \sqrt{nd} \cdot \det(M)^{1/nd} \\ &= \gamma \cdot \sqrt{nd} \cdot \Delta_K^{1/2d} \cdot \mathcal{N}(\det \mathbf{B}')^{(n-1)/2nd} \cdot \delta^{1/n} \\ &\leq \gamma \cdot \sqrt{nd} \cdot \Delta_K^{1/2d} \cdot \mathcal{N}\left(\det \mathbf{B}'\right)^{(n-1)/2nd} \cdot 2^{1/n} \cdot \gamma^{\varepsilon_n} \cdot \Delta_K^{\varepsilon_n/2d} \cdot \sqrt{n}^{\varepsilon_n} \cdot \mathcal{N}\left(\det \mathbf{B}'\right)^{1/2nd} \\ &\leq \gamma^{1+\varepsilon_n} \cdot \sqrt{n}^{1+\varepsilon_n} \Delta_K^{\varepsilon_n/2d} \cdot \sqrt{2d} \cdot \Delta_K^{1/2d} \cdot \mathcal{N}(\det \mathbf{B}')^{1/2d} \\ &\leq \gamma' \cdot \sqrt{2d} \cdot \det(M_1)^{1/2d},\end{aligned}$$

as desired. □

5.3 The case of $\mathrm{CVP}_{\mathrm{cov}}$

In this subsection, we reduce $\mathrm{CVP}_{\mathrm{cov}}$ in free modules of rank 2 to $\mathrm{CVP}_{\mathrm{cov}}$ in free modules of rank $n \geq 2$. This is probably the simplest of the three reductions from this section. Like in the SVP case, we simply embed our rank—2 module M_1 into a rank-n module by padding the extra dimensions with (scaled) identity vectors. We only need to ensure that these vectors are smaller than the covering radius of M_1, to be sure that these extra dimensions do not increase the covering radius of our module too much. Then, we create a target vector by padding zeros to the original target vector. Overall, we prove the following reduction.

Proposition 5.3. *Let $\gamma \geq 1$ a real number and $n \geq 2$ an integer. There is a (deterministic) polynomial-time reduction from solving $(\gamma', 2)$-free-module-CVP_{cov} in K^2 to (γ, n)-free-module-CVP_{cov} in K^n, for any $\gamma' \geq \sqrt{2} \cdot \gamma$.*

Proof. Consider a rank-2 free module M_1 given by a basis $\mathbf{B}' \in K^{2\times 2}$ and a target vector $\mathbf{t_1} \in \mathrm{Span}_K(M_1) = K^2$. Let us assume without loss of generality that $M_1 \subseteq \mathcal{O}_K^2$.

The reduction algorithm computes $\delta \leq (dn \cdot \lambda_d(\mathcal{O}_K))^{-1}$ rational and constructs the block matrix (spanning a module called M)

$$\mathbf{B} = \left(\begin{array}{c|c} \mathbf{B}' & 0 \\ \hline 0 & \delta \cdot I_{n-2} \end{array}\right) \in K^{n\times n}.$$

and the target vector $\mathbf{t} = (\mathbf{t_1}^T, 0, \ldots, 0)^T$ (with $n-2$ zeros). The reduction then calls the oracle solving (γ, n)-free-module-$\mathrm{CVP}_{\mathrm{cov}}$ on input $\mathbf{B}$ and $\mathbf{t}$, which outputs a vector $\mathbf{s}$. Let us call $\mathbf{s}_1$ the vector formed by the first two coordinates of $\mathbf{s}$. The reduction algorithm finally outputs $\mathbf{s}_1$.

One can check that computing an appropriate value of δ can be done in polynomial time since we know from Lemma 2.1 that $\lambda_d^{(\infty)}(\mathcal{O}_K) \leq \Delta_K^{1/d}$. Constructing $\mathbf{B}$ and $\mathbf{t}$ can also be performed in polynomial time, hence our reduction runs in polynomial time.

Let us now focus on correctness. From the definition of $\mathbf{B}$, we know that $\mathbf{s}_1 \in M_1$. We also know that

$$\|\mathbf{t_1} - \mathbf{s_1}\| \leq \|\mathbf{t} - \mathbf{s}\| \leq \gamma \cdot \mathrm{cov}(M).$$

Let us analyse $\mathrm{cov}(M)$. Because of the special shape of $\mathbf{B}$, we know that

$$\begin{aligned}\mathrm{cov}(M) &= \sqrt{\mathrm{cov}(M_1)^2 + \delta^2 \cdot \mathrm{cov}(\mathcal{O}_K^{n-2})^2} \\ &\leq \sqrt{\mathrm{cov}(M_1)^2 + (\delta \cdot dn \cdot \lambda_d(\mathcal{O}_K))^2} \leq \sqrt{\mathrm{cov}(M_1)^2 + 1}\end{aligned}$$

Moreover, we know from preliminaries that $\mathrm{cov}(M_1) \geq 1/2 \cdot \lambda_1(M_1) \geq \sqrt{d}/2$, where the last inequality follows from the fact that $M_1 \subseteq \mathcal{O}_K^2$. Combining this with the previous inequality yields

$$\mathrm{cov}(M) \leq \sqrt{2} \cdot \mathrm{cov}(M_1).$$

Hence, our reduction solves $(\sqrt{2}\gamma, 2)$-$\mathrm{CVP}_{\mathrm{cov}}$ in M_1 as desired. □

6 Combining the reductions

In this last section, we combine the three reductions from Sections 3, 4 and 5 to prove our main theorems.

Theorem 6.1. *Let $\gamma \geq 1$ and $n \geq 2$ be an integer. For any $\gamma' > 2 \cdot \gamma^3 \cdot \Delta_K^{3/2d}$, there is a probabilistic, polynomial-time reduction from solving (γ', n)-module-SVP in K^n to solving (γ, n)-free-module-SVP in K^n.*

Theorem 6.2. *Let $\gamma \geq 1$ and $n \geq 2$ be an integer. For any $\gamma' > \gamma^2 \cdot \sqrt{2n} \cdot \Delta_K^{1/2d}$, there is a probabilistic, polynomial-time reduction from solving (γ', n)-module-HSVP in K^n to solving (γ, n)-free-module-HSVP in K^n.*

Theorem 6.3. *Let $\gamma \geq 1$ and $n \geq 2$ be an integer. For any $\gamma' \geq \gamma^2 \cdot 5\sqrt{2} \cdot d \cdot \Delta_K^{2/d}$, there is a probabilistic, polynomial-time reduction from solving (γ', n)-module-CVP_{cov} in K^n to solving (γ, n)-free-module-CVP_{cov} in K^n.*

We note that, in the statements above, we chose to make the lower bound on γ' as simple as possible, but not necessarily as tight as possible. If the reader is interested in tighter bounds, it might be worth combining the reductions from the previous sections in a more careful way.

Interestingly, the reduction for SVP is the less tight of the three reductions, if we ignore the factors depending on the field and the module rank. Indeed, in the SVP case, the new approximation factor γ' is cubic in the original approximation factor γ, when for the other two reductions, the new approximation factor γ' is only quadratic in γ. We do not know whether it is possible to decrease the loss to quadratic in γ in the SVP case too, and leave it as an open problem.

Proof (Proof of Theorem 6.1). Let $\gamma_1 = \gamma'$, $\gamma_2 = \frac{\gamma'}{\gamma \Delta_K^{1/d}}$ and $\gamma_3 = \gamma_4 = \gamma$. It holds by definition that $\gamma_1 \geq \gamma_4 \cdot \gamma_2 \cdot \Delta_K^{1/d}$ hence, by Corollary 3.1, we have a reduction from (γ_1, n)-module-SVP to (γ_4, n)-free-module-SVP and γ_2-ideal-HSVP. Then, observe that because of the lower bound on γ' in the theorem statement, we have $\gamma_2 > 2\gamma_3^2 \cdot \Delta_K^{1/2d}$, so by Proposition 4.2 there is a reduction from γ_2-ideal-HSVP to $(\gamma_3, 2)$-free-module-SVP. Finally, by Proposition 5.1, there is a reduction from $(\gamma_3, 2)$-free-module-SVP to (γ_4, n)-free-module-SVP. Combining the three reductions provides a reduction from (γ_1, n)-module-SVP to (γ_4, n)-free-module-SVP as required. □

Proof (Proof of Theorem 6.2). Let $\gamma_1 = \gamma'$, $\gamma_2 = \left(\frac{\gamma'}{\gamma}\right)^n \cdot \Delta_K^{-1/2d}$ and $\gamma_4 = \gamma$. For γ_3, we treat the case $n = 2$ separately: if $n = 2$, we let $\gamma_3 = \gamma \cdot \sqrt{n}$ and if $n \geq 3$ we take $\gamma_3 = \gamma^{3/2} \cdot n^{3/4} \cdot \Delta_K^{1/4d}$.

First, let us observe that by definition of γ_1, γ_2 and γ_4, it holds that $\gamma_1 \geq \gamma_2^{1/n} \cdot \gamma_4 \cdot \Delta_K^{1/2nd}$. Hence, by Corollary 3.2, there is a reduction from (γ_1, n)-module-HSVP to (γ_4, n)-free-module-HSVP and γ_2-ideal-HSVP.

Then, observe that thanks to the lower bound on γ' in the theorem's statement, we have that $\gamma_2 > 2 \cdot (\gamma^{3/2} \cdot n^{3/4} \cdot \Delta_K^{1/4d})^2 \cdot \Delta_K^{1/2d}$ when $n \geq 3$ and $\gamma_2 > 2 \cdot (\gamma \cdot \sqrt{n})^2 \cdot \Delta_K^{1/2d}$ when $n = 2$. In both cases, by choice of γ_3, it holds that $\gamma_2 > 2\gamma_3^2 \cdot \Delta_K^{1/2d}$ and so from Proposition 4.1, we have a reduction from γ_2-ideal-HSVP to $(\gamma_3, 2)$-free-module-HSVP.

Finally, let ε_n be as in Proposition 5.2, that is $\varepsilon_n = 0$ if n is even and $\varepsilon_n = 1/(n-1)$ if n is odd. Note that $\varepsilon_n = 0$ when $n = 2$ and $\varepsilon_n \leq 1/2$ when $n \geq 3$. With this in mind, one can check that $\gamma_3 \geq \gamma_4^{1+\varepsilon_n} \cdot \sqrt{n}^{1+\varepsilon_n} \cdot \Delta_K^{\varepsilon_n/2d}$ in both cases $n = 2$ and $n \geq 3$. From Proposition 5.2, this implies the existence of a reduction from $(\gamma_3, 2)$-free-module-HSVP to (γ_4, n)-free-module-HSVP. Combining the three reductions provides a reduction from (γ_1, n)-module-HSVP to (γ_4, n)-free-module-HSVP as required. □

Proof (Proof of Theorem 6.3). Let $\gamma_1 = \gamma'$, $\gamma_2 = \gamma \cdot 5\sqrt{2} \cdot d \cdot \Delta_K^{1/d}$, $\gamma_3 = \sqrt{2}\gamma$ and $\gamma_4 = \gamma$. By definition and from the lower bound on γ' in the theorem statement, it holds that $\gamma_1 \geq \gamma_4 \cdot \gamma_2 \cdot \Delta_K^{1/d}$ hence, by Corollary 3.3, we have a reduction from (γ_1, n)-module-$\mathrm{CVP}_{\mathrm{cov}}$ to (γ_4, n)-free-module-$\mathrm{CVP}_{\mathrm{cov}}$ and γ_2-ideal-HSVP. Then, by definition of γ_2 and using the fact that $\lambda_d^{(\infty)}(\mathcal{O}_K) \leq \Delta_K^{1/d}$ (see Lemma 2.1), we have $\gamma_2 \geq 5\gamma_3 \cdot d \cdot \lambda_d^{(\infty)}(\mathcal{O}_K)$, so by Proposition 4.3 there is a reduction from γ_2-ideal-HSVP to $(\gamma_3, 2)$-free-module-$\mathrm{CVP}_{\mathrm{cov}}$. Finally, we have $\gamma_3 \geq \sqrt{2} \cdot \gamma_4$ and so by Proposition 5.3, there is a reduction from $(\gamma_3, 2)$-free-module-$\mathrm{CVP}_{\mathrm{cov}}$ to (γ_4, n)-free-module-$\mathrm{CVP}_{\mathrm{cov}}$. Combining the three reductions provides a reduction from (γ_1, n)-module-$\mathrm{CVP}_{\mathrm{cov}}$ to (γ_4, n)-free-module-$\mathrm{CVP}_{\mathrm{cov}}$ as required. □

Acknowledgments

Alice Pellet-Mary is supported by the CHARM ANR-NSF grant (ANR-21-CE94-0003) and by the PEPR quantique France 2030 programme managed by the ANR (ANR-22-PETQ-0008 PQ-TLS). Nam Tran is supported by CSIRO Data61 PhD Scholarship and CSIRO Data61 Top-up Scholarship. This work was done when Nam Tran was a Master student in the University of Limoges (France) and doing his internship at Institute of Mathematics of Bordeaux (IMB, France), founded by IMB.

References

BF14. Jean-François Biasse and Claus Fieker. Subexponential class group and unit group computation in large degree number fields. *LMS Journal of Computation and Mathematics*, 17(A):385–403, 2014.

BGV14. Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (leveled) fully homomorphic encryption without bootstrapping. *ACM Transactions on Computation Theory (TOCT)*, 6(3):1–36, 2014.

BHJ22. Werner Bley, Tommy Hofmann, and Henri Johnston. Computation of lattice isomorphisms and the integral matrix similarity problem. *arXiv preprint arXiv:2202.03526*, 2022.

BS16. Jean-François Biasse and Fang Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. In *SODA*, pages 893–902. Society for Industrial and Applied Mathematics, 2016.

BST+20. M. Bhargava, A. Shankar, T. Taniguchi, F. Thorne, J. Tsimerman, and Y. Zhao. Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves. *Journal of the American Mathematical Society*, 33(4):1087–1099, October 2020.

CDPR16. Ronald Cramer, Léo Ducas, Chris Peikert, and Oded Regev. Recovering short generators of principal ideals in cyclotomic rings. In *EUROCRYPT 2016: Advances in Cryptology - EUROCRYPT 2016*, 2016.

CDW17. Ronald Cramer, Léo Ducas, and Benjamin Wesolowski. Short Stickelberger class relations and application to Ideal-SVP. In *EUROCRYPT 2017: Advances in Cryptology - EUROCRYPT 2017*, 2017.

Coh12. Henri Cohen. *Advanced topics in computational number theory*, volume 193. Springer Science & Business Media, 2012.

DM22. Gabrielle De Micheli and Daniele Micciancio. A fully classical LLL algorithm for modules. *Cryptology ePrint Archive*, 2022.

FPS22. Joël Felderhoff, Alice Pellet-Mary, and Damien Stehlé. On module unique-svp and ntru. In *Advances in Cryptology–ASIACRYPT 2022: 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5–9, 2022, Proceedings, Part III*, pages 709–740. Springer, 2022.

FS10. Claus Fieker and Damien Stehlé. Short Bases of Lattices over Number Fields. In Guillaume Hanrot, François Morain, and Emmanuel Thomé, editors, *ANTS 2010: Algorithmic Number Theory*, volume 6197. Springer, 2010.

Gen09a. Craig Gentry. *A fully homomorphic encryption scheme*. PhD thesis, Stanford University, 2009.

Gen09b. Craig Gentry. Fully homomorphic encryption using ideal lattices. In *STOC 09: Proceedings of the forty-first annual ACM symposium on Theory of computing*. ACM Press, 2009.

GGH+16. Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai, and Brent Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. *SIAM Journal on Computing*, 45(3):882–929, 2016.

Hop98. Andreas Hoppe. *Normal forms over Dedekind domain, efficient implementation in the computer algebra system KANT*. PhD thesis, TU Berlin, 1998.

HPS06. Jeffrey Hoffstein, Jill Pipher, and Joseph H Silverman. Ntru: A ring-based public key cryptosystem. In *Algorithmic Number Theory: Third International Symposiun, ANTS-III Portland, Oregon, USA, June 21–25, 1998 Proceedings*, pages 267–288. Springer, 2006.

Law97. C Lawrence. Washington. introduction to cyclotomic fields, volume 83 of. *Graduate Texts in Mathematics*, page 104, 1997.

LM06. Vadim Lyubashevsky and Daniele Micciancio. Generalized compact knapsacks are collision resistant. In *Automata, Languages and Programming: 33rd International Colloquium, ICALP 2006, Venice, Italy, July 10-14, 2006, Proceedings, Part II 33*, pages 144–155. Springer, 2006.

LPR13. Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. *Journal of the ACM (JACM)*, 60(6):1–35, 2013.

LPSW19. Changmin Lee, Alice Pellet-Mary, Damien Stehlé, and Alexandre Wallet. An LLL-Algorithm for Module Lattice. In Steven D.Galbraith and Shiho Moriai, editors, *Advances in Cryptology - ASIACRYPT 2019*, volume 11922 of *Lecture Notes in Computer Sciences*. Springer, 2019.

LS15. Adeline Langlois and Damien Stehlé. Worst-case to average-case reductions for module lattices. *Designs, Codes and Cryptography*, 75(3):565–599, 2015.

PR06. Chris Peikert and Alon Rosen. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. In *Theory of Cryptography: Third Theory of Cryptography Conference, TCC 2006, New York, NY, USA, March 4-7, 2006. Proceedings 3*, pages 145–166. Springer, 2006.

PS21. Alice Pellet-Mary and Damien Stehlé. On the Hardness of NTRU Problem. In Mehdi Tibouchi and Huaxiong Wang, editors, *Advances in Cryptology - ASIACRYPT 2021*, volume 13090. Springer, 2021.

SSTX09. Damien Stehlé, Ron Steinfeld, Keisuke Tanaka, and Keita Xagawa. Efficient public key encryption based on ideal lattices. In *Advances in Cryptology–ASIACRYPT 2009: 15th International Conference on the Theory and Application of Cryptology and Information Security, Tokyo, Japan, December 6-10, 2009. Proceedings 15*, pages 617–635. Springer, 2009.

Ste15. Noah Stephens-Davidowitz. Dimension-preserving reductions between lattice problems. 2015.