Average hardness of SIVP for module lattices of fixed rank

Koen de Boer, Aurel Page[1], Radu Toma[2], and Benjamin Wesolowski[3]

[1]*Inria, Univ. Bordeaux, CNRS, Bordeaux INP, IMB, UMR 5251, F-33400, Talence, France*
[2]*Sorbonne Univ. and Univ. Paris Cité, CNRS, IMJ-PRG, F-75005 Paris, France*
[3]*ENS de Lyon, CNRS, UMPA, UMR 5669, Lyon, France*

November 18, 2025

Abstract

The problem of finding short vectors in Euclidean lattices is a central hard problem in complexity theory. The case of module lattices (i.e., lattices which are also modules over a number ring) is of particular interest for cryptography and computational number theory. The hardness of finding short vectors in the asymptotic regime where the rank (as a module) is fixed is supporting the security of quantum-resistant cryptographic standards such as ML-DSA and ML-KEM.

In this article we prove the average-case hardness of this problem for uniformly random module lattices (with respect to the natural invariant measure on the space of module lattices of any fixed rank). More specifically, we prove a polynomial-time worst-case to average-case self-reduction for the *approximate Shortest Independent Vector Problem* (γ-SIVP) where the average case is the (discretized) uniform distribution over module lattices, with a polynomially-bounded loss in the approximation factor, assuming the Extended Riemann Hypothesis.

This result was previously known only in the rank-1 case (so-called *ideal lattices*). That proof critically relied on the fact that the space of ideal lattices is a compact group. In higher rank, the space is neither compact nor a group. Our main tool to overcome the resulting challenges is the theory of automorphic forms, which we use to prove a new quantitative rapid equidistribution result for random walks in the space of module lattices.

Contents

1 Introduction

1.1 Motivation

A lattice is a discrete subgroup in a Euclidean vector space. It is typically described by a *basis*, a collection $\mathbf{B} = (b_1, \dots, b_n)$ of linearly independent vectors, and the lattice is the group $\Lambda = b_1\mathbb{Z} + \cdots + b_n\mathbb{Z}$ obtained from all linear combinations with integer coefficients. Since it is discrete, a lattice contains a non-zero vector of smallest possible Euclidean norm, a *shortest vector*.

The task of finding such a shortest vector (the *Shortest Vector Problem*, SVP) is a central hard problem in complexity theory. More generally, one can look for a lattice vector whose norm is within a small factor $\gamma \geq 1$ of the shortest (the *approximate Shortest Vector Problem*, γ-SVP), or for a collection of n short independent vectors (the approximate *Shortest Independent Vector Problem*, γ-SIVP). For small enough approximation factors, problems of this type are believed to be hard, and the best known algorithms have exponential complexity in the dimension of the lattice, in both the classical and quantum paradigms. In their hardest regimes, they are even known to be NP-hard [Mic98; HR07]. However, applications typically fall outside this NP-hard regime, often depend on the *average hardness* of the problems, and mobilize lattices with additional algebraic structure, like *module lattices*. The main question addressed in this article is:

> How hard are lattice problems *on average* in *module lattices*?

Average hardness. No NP-hard problem is known to be hard *on average* (for random instances), and generating random instances that appear consistently hard is a delicate task. This property is critical for applications to cryptography: one needs randomly sampled instances of the problem to be hard with overwhelming probability. Lattice problems are a remarkable family of problems enjoying some proofs of average-case hardness. This property is typically ensured by proving a *worst-case to average-case* reduction: a proof that if random instances of a problem A can be solved efficiently with good probability, then all instances (even the "worst") of problem B can be solved efficiently. Thus, if there exist hard instances of B, then random instances of A are hard. A self-reduction, when $A = B$, is particularly interesting, as it implies that random instances of the problem are, in a precise sense, as hard as they could possibly be. In approximation problems, like γ-SVP, a reduction might degrade the approximation factor. One strives to keep this loss as small as possible, to stay in a regime where the problem is hard.

Ajtai [Ajt96] launched the field of lattice-based cryptography by proving a worst-case to average-case reduction from the approximate shortest vector problem (the worst case, although in a regime unlikely to be NP-hard) to SIS (the average case, for some carefully designed distribution on the set of instances). This line of research has since evolved into a front-runner of quantum-resistant cryptography, now making it into the real world [Nat24b; Nat24a]. SIS, and later LWE [Reg05], have provided highly fertile ground for cryptography, leading to breakthroughs like fully homomorphic encryption [Gen10].

Beyond applications to cryptography, understanding worst-case to average-case reductions for lattice problems helps with the analysis of lattice algorithms. Algorithms such as LLL [LLL82] have experimentally appeared to perform better than their worst-case analysis suggests, both in terms of the running time and the output quality. This mystery has found some explanation through the study of random lattices, see for instance [NS06; KV18]. Indeed, the analysis of algorithms is often eased by heuristics on their geometry, such as the *Gaussian heuristic*. Such heuristics are only true in an *average* sense, for random lattices. The average case being easier to analyze, a worst-case to average-case reduction provides a bridge to deduce information about the worst case. This approach has already been fruitful in the case of *ideal lattices* [BDP+20; BPW25], a particular case of *module lattices*.

Module lattices. Many variants of lattice problems have been studied, and applications to cryptography and computational number theory motivated *algebraically structured* variants: finding short vectors in lattices which are ideals or modules over a number ring (they are called *module lattices*, of which *ideal lattices* are a special case). These can be thought of as lattices with "many symmetries", offering opportunities for more complex algebraic manipulations, faster arithmetic, and shorter representation of elements — all great features for the design of cryptosystems.

A module lattice over a number field K is essentially a lattice $\Lambda \subset K^r$ such that $x\Lambda \subseteq \Lambda$ for any integral element x of the field K (this last condition means that Λ is a module over the ring of integers $\mathcal{O}_K \subset K$). This is a simplification of the definition provided in Section 2.3.2. For the present discussion, we further assume that Λ has full-rank (it contains a basis of the vector space K^r), and we call r the *rank* of the lattice. Forgetting about its module structure, the lattice Λ has $\mathbb{Z}$-rank $r \cdot \deg(K)$, where $\deg(K) = [K : \mathbb{Q}]$ is the degree of the number field, its dimension as a $\mathbb{Q}$-vector space. There is thus a spectrum of ways to construct large lattices: one can balance between choosing a field of large degree $\deg(K)$, or choosing a large rank r. In one extreme case, one can let $K = \mathbb{Q}$ so $\deg(K) = 1$, and we obtain generic lattices (with no additional module structure). At the other end of the spectrum, one can consider a large degree field K and set $r = 1$, and obtain "rank one" module lattices $\Lambda \subset K$, also known as *ideal lattices*; they are in a sense the "most structured" case.

The computational study of module lattices started in the context of computational number theory, as the efficient manipulation of ideals in number fields requires seeing them as lattices (see [Coh13] for a variety of examples). The domain accelerated after its introduction to cryptography, first with Ring-LWE [Mic02] (proven to be at least as hard as an ideal version of SIVP), then with Module-LWE [LS15] (proven to be at least as hard as a module version of SIVP). The digital signature scheme ML-DSA [Nat24b; DKL+18], and the key-encapsulation mechanism ML-KEM [Nat24a; BDK+18], both based on module lattices, recently became the first public-key cryptosystems standardized by the American National Institute of Standards and Technologies for resistance against quantum adversaries. These cryptosystems are proven secure under the assumption that some module-variants of lattice problems are hard, and it has become critical for cryptographers to understand this presumed hardness. The modules at play in these schemes have small rank (at most five). This regime of "small rank" module lattices is precisely the focus of the present paper.

The invariant probability measure. To study the average hardness of lattice problems, one first needs to specify a probability measure on the space of instances: what is a *random* lattice? In this paper, we work with arguably the most natural choice, a measure on the space of lattices that is both mathematically canonical, and practically relevant.

Every lattice can be described by a basis, an element of $\mathrm{GL}_n(\mathbb{R})$. Rescaling has no impact on the difficulty of finding short vectors, so we only consider lattices of volume 1, with basis in $\mathrm{SL}_n(\mathbb{R})$. Now, two bases describe the same lattice if and only if they differ by a *change of basis*: a matrix in $\mathrm{SL}_n(\mathbb{Z})$. Therefore, the space of lattices (of volume 1) can be identified with the quotient $X_n = \mathrm{SL}_n(\mathbb{Z})\backslash \mathrm{SL}_n(\mathbb{R})$ (see Section 2.3.2 for the case of module lattices). This is a homogeneous space for the group $\mathrm{SL}_n(\mathbb{R})$ and it inherits the Haar measure. A fundamental result in reduction theory is that the space of lattices has finite volume and we can thus normalize the measure to a probability measure. It is also referred to as the SL_n-invariant measure, or simply *the invariant measure*, written μ in this introduction. Several facts motivate the study of this particular measure.

- This measure was first introduced by Siegel [Sie45] to prove that the expected value of the number of lattice points inside a ball centered at zero is approximated by the volume of the ball. An important line of research then continued to study more refined such statistics

[Rog55], as well as interactions with algorithms (e.g. [Ajt02; NS06]). This distribution is often the most natural and convenient choice when speaking of "random lattices".

- The invariance of the measure also allows for the theory of automorphic forms to be used as a tool. This rich theory unlocks the spectral analysis of the space $L^2(X_n)$ of square-integrable functions $f : X_n \to \mathbb{C}$. As Section 4 shows, we take full advantage of this.

- Lattice problems are believed to be hard, so to hope for a worst-case to average-case reduction, *easy instances must be rare*: more precisely, the probability to sample a lattice for which the problem is easy must be negligible. There are easy instances for SVP: for instance, if a lattice contains one particularly small vector (exponentially smaller than all other independent vectors), the LLL algorithm [LLL82] will find it in polynomial time. Such "very imbalanced" lattices should have small measure. Conveniently, this is the case for the invariant measure. Sections of the space X containing very imbalanced lattices are referred to as *cusps*, and they do have very small μ-volume, a fact quantified in Section 5 for module lattices. In fact, most of the μ-random lattices, forming the *bulk* of the space, are rather *balanced*.

- For a worst-case to average-case reduction, we need the average-case distribution to be efficiently sampleable. Conveniently, the invariant measure naturally comes up as the limit distribution of simple random processes. In particular, one can start from an arbitrary lattice (say $L_0 = \mathbb{Z}^n \in X_n$), select a "large" prime number p, and sample a uniformly random sublattice $L \subseteq L_0$ of index p. The probability distribution of L is, in a precise sense, *close* to the invariant measure [CU04; GM03] — we call this phenomenon *Hecke equidistribution*.[1] This convenient construction is deceptively simple, as it compares a discrete distribution to a continuous distribution, and hides some computational difficulties. It is nevertheless a powerful idea at the heart of our results, and at least suggests that sampling from the invariant measure should be easy.

Finally, let us point out the main *downside* of the invariant measure: it is continuous. In a computational context, we do not actually manipulate continuous values. Continuity is extremely convenient for algorithmic design and analysis, but in the end, all needs to be discretized, and one must prove that the analysis carries through this discretization. In particular, the average-case distribution for lattice problems is actually a discretized version of the invariant measure. These issues are the object of Section 9.

Prior work, and the inspiring case of ideal lattices. As fruitful as the worst-case to average-case reduction of Ajtai [Ajt96] has been, it has drawbacks. SIS can be posed as a shortest vector problem, so Ajtai's reduction can essentially be seen as a self-reduction (not quite, but an SIVP variant achieves that [Ajt99]) to an average-case distribution that does not resemble the invariant distribution (the SIS distribution is supported on a "small" subset of carefully designed lattices). Yet, the reduction does not preserve the dimension of the lattice. This dimension change incurs a loss in the approximation factor — an obstacle towards approaching an NP-hard threshold. In our regime, this causes an additional issue: we work in fixed rank, and the analogous reductions for modules do not preserve the rank [LS15]. Changing the rank makes for weaker asymptotic statements — especially since there seems to be a hardness gap between rank 1 and other small ranks (see [LPS+19] for an analysis on the relative hardness across ranks).

Self-reductions of SVP and variants have successfully been developed for ideal lattices (i.e., rank 1). They first arise in the work of Gentry [Gen10] on fully homomorphic encryption. There, he develops a worst-case to average-case reduction for the *closest vector problem* (CVP,

[1] This is short for the *equidistribution of Hecke points*, as it is commonly referred to in the literature.

a problem closely tied to SVP) in ideal lattices. The distribution he is considering is the uniform distribution on prime ideals of bounded norm. Translating this result to SIVP through the quantum equivalence of Regev [Reg05] results in a worst-case to average-case (quantum) reduction for SIVP where the average-case distribution is uniform on the *inverse* of prime ideals of bounded norm.

The ideal shortest vector problem was then approached by de Boer, Ducas, Pellet-Mary, and Wesolowski [BDP+20]. They prove a random self-reduction for the average-case distribution defined by the invariant measure, assuming the Extended Riemann Hypothesis (ERH). Their reduction is based on a continuous random walk on the space of ideal lattices, viewed as the so-called *Arakelov class group*. The use of this rich structure was a fruitful addition to the literature on lattice-based cryptography. It was used in the article [FPS+23a] to extend Gentry's work to the uniform distribution on prime ideals (instead of their inverse), with applications to the NTRU cryptosystem. Surprisingly, this work critically relies on the results of [BDP+20] on the invariant measure to analyze a different distribution on ideal lattices. The work [BDP+20] provides a rigorous understanding of random ideal lattices (assuming the Extended Riemann Hypothesis) which has unlocked algorithmic advances. It was used by de Boer [Boe22] to develop the first polynomial time algorithm to compute power residue symbols, and more recently, it has unlocked the first rigorous subexponential algorithms for some of the most fundamental problems in algebraic number theory like the computation of class groups and unit groups [BPW25]. We are hoping that our generalization from the ideal case to the module case will find such varied applications.

The article [BDP+20] is a direct precursor of our paper, both through its choice of the natural invariant measure, and through its methods. They transfer computational problems in an ideal lattice to random sublattices, effectively performing a random walk in the space of ideal lattices. This space is a compact and abelian topological group, and the study of this random walk boils down to a study of generalized class groups and Fourier analysis.

Extending this strategy to modules of higher rank presents significant challenges, related to the fact that the space of module lattices in rank > 1 is no longer compact, nor is it a group. A key insight is that the Fourier analysis underlying [BDP+20] is the theory of automorphic forms for $\mathrm{GL}(1)$. The much deeper automorphic machinery for the non-commutative group $\mathrm{GL}(r)$, $r > 1$, provides a higher rank analog, as already observed in [DK22]. However, exploiting it has proved considerably more delicate due to the necessity of studying important, yet historically overlooked aspects with high precision.

A concrete and fundamental issue arising with $r > 1$ is imbalancedness. On one hand, ideal lattices cannot have extremely short vectors: their shortest vectors are not much shorter than the vectors of their shortest bases — we say that these lattices are balanced. On the other hand, module lattices of higher rank can be arbitrarily imbalanced. Topologically, this manifests into the fact that the space of module lattices for rank $r > 1$ is not compact. This is an entirely new dimension of the problem, and it leads to serious limitations to a naive generalization of the random walk.

We note that the idea of random walks giving rise to reductions and their study using automorphic theory also emerged in another branch of cryptography based on abelian varieties, in particular elliptic curves. See for instance [JMV09] and [PW24]. In contrast to the above, this setting is discrete by nature, given by graphs of abelian varieties connected through isogenies. For example, in the case of supersingular elliptic curves, one may study random walks using automorphic forms on definite quaternion algebras [PW24].

1.2 Results

We obtain in this paper the first random self-reduction of a shortest vector problem for module lattices beyond ideal lattices, Theorem 1. This also marks the first application of automorphic

forms on $\mathrm{GL}(n)$ to the complexity theory of lattice problems.

Let us start by formalizing the main computational problem we consider in this article, γ-SIVP. Recall that the successive minima of a lattice L of dimension n are defined as

$$\lambda_j(L) = \min\left\{ \lambda \in \mathbb{R}_{>0} \;\middle|\; \begin{array}{l} \text{there exist } \mathbb{R}\text{-linearly independent vectors } (x_i)_{i=1}^{j} \\ \text{such that } x_i \in L \text{ and } \|x_i\| \le \lambda \text{ for all } i \end{array} \right\},$$

for $j \in \{1, \dots, n\}$. Given as input a basis $\mathbf{B}$ of an n-dimensional lattice L and an approximation factor $\gamma \in \mathbb{R}_{\ge 1}$, the *$\gamma$-shortest independent vector problem* (or γ-SIVP) is the computational task of finding $\mathbb{R}$-linearly independent lattice vectors $x_1, \dots, x_n \in L$ that satisfy $\|x_i\| \le \gamma \cdot \lambda_n(L)$ for all $i \in \{1, \dots, n\}$. The problem remains the same when we look at module lattices: the input is a module lattice M, and we require the same condition $\|x_i\| \le \gamma \cdot \lambda_n(M)$.

Let us now briefly introduce the average-case distribution: the discretized version of the invariant probability measure μ on the space $X_r(K)$ of module lattices of rank r over a number field K. It can be described through a rounding algorithm, which we call $\mathrm{Round}_{\mathrm{Lat}}$ and defined in Section 3. Given an arbitrary lattice L, the output $\mathrm{Round}_{\mathrm{Lat}}(L)$ is a randomly generated *rational* module lattice (one which can be represented and manipulated on a computer or, more formally, on a Turing machine) that is geometrically close to L. We write $\mathrm{Round}_{\mathrm{Lat}}(\mu_{\mathrm{cut}})$ for the distribution on rational module lattices coming from applying $\mathrm{Round}_{\mathrm{Lat}}$ to μ-random lattices (with a tail-cut, removing a negligibly small section of the space, to ensure that the distribution is supported on a compact set). This defines the average case; see Section 10 for the precise definition.

We insist that $\mathrm{Round}_{\mathrm{Lat}}$ replaces any lattice with a "very close" one: the distinction between μ_{cut} and $\mathrm{Round}_{\mathrm{Lat}}(\mu_{\mathrm{cut}})$ is similar to the distinction between the continuous uniform distribution on $[0, 1]$, and its discretization by rounding real numbers in $[0, 1]$ to a certain number of bits of precision.

Theorem 1. *Let K be a number field of degree d and discriminant Δ_K. Fix a rank $r \in \mathbb{Z}_{>1}$, and let $n = rd$. Assume ERH for the L-function of every Hecke character of K of trivial modulus. Let $\mathscr{O}$ be an oracle for γ'-SIVP which succeeds with probability*[2] *$p = 2^{-o(n)}$ when its input follows distribution $\mathrm{Round}_{\mathrm{Lat}}(\mu_{\mathrm{cut}})$. There is a probabilistic polynomial time algorithm for γ-SIVP over any module lattice of rank r over K with $\gamma = \mathrm{poly}_r(|\Delta_K|^{1/d}, d) \cdot \gamma'$, making an expected number of*[3] *$\mathrm{poly}_r(\log |\Delta_K|) \cdot p^{-1}$ queries to $\mathscr{O}$.*

This result relies heavily on a quantitative Hecke equidistribution theorem for specific natural test functions that is uniform in all parameters. The full statement is given in Theorem 3, and we believe it is of independent interest. See a special case of this theorem in a simplified version, Theorem 2, in the next section.

Indeed, the problem of equidistribution of Hecke points has a rich history: it was already considered by Linnik and Skubenko [LS64] and became particularly influential at the turn of the century through its generalizations (see e.g. Sarnak's ICM address [Sar91]). Solutions of greater and greater generality were proven using a wealth of methods, from representation theoretic in [COU01] to ergodic theoretic, based on measure rigidity in [EO06] (see the cited papers for more references).

Most of the literature has focused on proving statements as general as possible, with explicit and sharp rates of equidistribution for *general* test functions. However, we return to the classical interpretation in terms of lattices and ask the following natural question. Let L be any given

[2]The oracle is *Monte Carlo* in the sense that when it does not succeed, it might still return an incorrect response. The assumption that the error probability satisfies $p = 2^{-o(n)}$ is not fundamental: the problem can be solved in time $2^{O(n)}$ anyway, and we did not attempt to fine-tune our approach for the narrow regime where p is in $2^{-O(n)}$ but not in $2^{-o(n)}$.

[3]The notation $f = \mathrm{poly}_r(g)$ means that $|f| = |g|^{O(1)}$ where the implicit constants in $O(1)$ may depend on r (but on no other parameter).

lattice and consider a smoothened δ-distribution centered at L (i.e. take a bump function as test function). How does the equidistribution rate of Hecke operators applied to this distribution depend on L and, in particular, on the rank and balancedness of L? Adapting the work of Clozel–Ullmo [CU04], introducing geometry of numbers and carefully making constants explicit, we give an answer to this question. We expect further interesting refinements to be possible.

We rely on another result that we believe to be of independent interest: we prove that random module lattices are somewhat balanced with overwhelming probability; it is the content of our Theorem 4. This is related to recent work of Gargava, Serban, Viazovska and Viglino [GSV+25b; GSV+25a] but our methods are different. Precisely, relying on computations by Thunder [Thu98] and generalizing work of Shapira and Weiss [SW14], we bound the proportion of semistable lattices in the sense of Grayson–Stuhler [Gra84].

1.3 Technical overview

In this section, we give an overview of our worst-case to average-case reduction for γ-SIVP.

Randomizing lattices. For the moment, let us forget about modules, and consider generic lattices. The starting point of our strategy is rather simple: we leverage the fact that given a lattice L_0 and a large prime p, a uniformly random sublattice $L \subseteq L_0$ of index p is equidistributed in the space of lattices, with respect to the measure μ. Before properly quantifying this property and translating them to module lattices, let us sketch how it can be used to build worst-case to average-case reductions.

Suppose we have an algorithm for γ-SIVP that works well on average: given a μ-random lattice L, the algorithm finds linearly independent vectors $(x_i)_{i=1}^n$ such that $\|x_i\| \leq \gamma \cdot \lambda_n(L)$ with good probability. Now, we are given a lattice L_0, a worst-case instance. A straightforward idea would be to pick a large enough prime p and a sublattice $L \subset L_0$ of index p, and use our algorithm on L. As L is equidistributed, we expect the algorithm to find linearly independent vectors $(x_i)_{i=1}^n$ such that $\|x_i\| \leq \gamma \cdot \lambda_n(L)$ with good probability. Since $L \subset L_0$, these vectors are also in L_0. However, proposing $(x_i)_{i=1}^n$ as a solution of SIVP for L_0, the lengths must be compared to $\lambda_n(L_0)$ instead of $\lambda_n(L)$.

In general, we only have $\lambda_n(L) \leq p\lambda_n(L_0)$ (an inequality reached with $L_0 = \mathbb{Z}^n \supset \mathbb{Z}^{n-1} \oplus p\mathbb{Z} = L$), which suggests that $(x_i)_{i=1}^n$ only solves $p\gamma$-SIVP, a considerable loss in the quality of the solution. However, the extreme case $\lambda_n(L) \approx p\lambda_n(L_0)$ is actually rare, and in a precise sense, for random sublattices L, one expects $\lambda_n(L) \approx p^{1/n}\lambda_n(L_0)$. Indeed, as L is equidistributed, the Gaussian heuristic applies, thus we expect $\lambda_n(L)$ to be of the order of $\det(L)^{1/n} = p^{1/n}\det(L_0)^{1/n} = O(p^{1/n}\lambda_n(L_0))$. This "balancedness of random lattices" is studied in more detail in Section 5, where we prove Theorem 4.

The problem of imbalancedness. In conclusion, this simple strategy appears to provide a worst-case to average-case reduction for SIVP, with a loss of $p^{1/n}$ in the approximation factor. Now, what does p *sufficiently large* mean? On one hand, we want it to be small, to stay in a regime where SIVP is as hard as possible: the smaller the better, but let us aim for an approximation factor that is polynomial in the dimension n (a regime in which all known algorithms have exponential complexity). In other words, we require that $p^{1/n} = n^{O(1)}$, i.e., $p = n^{O(n)}$. On the other hand, we require p to be large enough for the random sublattice L to be equidistributed. This is where difficulties arise, as this constraint actually depends on the initial lattice L_0.

For instance, consider the lattice $L_\varepsilon = \varepsilon\mathbb{Z} \oplus \mathbb{Z}^{n-1}$, where $\varepsilon \in \mathbb{R}_{>0}$ is very small. It contains the small vector $x_\varepsilon = (\varepsilon, 0, \ldots, 0)$. For any index-$p$ sublattice $L \subset L_\varepsilon$, we have $px_\varepsilon \in L$, so $\lambda_1(L) \leq \|px_\varepsilon\| = p\varepsilon$. If L were equidistributed, we would expect $\lambda_1(L)$ to be of the order of

$\det(L)^{1/n}$, yet $\lambda_1(L) \leq p\varepsilon$ and $\det(L)^{1/n} = (p\varepsilon)^{1/n}$. Therefore, for index-$p$ sublattices of L_ε to be equidistributed, we need p to be at least as large as ε^{-1}.

These lattices L_ε, with vanishingly small ε, are *imbalanced*, they contain unusually short vectors. We can think of these imbalanced lattices as living in a remote corner of the space of lattices, so far away that to reach the rest, we need to take a gigantic step of index $p > \varepsilon^{-1}$. For such initial lattices $L_0 = L_\varepsilon$, the simple reduction sketched above cannot work, as the loss $p^{1/n}$ in the approximation factor could be arbitrarily large.

A trichotomy. This notion of *balancedness* is key, and to quantify it properly, let us return to our actual objects of interest: module lattices. For the rest of the article, we fix a number field K of degree d, we fix a rank $r = O(1)$, and we will consider module lattices of rank r over K. Such a module lattice M is still a lattice in the usual sense, of dimension dr, and we can speak of its successive minima $\lambda_i(M)$. Its module structure gives rise to a convenient variant of this notion, the K-successive minima $\lambda_i^K(M)$ defined as

$$\lambda_j^K(M) = \min\left\{ \lambda \in \mathbb{R}_{>0} \;\middle|\; \begin{array}{l} \text{there exist } K\text{-linearly independent vectors } (x_i)_{i=1}^j \\ \text{such that } x_i \in M \text{ and } \|x_i\| \leq \lambda \text{ for all } i \end{array} \right\},$$

for $j \in \{1, \ldots, r\}$. Each $\lambda_i(M)$ is approximately as large as $\lambda^K_{\lceil i/d \rceil}(M)$ (see Lemma 2.13). Now, we say that a module lattice M is α-*balanced* if $\lambda^K_{j+1}/\lambda^K_j \leq \alpha$ for all $j \in \{1, \ldots, r-1\}$.

As discussed above, the straightforward reduction consisting in taking random sublattices fails for very imbalanced lattices like L_ε. The notion of α-balancedness measures this precisely, and allows us to divide our reduction into three regimes, illustrated in Figure 1.

- **The bulk.** "Most" lattices are fairly balanced: they form what we call the *bulk* of the space. Informally, we say that M belongs to the bulk if it is α-balanced with $\alpha = d^{O(1)}$. We prove that for such M, the simple strategy sketched above (reducing SIVP to random sublattices) can be made to work. In Section 1.3.1, we give more details on this regime and an overview of the proof of equidistribution. The full proof is the object of Section 4 and Section 5.

- **The cusp.** As illustrated with L_ϵ, the simple strategy fails for imbalanced lattices. When the imbalancedness is extreme enough, it can be detected and exploited by polynomial time algorithms like LLL. This region of the space is referred to as the *cusp*, and roughly consists of lattices which are *not* α-balanced for some threshold $\alpha = 2^{O(d)}$. This region has very small μ-measure, and can be thought of as very "thin" and "elongated", with lattices like L_ϵ going "to infinity" as $\varepsilon \to 0$ (see Figure 1). In Section 1.3.2, we give an overview of the strategy to reduce SIVP from the cusp to the balanced case. The full proof is the object of Section 6.

- **The flare.** Between the bulk (where randomization works well) and the cusp (where algorithms like LLL come in handy) remains a region of moderately-balanced lattices: the *flare*[4]. It consists of lattices that are $2^{O(d)}$-balanced, but not $d^{O(1)}$-balanced. From such a lattice, we prove that we can reduce SIVP to another lattice which is in the bulk. We give an overview of this step in Section 1.3.3. The full proof is the object of Section 7.

1.3.1 The bulk

In this section, we explain our technique in the regime where lattices are balanced: we start from a lattice L_0 in the bulk. As already explained, we reduce SIVP in L_0 to SIVP in a random

[4]This notion is not canonical. It comes from the gradual widening in Figure 1.

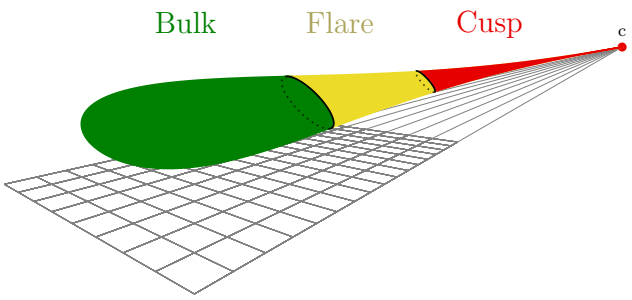

Figure 1: Schematic illustration of a single connected component of the space of module lattices.

sublattice $L \subseteq L_0$ — but we are now in the context of module lattices. We work in the space X_r of rank-r module lattices (over K). It is defined analogously to the space $\mathrm{SL}_n(\mathbb{Z})\backslash \mathrm{SL}_n(\mathbb{R})$ of generic lattices, but the module structure introduces technicalities, the details of which are deferred to Section 2.3.2.

Instead of a prime number p, and a sublattice $L \subseteq L_0$ of index p (i.e., $L_0/L \cong \mathbb{Z}/p\mathbb{Z}$), we consider a prime ideal $\mathfrak{p}$ (in the ring of integers $\mathcal{O}_K$ of K) and consider sub-module lattices $L \subseteq L_0$ of index $N(\mathfrak{p})$ with $L_0/L \cong \mathcal{O}_K/\mathfrak{p}$ as $\mathcal{O}_K$-modules (we might say that L has "index $\mathfrak{p}$" in L_0).

Random processes and Hecke operators. This process of taking random sublattices can be thought of as a random walk in the space X_r. It can be formalized as an operator on probability distributions of X_r, or, more conveniently, on the Hilbert space $L^2(X_r)$ (of square-integrable functions $X_r \to \mathbb{C}$ for the measure μ). Given a prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$, the Hecke operator $T_\mathfrak{p} : L^2(X_r) \to L^2(X_r)$ is defined for each $f \in L^2(X_r)$ and each $L \in X_r$ as

$$T_\mathfrak{p} f(L) = \frac{1}{D_\mathfrak{p}} \sum_{\substack{M \subset L \\ L/M \cong \mathcal{O}_K/\mathfrak{p}}} f(M),$$

where $D_\mathfrak{p} = 1 + N(\mathfrak{p}) + \ldots + N(\mathfrak{p})^{r-1}$ is the number of terms in the sum. This operator is averaging over all "index $\mathfrak{p}$" sublattices. Its probabilistic interpretation is as follows. Suppose that $f \in L^2(X_r)$ is a probability density function. Then, $T_\mathfrak{p} f$ is the probability density function for the experiment which consists in sampling a lattice L with density f, then selecting a uniformly random sublattice of L of index $\mathfrak{p}$. Assuming that the measure μ is a probability measure implies that the constant function $\mathbf{1}$ is its probability density function. Note that $T_\mathfrak{p}\mathbf{1} = \mathbf{1}$.

The idea that, for $\mathfrak{p}$ large enough, sublattices of index $\mathfrak{p}$ are equidistributed can be formalized as follows. For an initial probability distribution $f \in L^2(X_r)$, the L^1-distance (which is the notion of statistical distance we use in this paper) $\|T_\mathfrak{p} f - \mathbf{1}\|_1$ converges to 0 as $N(\mathfrak{p})$ grows. To apply this, we must now ask for an explicit rate of convergence, which will depend on f.

Note that, starting from a lattice L_0, it is tempting to consider the Dirac distribution δ_{L_0} centered at L_0, and to study the distribution $T_\mathfrak{p}\delta_{L_0}$ of uniformly random sublattices of L_0. However, these are discrete distributions in a continuous space: no matter how large $\mathfrak{p}$ is, the distribution $T_\mathfrak{p}\delta_{L_0}$ remains discrete and $\|T_\mathfrak{p}\delta_{L_0} - \mathbf{1}\|_1 = 1$. Instead, we "smoothen" the distribution δ_{L_0}, and consider a continuous distribution φ_{L_0} that is highly concentrated around L_0. One can think of it as the uniform distribution in a small ball around L_0: it samples random lattices which are, geometrically, very close to L_0. The precise definition of φ_{L_0} is the object of Section 4.1.

Equidistribution via the theory of automorphic forms. The question becomes: given a lattice L_0 and a probability density function φ_{L_0} concentrated around L_0 as above, how fast does $T_{\mathfrak{p}}\varphi_{L_0}$ tend to $\mathbf{1}$ in L^1-norm as $N(\mathfrak{p})$ grows? In other words, how large does $N(\mathfrak{p})$ need to be for the distance $\|T_{\mathfrak{p}}\varphi_{L_0} - \mathbf{1}\|_1$ to be negligibly small?

To answer this, we follow the ideas of Clozel–Ullmo in their work on Hecke equidistribution [CU04]. They apply the principle behind the Weyl criterion, which suggests spectrally decomposing φ_{L_0} and analyzing the action of $T_{\mathfrak{p}}$ on the spectral components, given in terms of automorphic forms or automorphic representations. For $\mathrm{GL}(r)$, doing this relies on deep theorems by Langlands and Moeglin–Waldspurger, who made the decomposition explicit enough for computations. We review this theory in Section 2.7.

The main input is the spectral gap for $T_{\mathfrak{p}}$, an important object of study in number theory (see the Ramanujan Conjecture [BB13]), consisting in strong bounds for its eigenvalues. However, generalizing Clozel–Ullmo [CU04] to number fields requires some care due to the fact that $L^2(X_r)$ contains a large subspace behaving like $L^2(X_1)$, where $T_{\mathfrak{p}}$ acts by unitary characters. Its eigenvalues thus have absolute value 1 there.

To make this formal, we introduce a "splitting" of $\mathrm{GL}(r)$ into $\mathrm{SL}(r)$ and $\mathrm{GL}(1)$ using the determinant function (see Section 2.6). It corresponds to a decomposition

$$L^2(X_r) = L^2_{\mathrm{det}}(X_r) \oplus L^2_{\mathrm{det}}(X_r)^{\perp}.$$

On $L^2_{\mathrm{det}}(X_r)^{\perp}$, the operator $T_{\mathfrak{p}}$ has small eigenvalues, whilst the space $L^2_{\mathrm{det}}(X_r)$ captures the spectral theory of $\mathrm{GL}(1)$. We also use this splitting through corresponding "distance functions" that allow us to define φ_{L_0}: first, take a basis $z \in \mathrm{GL}_r(K_{\mathbb{R}})$ for L_0 and construct the normalized bump function f_z that is the characteristic function of a ball in the $\mathrm{SL}(r)$-direction and a Gaussian in the $\mathrm{GL}(1)$-direction, both centered at elements corresponding to z. Then we average f_z over all bases of L_0 to obtain φ_{L_0} (this is sometimes called an automorphic kernel). See Section 4.1 for more details.

Schematically, we now do the following. We choose a special basis of automorphic forms (ϖ) for the space $L^2_{\mathrm{det}}(X_r)^{\perp}$ and (χ) for the space $L^2_{\mathrm{det}}(X_r)$. In particular, there is the constant function $\mathbf{1} = \chi_0$. These spaces have discrete, as well as continuous spectrum, and we informally write the decomposition of φ_{L_0} as

$$\varphi_{L_0} = \int_{\chi} \langle \varphi_{L_0}, \chi \rangle \, \chi + \int_{\varpi} \langle \varphi_{L_0}, \varpi \rangle \, \varpi.$$

Crucially, the operator $T_{\mathfrak{p}}$ acts on ϖ and χ by scalars. It is normalized so that $T_{\mathfrak{p}}\mathbf{1} = \mathbf{1}$. By representation theoretic methods, one may compute that $T_{\mathfrak{p}}$ acts on ϖ with eigenvalue bounded in absolute value by $rN(\mathfrak{p})^{-3/8}$, fact which relies on bounds towards the Ramanujan conjecture.

However, on χ it acts by $\chi(\mathfrak{p})$, a number of absolute value one. Fortunately, we have a phenomenon generalizing the orthogonality of characters: a sum of the shape $\sum_{\mathfrak{p}} \chi(\mathfrak{p})$ exhibits cancellation for all $\chi \neq \chi_0$. A strong quantitative version of this fact was proved and used in [BDP+20] to treat the case of ideal lattices (the $\mathrm{GL}(1)$ case) under the Extended Riemann Hypothesis. We therefore study an average of Hecke operators

$$T_{\mathcal{P}} = \frac{1}{|\mathcal{P}|} \sum_{\mathfrak{p} \in \mathcal{P}} T_{\mathfrak{p}},$$

where $\mathcal{P}$ consists of all primes of norm at most B for some $B > 1$. At the level of the algorithm, this means we randomize the prime $\mathfrak{p}$.

The spectral gap and the results of [BDP+20], together with Parseval's identity, show a bound of the rough shape (see below for a more precise statement)

$$\begin{aligned} \|T_{\mathcal{P}}\varphi_{L_0} - \mathbf{1}\| &= \left\| \int_{\chi \neq \chi_0} \langle \varphi_{L_0}, \chi \rangle \, T_{\mathcal{P}}\chi + \int_{\varpi} \langle \varphi_{L_0}, \varpi \rangle \, T_{\mathcal{P}}\varpi \right\| \\ &\leq rd^{3/2}B^{-3/8} \, \|\varphi_{L_0} - \mathbf{1}\| \leq rd^{3/2}B^{-3/8} \, \|\varphi_{L_0}\| \, . \end{aligned}$$

This generalizes the work of Clozel–Ullmo to number fields.

However, we turn to the question of how this rate of equidistribution depends on L_0: we must bound $\|\varphi_{L_0}\|$, which is one of our new contributions. We reduce this to a counting problem that has been encountered in other contexts of analytic number theory. When $K = \mathbb{Q}$, taking a basis matrix $z \in \mathrm{SL}_n(\mathbb{R})$ to represent L_0, it asks for a bound on the number of $\gamma \in \mathrm{SL}_n(\mathbb{Z})$ such that γz lies in a ball of small radius around z in the symmetric space $\mathrm{SL}_n(\mathbb{R})/\mathrm{SO}(n)$. While a generalization of the classical circle problem asks for bounds uniform in the radius, in this case we require uniformity in the center of the ball. Indeed, if z goes deeper into the cusp, defining a very imbalanced lattice L_0, then this number of γ grows.

We solve this problem over any number field in Section 4.2.2, producing bounds in terms of the K-successive minima of the lattice L_0. Considering lattices defined by diagonal matrices and unipotent γ, our bounds seem to be essentially sharp.

Piecing everything together, we obtain the quantitative equidistribution theorem, Theorem 3, with very explicit dependence on all parameters. We give a simplified variant here to point out the quantities that show up.

Theorem 2 (Hecke equidistribution theorem: special case)**.** *For ℓ prime, let K be the ℓ-th cyclotomic field, and let $d = \ell - 1$ be its degree. Let $X_r(K)$ be the space of rank r module lattices over K equipped with the invariant probability measure μ. Let φ_{L_0} be the bump function on $X_r(K)$ centered around a lattice L_0 defined in Section 4.1, and let $\mathbf{1}$ denote the constant 1 function on $X_r(K)$. If $\mathfrak{p}$ is a prime ideal of norm p, define $T_\mathfrak{p}$ as the Hecke operator averaging over submodules with quotient space given by $\mathcal{O}_K/\mathfrak{p}$. For a large parameter $B \gg d \log d$, let*

$$T_\mathcal{P} = \frac{1}{|\mathcal{P}|} \sum_{\mathfrak{p} \in \mathcal{P}} T_\mathfrak{p},$$

where $\mathcal{P}$ is the set of primes of norm at most B. Finally, assume ERH for the L-function of every Hecke character of K of trivial modulus. Then, for any $\varepsilon > 0$, if L is α-balanced, we have

$$\|T_\mathcal{P} \varphi_{L_0} - \mathbf{1}\| = O\left(d^{3/2+\varepsilon} B^{-1/2+\varepsilon} + (rd)^{O(r^2 d)} \alpha^{O(r^3 d)} B^{-3/8+\varepsilon}\right)$$

where the implied constants depend only on ε.

Note that the $\mathbb{Q}$-dimension of a module lattice L over a degree d field K is given by $n = dr$. For the quantity $\|T_\mathcal{P} \varphi_{L_0} - \mathbf{1}\|$ to be negligible, e.g. smaller than 2^{-n}, we must have that

$$B \gg \max((rd)^{Cr^2 d}, \alpha^{Cr^3 d}) \tag{1}$$

for some large enough constant $C > 0$. With such B, the process of choosing a random sublattice $L \subset L_0$ produces a μ-random lattice L (up to a negligible error).

Following the steps and observations described above, we can now solve SIVP for L_0 by solving it in L: we find linearly independent vectors $(x_i)_{i=1}^n$ in L such that $\|x_i\| \leq \gamma \lambda_n(L)$, and since L is μ-random, we have with overwhelming probability that $\lambda_n(L)$ is roughly bounded by $\det(L)^{\frac{1}{n}} = O(B^{1/n} \lambda_n(L_0))$ (Theorem 4). This results in a loss of $B^{1/n}$ in the approximation factor. Minimizing B above, this remains polynomial in n if $\alpha \ll n^{O(1/r)}$. This means that the randomization works well when L_0 is α-balanced for[5] $\alpha = \mathrm{poly}_r(d)$. This region of the space with polynomially-bounded α constitutes the *bulk* as defined above.

As this randomization requires L_0 to be balanced, we next show how to reduce SIVP in imbalanced lattices to the balanced case.

[5]Note that the dependence in the rank is exponential, hinting at difficulties for the regime asymptotic in r.

1.3.2 The cusp

Very imbalanced lattices are generally speaking easier instances of short vector problems due to the existence of the LLL algorithm, as previously noted. However, applying such an algorithm in our situation still requires some careful lattice "surgery", cutting and glueing together instances following a divide and conquer strategy. We obtain in Theorem 5 a reduction from SIVP in any module lattice of rank r to SIVP in at most r module lattices, still of rank r, but now with the guarantee that they are somewhat balanced (they are in the flare).

Finding dense sublattices. The idea is the following. Consider a lattice L that is *not* α-balanced, for some α (large enough, and part of our task here is determining what *large enough* means). There is an index k such that $\lambda^K_{k+1}(L) > \alpha\lambda^K_k(L)$. This translates to a gap of the form $\lambda_{j+d}(L) > \alpha\lambda_j(L)$ between the standard successive minima. One can compute an LLL-reduced basis $(b_i)_i$ of L, with the guarantee that

$$\|b_i\| \leq 2^{(rd-1)/2}\lambda_i(L),$$

for all i. If $\alpha > 2^{(rd-1)/2}$, we obtain that $\|b_i\| < \lambda_{j+d}(L)$ for all $i \leq j$. This means that the first j vectors founds by LLL are all in the subspace generated by the first $j + d - 1$ smallest vectors of the lattice. This is not sufficient yet, but under a slightly stronger bound for α, and looking at *module* sublattices, we realize that LLL reveals K-independent vectors $(b'_i)_{i=0}^k$ such that $\|b'_i\| < \lambda^K_{k+1}(L)$. In particular, these vectors span the same K-subspace V as the k first K-minima. We can therefore deduce a basis of $L' = L \cap V$: a sublattice of L' whose K-minima are exactly $\lambda^K_1(L), \ldots, \lambda^K_k(L)$. The detailed proof is the object of Lemma 6.2. Finding short vectors in L' immediately reveals short vectors in L. Furthermore, while L' might still not be α-balanced, it has at least one fewer gaps than L (the one separating $\lambda^K_k(L)$ from $\lambda^K_{k+1}(L)$). A recursive application of this strategy ultimately leads to a lattice with no gaps left: an α-balanced lattice.

Lattice surgery. Note that $\lambda_1(L') = \lambda_1(L)$, so a solution for SVP can easily be transferred. But for SIVP, we need to find $n = rd$ independent vectors of L, that is more than exist in L'. A solution of SIVP in L' does not give a complete solution for L: we also need to solve SIVP in a "complementary lattice": the orthogonal projection $\pi(L)$ of L along $V = \mathrm{span}_K(L')$. The successive minima of $\pi(L)$ are very close to $\lambda^K_{k+1}(L), \ldots, \lambda^K_r(L)$; the small discrepancy causes a small loss in the approximation factor. This is proved in Lemma 6.3.

In summary, LLL can detect large gaps between $\lambda^K_k(L)$ and $\lambda^K_{k+1}(L)$, and can effectively split the lattice L "around that gap", resulting in two lattices L' (or rank k) and L'' (of rank $r - k$) such that the minima of L' are $\lambda^K_1(L), \ldots, \lambda^K_k(L)$, and the minima of L'' are *almost* $\lambda^K_{k+1}(L), \ldots, \lambda^K_r(L)$. To solve SIVP in L, it is sufficient to solve SIVP in L' and L''. Applying this recursively results in a collection of lattices $L_1, \ldots, L_t$ whose successive minima have no remaining large gap, and whose ranks sum to r (Lemma 6.5). This reduction of the dimension sounds good in practice, but to ultimately achieve a worst-case to average-case reduction, we wish to preserve the dimension. Therefore, in a final step, we show how each L_i can be embedded in a module lattice of rank r in a way that preserves its balancedness (Lemma 6.6).

1.3.3 The flare

If α is larger than some polynomial in d but not exponentially large, we must proceed differently. The idea is still to take sublattices with the goal of reducing the size of α, which measures "gaps" in between the successive minima. The principle is as follows.

Take a unimodular lattice L of rank 2 over $\mathbb{Q}$ with shortest vector v of very small size λ_1. There exists a reduced basis (v, w) of L with w a vector of much larger size $\lambda_2 \asymp 1/\lambda_1$. Choosing a sublattice of index p amounts to multiplying either v or w by p and taking some

linear combinations to form a new basis. Put another way, one chooses a subspace of dimension one inside the 2-dimensional $\mathbb{Z}/p\mathbb{Z}$-vector space L/pL.

There are $p+1$ possibilities to do so, yet only one that contains the projection of v: indeed, v is a primitive vector and spans a unique one-dimensional subspace in L/pL. Thus, with very high probability, i.e. $p/(p+1)$, the sublattice does not contain v, but it contains pv — the basis of the new sublattice is of the form $(pv, w + kv)$ for some $0 \leq k \leq p-1$. If $p\lambda_1 < \lambda_2$, then $p\lambda_1$ must be the shortest length in the sublattice, and λ_2 remains a good approximation for the second successive minimum. The gap between λ_1 and λ_2 can thus be reduced by $1/p$.

To generalize this idea to higher rank n, we must use different types of Hecke operators. This corresponds to taking sublattices with different, fixed structures of the quotient space: consider those sublattices corresponding to subspaces of L/pL of dimension k for some $1 \leq k \leq n-1$. Now, let $1 \leq i \leq n-1$ and assume we have a large i-th gap λ_{i+1}/λ_i and $p < \lambda_{i+1}/\lambda_i$. Then we can prove that, with high probability, sublattices $L' \subset L$ such that $L/L' \cong (\mathbb{Z}/p\mathbb{Z})^i$ have i-th gap reduced by $1/p$, i.e., equal to $\lambda_{i+1}/p\lambda_i$, and all other gaps remain approximately the same (see Section 7.1).

With this technique, we could close "exponentially large" gaps, but it requires knowing at which index the gaps are, and how large they are. Gaps in the flare are *moderately* large, so they cannot be detected in the same way as gaps in the cusp (Section 1.3.2). We therefore "guess" the dyadic sizes and apply the process. There are $O(n \log n)$ dyadic intervals for each gap, but there are r-many gaps. The number of possible guesses is thus exponential in the rank — this is fine in our fixed-rank regime, but is another big obstacle to treating generic lattices. Once the correct guess has been found, SIVP is reduced from the flare to the bulk (see Section 7).

1.4 Acknowledgments

The authors would like to thank Thibault Monneret for his comments, which helped improve this article. R.T. was supported by European Research Council Advanced Grant 101054336 and the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 101034255. At the time of this research, K.dB. was affiliated with the Mathematical Institute, Universiteit Leiden. B.W. was supported by the PEPR quantique France 2030 programme (ANR-22-PETQ-0008), and by the HQI initiative (ANR-22-PNCQ-0002). B.W. was supported by the European Research Council under grant No. 101116169 (AGATHA CRYPTY). B.W. and A.P. were supported by the ANR CHARM project (ANR-21-CE94-0003). A.P. was supported by the ANR AGDE (ANR-20-CE40-0010).

2 Preliminaries

2.1 Notation

For every abelian group A, let $A_{\mathbb{R}}$ denote $A \otimes \mathbb{R}$. For a representation V of a group G, let V^G denote the space of fixed points $\{v \in V \mid gv = v \text{ for all } g \in G\}$.

For two complex-valued functions f and g, we occasionally write $f(x) \ll g(x)$ to mean $f = O(g)$. We write $f = O_r(g)$ of the implicit constants depend on a parameter r. We write $f = \mathrm{poly}(g)$ to signify $|f| = |g|^{O(1)}$ and $f = \mathrm{poly}_r(g)$ to signify $|f| = |g|^{O_r(1)}$. For $n \in \mathbb{Z}_{>0}$ we denote $[n] = \{1, \ldots, n\}$. The expression $\log x$ denotes the natural logarithm of x and $\log_2 x$ denotes the base 2 logarithm. For a finite set X, we denote by $|X|$ its cardinality.

2.2 Number fields

Let K be a number field of degree d with signature (r_1, r_2) (i.e., there are r_1 real embeddings $K \to \mathbb{R}$, and $2r_2$ complex embeddings $K \to \mathbb{C}$). Let $\mathcal{O}_K$ be its ring of integers with discriminant Δ_K and denote by $\mathrm{Cl}(K)$ the ideal class group. Let h_K be the class number, R_K the regulator,

and w_K the number of roots of unity in K. Let $r_u = r_1 + r_2 - 1$ be the rank of the group of units $\mathcal{O}_K^\times$.

We fix a set of r_2 complex embeddings $\{\sigma_1, \dots \sigma_{r_2}\}$ such that the union of $\{\sigma_i, \overline{\sigma_i}\}$ exhausts all complex embeddings. We have that $K_\mathbb{R} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ and there is a natural embedding $K \to K_\mathbb{R}$, with the real components given by the r_1 real embeddings $x \mapsto \rho(x)$ and the complex components given by the r_2 embeddings $x \mapsto \sigma(x)$ fixed above. We call this map the Minkowski embedding.

There is a unique positive involution $a \mapsto a^*$ on $K_\mathbb{R}$ given by complex conjugation in each factor under the isomorphism with $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. The canonical metric on $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ is given by

$$\langle x, y\rangle_0 = \sum_\rho x_\rho y_\rho + \sum_\sigma 2\operatorname{Re}(x_\sigma \overline{y_\sigma}) = \operatorname{tr}_{K_\mathbb{R}/\mathbb{R}}(x \cdot y^*).$$

At the non-archimedean places, given by prime ideals $\mathfrak{p} \in \mathcal{O}_K$, we have the completions $K_\mathfrak{p}$ of K and $\mathcal{O}_\mathfrak{p}$ of $\mathcal{O}_K$. Let $\widehat{\mathcal{O}}_K = \prod_\mathfrak{p} \mathcal{O}_\mathfrak{p}$ denote the profinite completion of $\mathcal{O}_K$ and $\mathbb{A}_K = K_\mathbb{R} \times \prod'_\mathfrak{p} K_\mathfrak{p}$ the ring of adèles of K. We refer to [Neu99] for more details on these constructions.

2.3 Lattices

2.3.1 Euclidean $K_\mathbb{R}$-modules

A *Euclidean $K_\mathbb{R}$-module* of rank r is a pair $(V, \langle\cdot,\cdot\rangle)$ where V is a free $K_\mathbb{R}$-module of rank r and $\langle\cdot,\cdot\rangle\colon V \otimes_\mathbb{R} V \to \mathbb{R}$ is a positive definite inner product on the real vector space V such that

$$\langle ax, y\rangle = \langle x, a^* y\rangle \text{ for all } x, y \in V \text{ and } a \in K_\mathbb{R}.$$

Example 2.1. The module $V_0 = K_\mathbb{R}^r$ equipped with the standard inner product

$$\langle x, y\rangle_0 = \sum_{i=1}^r \operatorname{tr}_{K_\mathbb{R}/\mathbb{R}}(x_i y_i^*) = \sum_{i=1}^r \langle x_i, y_i\rangle_0$$

is a Euclidean $K_\mathbb{R}$-module of rank r. More generally, for $g \in \mathrm{GL}_r(K_\mathbb{R})$, the $K_\mathbb{R}$-module $V = K_\mathbb{R}^r$ equipped with $\langle x, y\rangle = \langle gx, gy\rangle_0$ is a Euclidean $K_\mathbb{R}$-module of rank r, and $g\colon V \to V_0$ is an isomorphism.

Any abstract Euclidean $K_\mathbb{R}$-module is isomorphic to the more concrete V_0. To see this, first let $(e_v)_v$ be the primitive idempotents of the $\mathbb{R}$-algebra $K_\mathbb{R}$ indexed by the infinite places v of K, meaning that $e_v K_\mathbb{R} \cong \mathbb{R}$ if v is a real place and $e_v K_\mathbb{R} \cong \mathbb{C}$ if v is a complex place. Note that $e_v^* = e_v$ for all v.

Now let V be a Euclidean $K_\mathbb{R}$-module of rank r. Then the e_v act as self-adjoint idempotents on V, i.e. they induce an orthogonal decomposition

$$V = \bigoplus e_v V$$

that commutes with the action of $K_\mathbb{R}$.

Let v be a real place of K. Then $e_v V$ is a real Euclidean space of dimension r, and therefore there exists an isomorphism $g_v\colon e_v V \to K_v^r \cong \mathbb{R}^r$ to the standard Euclidean space of dimension r.

Let v be a complex place of K, fix an isomorphism $K_v \cong \mathbb{C}$, and let W be the $\mathbb{C}$-vector space $e_v V$ of dimension r. For $x, y \in W$, define

$$H(x, y) = \langle x, y\rangle - i\langle ix, y\rangle \in \mathbb{C},$$

so that $\langle x, y\rangle = \operatorname{Re} H(x, y)$. Then the identity $\langle ax, y\rangle = \langle x, \bar{a} y\rangle$ for $x, y \in W$ and $a \in \mathbb{C}$ implies that H is a positive definite Hermitian form on W. Therefore, there exists an isomorphism $g_v\colon W \to \mathbb{C}^r$ to the standard Hermitian space of dimension r. In particular, we have

$$\langle x, y\rangle = \operatorname{Re} H(g_v x, g_v y)$$

for all $x, y \in e_v V$.

Putting all places together, there exists an isomorphism $g\colon V \to V_0$ of Euclidean $K_\mathbb{R}$-modules.

2.3.2 Module lattices

A *module lattice* of rank r is a pair $(M, \langle\cdot,\cdot\rangle)$ where M is a projective $\mathcal{O}_K$-module of rank r and $(M_{\mathbb{R}}, \langle\cdot,\cdot\rangle)$ is a Euclidean $K_{\mathbb{R}}$-module. We will often omit $\langle\cdot,\cdot\rangle$ from the notation.

Example 2.2. Let $M_0 \subset V_0$ be an $\mathcal{O}_K$-sub-module such that $M_0 \cdot \mathbb{R} = V_0$, i.e. that is also a lattice in V_0. Then $(M_0, \langle\cdot,\cdot\rangle_0)$ is a module lattice. We refer to those as *embedded* module lattices.

Let M be an arbitrary module lattice. By the previous section, there exists an isomorphism $g\colon M_{\mathbb{R}} \to V_0$ of Euclidean $K_{\mathbb{R}}$-modules. Since M is projective, the restriction of g to M is injective. In other words, $(M, \langle\cdot,\cdot\rangle)$ is isomorphic to an embedded module lattice.

Let $\lambda \in \mathbb{R}_{>0}$. A *similitude* $f\colon M_1 \to M_2$ of factor λ is an isomorphism of $\mathcal{O}_K$-modules that multiplies the inner product by λ. An *isomorphism of module lattices* is a similitude of factor 1, i.e. an isomorphism of $\mathcal{O}_K$-modules that preserves the inner product.

Let $X_r(K)$, also denoted X_r when K is clear from the context, be the space of similarity classes of modules lattices of rank r. We recall that any such module lattice is isomorphic as an $\mathcal{O}_K$-module to $\mathcal{O}_K^{r-1} \oplus \mathfrak{a}$ for an ideal $\mathfrak{a}$ in some fixed set of representatives of the ideal class group of K. Using the Minkowski embedding $\mathcal{O}_K \to K_{\mathbb{R}}$, this implies that we have an isomorphism

$$X_r(K) \cong \bigsqcup_{\mathfrak{a}\in \mathrm{Cl}(K)} \mathrm{GL}_r(\mathcal{O}_K, \mathfrak{a}) \backslash \mathrm{GL}_r(K_{\mathbb{R}}) / (\mathrm{U}_r(K_{\mathbb{R}}) \cdot \mathbb{R}_{>0}), \tag{2}$$

where $\mathrm{U}_r(K_{\mathbb{R}}) = \{g \in \mathrm{GL}_r(K_{\mathbb{R}}) \mid g(g^t)^* = \mathrm{id}\}$, the group $\mathbb{R}_{>0}$ is embedded via $\lambda \mapsto (1 \otimes \lambda)\,\mathrm{id} \in \mathrm{GL}_r(K_{\mathbb{R}})$, and $\mathrm{GL}_r(\mathcal{O}_K, \mathfrak{a}) = \mathrm{Aut}(\mathcal{O}_K^{r-1} \oplus \mathfrak{a})$. We write

$$X_{r,\mathfrak{a}} = \mathrm{GL}_r(\mathcal{O}_K, \mathfrak{a}) \backslash \mathrm{GL}_r(K_{\mathbb{R}}) / (\mathrm{U}_r(K_{\mathbb{R}}) \cdot \mathbb{R}_{>0}) \tag{3}$$

and we often use the notation $\Gamma_{\mathfrak{a}} = \mathrm{GL}_r(\mathcal{O}_K, \mathfrak{a})$, when r and K are understood from context. Note that we also have a map $X_r(K) \to X_n(\mathbb{Q})$ where $n = rd$, obtained by forgetting the structure of $\mathcal{O}_K$-module.

Choosing a representative $\mathfrak{a} \in \mathrm{Cl}(K)$ and a matrix $z \in \mathrm{GL}_r(K_{\mathbb{R}})$ we uniquely determine a class of module lattices, which we call $L_{z,\mathfrak{a}}$. By abuse of notation, we let $L_{z,\mathfrak{a}}$ denote the representative in this class given by

$$L_{z,\mathfrak{a}} = (\mathcal{O}_K^{r-1} \oplus \mathfrak{a}) \cdot z \subset K_{\mathbb{R}}^r,$$

viewing $\mathcal{O}_K \subset K_{\mathbb{R}}$ through the Minkowski embedding.

The Haar measure on $\mathrm{GL}_r(K_{\mathbb{R}})$ induces a measure μ on $X_r(K)$, whose total volume is finite. We normalize μ to be a probability measure and we often refer to it as the *uniform* measure. The measure μ gives a meaning to *random module lattices*, distributed according to μ, or with distribution given by a density function $f \in L^1(X_r)$ with respect to μ. For computations, however, we often work with a more explicit normalization of μ, namely μ_{Riem}, descending from $\mathrm{GL}_r(K_{\mathbb{R}})/(\mathrm{U}_r(K_{\mathbb{R}}) \cdot \mathbb{R}_{>0})$ and defined in Section 2.6.

In order to use representation theoretic arguments, it will often be easier to use the adélic version of the space of lattices. We can rewrite our union of double quotients as a single adélic double quotient as follows:

$$X_r(K) \cong \mathrm{GL}_r(K) \backslash \mathrm{GL}_r(\mathbb{A}_K) / (\mathrm{GL}_r(\widehat{\mathcal{O}}_K) \cdot \mathrm{U}_r(K_{\mathbb{R}}) \cdot \mathbb{R}_{>0}).$$

Let $\mathbb{X}_r = \mathbb{X}_r(K) = \mathrm{GL}_r(K) \backslash \mathrm{GL}_r(\mathbb{A}_K) / \mathbb{R}_{>0}$. We can therefore write

$$L^2(X_r) = L^2(\mathbb{X}_r)^{\mathrm{GL}_r(\widehat{\mathcal{O}}_K) \cdot \mathrm{U}_r(K_{\mathbb{R}})}$$

where $\mathrm{GL}_r(\mathbb{A}_K)$ acts on $L^2(\mathbb{X}_r)$ by $g \cdot f(x) = f(xg)$.

2.3.3 Representation and sizes of elements, ideals and modules

Assumptions. In this paper, we assume that $K = \mathbb{Q}[x]/f(x)$ is represented by a polynomial $f \in \mathbb{Z}[x]$ satisfying $\log \max |f_i| \leq \text{poly}(\log |\Delta_K|)$. Additionally, we assume that we have a $\mathbb{Z}$-basis of $\mathcal{O}_K$, written $(\beta_1, \ldots, \beta_d)$. Without loss of generality (by applying LLL and Lemma 2.12), we may assume that it satisfies $\max_i \|\beta_i\| \leq 2^d \cdot |\Delta_K|^{1/d}$.

Representations. We represent an element $\alpha \in K$ by its coordinates $(a_1, \ldots, a_d) \in \mathbb{Q}^d$ with respect to the $\mathbb{Z}$-basis $(\beta_1, \ldots, \beta_d)$. This means that $\alpha = \sum_{i=1}^d a_i \beta_i$. A (fractional) ideal $\mathfrak{a}$ of $\mathcal{O}_K$ can be represented by a generating matrix $B_\mathfrak{a} = (\alpha_1, \ldots, \alpha_d) \in K^d$, for which we have that $\mathfrak{a}$ is generated by these α_i as a $\mathbb{Z}$-module. Each of these generators α_i is then represented by $(a_1^{(i)}, \ldots, a_d^{(i)}) \in \mathbb{Q}^d$ and hence $B_\mathfrak{a}$ can be written as a matrix in $\mathbb{Q}^{d\times d}$. In this paper, we choose to have a unique representation for an ideal by always demanding that $B_\mathfrak{a}$ (as a matrix in $\mathbb{Q}^{d\times d}$) is in Hermite normal form. That is, we write the generating matrix of $\mathfrak{a}$ as $\frac{1}{m} \cdot (m \cdot B_\mathfrak{a})$, where $m \in \mathbb{Z}_{>0}$ and $m \cdot B_\mathfrak{a} \in \mathbb{Z}^{d\times d}$ is in Hermite normal form.

A rank r module lattice M is represented by its *pseudo-basis* (see, for example, [Coh99]), which consists of a matrix $\mathbf{A} \in K^{r\times r}$ (with columns $\mathbf{A}_i \in K^r$) and a sequence of r ideals $\mathbf{I} := (\mathfrak{a}_1, \ldots, \mathfrak{a}_r)$. Again, each of the $\mathbf{A}_{ij} \in K$ can be represented by a sequence in $\mathbb{Q}^d$, and each of the ideals of $\mathbf{I}$ can be represented by its generating matrix. The module lattice is then defined by the rule

$$M = \left\{ \sum_{i=1}^r \mathbf{A}_i \cdot \alpha_i \in K^r \mid \alpha_i \in \mathfrak{a}_i \right\}.$$

Sizes of elements, ideals and modules. For $n \in \mathbb{Z}$, we define $\text{size}(n) = 1 + \lceil \log_2(|n|) \rceil$ (where the extra 1 is for encoding the sign). For $q = \frac{a}{b} \in \mathbb{Q}$ with $a, b \in \mathbb{Z}$ coprime, we set $\text{size}(q) = \text{size}(a) + \text{size}(b)$. For $\alpha \in K$ represented by $(a_1, \ldots, a_d) \in \mathbb{Q}^d$ we put $\text{size}(\alpha) = \sum_{i=1}^d \text{size}(a_i)$. For an ideal $\mathfrak{a}$ of K, we define $\text{size}(\mathfrak{a}) := \text{size}(mB_\mathfrak{a}) + \text{size}(m)$, where the generating matrix equals $\frac{1}{m} \cdot (mB_\mathfrak{a})$ and $(mB_\mathfrak{a}) \in \mathbb{Z}^{d\times d}$ is in Hermite normal form.

For a rank r module lattice M with pseudo basis $(\mathbf{A}, \mathbf{I})$ with $\mathbf{A} \in K^{r\times r}$ and $\mathbf{I} = (\mathfrak{a}_1, \ldots, \mathfrak{a}_r)$ we put

$$\text{size}(M) := \sum_{i,j=1}^r \text{size}(\mathbf{A}_{ij}) + \sum_{i=1}^r \text{size}(\mathfrak{a}_i).$$

Rules for sizes. For the $\mathbb{Z}$-basis $(\beta_1, \ldots, \beta_d)$ of $\mathcal{O}_K$, we surely have, by Cauchy-Schwarz, $\|\beta_i\beta_j\| \leq \left(\sum_\sigma |\sigma(\beta_i)|^2 |\sigma(\beta_j)|^2\right)^{1/2} \leq \sum_\sigma |\sigma(\beta_i)||\sigma(\beta_j)| \leq \|\beta_i\|\|\beta_j\| \leq 2^{2d} \cdot |\Delta_K|^{2/d}$ per assumption. Additionally, we can deduce that, writing $B = (\sigma(\beta_j))_{\sigma,j}$ as a basis in the Minkowski space $K_\mathbb{R}^{d\times d}$, and using Lemma A.1 and the fact that $\lambda_1(\mathcal{O}_K) = \sqrt{d}$,

$$\|B^{-1}\| \leq \sqrt{d} \prod_i \|\beta_i\| \leq \sqrt{d} \cdot 2^{d^2} \cdot |\Delta_K|.$$

Hence, $\|B^{-1}(\beta_i \cdot \beta_j)\| \leq \|B^{-1}\|\|\beta_i \cdot \beta_j\| \leq \sqrt{d} \cdot 2^{d^2+2d} \cdot |\Delta_K|^{1+2/d}$. So, the co-ordinates of the product $\beta_i\beta_j$ in terms of the basis $(\beta_1, \ldots, \beta_d)$ are bounded by $\sqrt{d} \cdot 2^{d^2+2d} \cdot |\Delta_K|^{1+2/d}$.

Lemma 2.3 (Rules on sizes of elements)**.** *For fractional $\mathcal{O}_K$ ideals $\mathfrak{a}, \mathfrak{a}_i$ of K, we have* $\text{size}(\mathfrak{a}) \leq d^2 \,\text{size}(N(\mathfrak{a})) \ll d^2 \log N(\mathfrak{a})$ *and* $\text{size}(\prod_{i=1}^k \mathfrak{a}_i) \leq d^2 \sum_{i=1}^k \text{size}(\mathfrak{a}_i)$.

Proof. See Section A.5 in the Appendix. □

Sizes and Module-HNF In this paper, we will make use of a Hermite-normal form algorithm that works over module-lattices, and thus applies basis operations that are compatible with the module structure [Coh99, Section 1.4]. Computing this Hermite-normal form of a given pseudo-basis of a module lattice can be done within polynomial time of the input size [BF12]. This Hermite-normal form can be made unique (i.e., not depending on the specific pseudo-basis given) with no significant overhead [Coh99, Theorem 1.4.11].

Due to the polynomial time algorithm of [BF12] it must surely be true that the output $(\mathbf{H}, (\mathfrak{h}_i)_{i\in[r]})$ of the module Hermite Normal Form algorithm must have size polynomially bounded in the size of the input module lattice $(\mathbf{B}, (\mathfrak{a}_i)_{i\in[r]})$, i.e.,

$$\text{size}(H, (\mathfrak{h}_i)_{i\in[r]}) \leq \text{poly}(\text{size}(\mathbf{B}, \mathfrak{a}_i)_{i\in[r]})).$$

2.3.4 Sublattices

We record the following standard definition and refer to [FPS22, App. B.2] for a proof of the equivalences.

Definition 2.4. Let M be a $\mathcal{O}_K$-module. A sub-module $N \subseteq M$ is said to be *primitive* if it satisfies any of the following equivalent conditions:

- The module N is maximal for the inclusion relation in the set of submodules of M of rank at most $\text{rank}(N)$.
- There is a module N' with $M = N + N'$ and $\text{rank}(M) = \text{rank}(N) + \text{rank}(N')$.
- There is a module N' with $M = N \oplus N'$.
- We have $N = M \cap \text{span}_K(N)$.

Algorithm 1 Computing a random sub-module M' of M such that $M/M' \simeq \mathcal{O}_K/\mathfrak{p}$

Require:

- A pseudos $(\mathbf{B}, \mathbf{I})$ of a rank r module lattice M, with $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_r) \in K^{r\times r}$ and $\mathbf{I} = (\mathfrak{a}_1, \ldots, \mathfrak{a}_r)$.
- A prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$,

Ensure: A pseudo-basis $(\mathbf{B}', \mathbf{I}')$ of a module M' that satisfies $M/M' \simeq \mathcal{O}_K/\mathfrak{p}$.

1: Draw a random integer u from $\{1, \ldots, \sum_{i=0}^{r-1} q^i\}$, with $q = N(\mathfrak{p})$ and pick the smallest $j \geq 1$ such that $\sum_{i=0}^{j-1} q^i \geq u$.
2: Put $\mathbf{I}' = (\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{p}\mathfrak{a}_j, \ldots, \mathfrak{a}_r)$. I.e., multiply the j-th ideal in $\mathbf{I}$ by $\mathfrak{p}$ to obtain $\mathbf{I}'$.
3: Put, for all $i < j$, $\mathbf{b}'_i = \mathbf{b}_i + \gamma_i \mathbf{b}_j$ where γ_i is uniformly drawn from a set of representatives of $\mathfrak{a}_i/\mathfrak{p}\mathfrak{a}_i$, and put $\mathbf{b}'_i = \mathbf{b}_i$ for $i \geq j$. Assemble $\mathbf{b}'_i$ into a matrix $\mathbf{B}'$. Equivalently, we put $\mathbf{B}' = \mathbf{B} \cdot T$ where $T = I + \sum_{i<j} \gamma_i \mathbf{e}_{ji}$ where $\mathbf{e}_{ji}$ is the matrix with a one on place ji and zeroes elsewhere.
4: **return** $(\mathbf{B}', \mathbf{I}')$.

Algorithm for taking a random index $N(\mathfrak{p})$ sub-module lattice

Lemma 2.5. *Algorithm 1 is correct, outputs a uniformly random sub-module $M' \subseteq M$ satisfying $M/M' \simeq \mathcal{O}_K/\mathfrak{p}$ and runs in time polynomial in the input size.*

Proof. (Correctness) We have that $M' \subseteq M$ since any element of M' can be written as (with $\alpha_i \in \mathfrak{a}_i$ for $i \neq j$ and $\alpha_j \in \mathfrak{p}\mathfrak{a}_j \subseteq \mathfrak{a}_j$)

$$\sum_{i=1}^{r} \alpha_i \mathbf{b}'_i = \sum_{i=1}^{r} \alpha_i(\mathbf{b}_i + \gamma_j \mathbf{b}_j) = \sum_{i=1, i\neq j}^{r} \alpha_i \mathbf{b}_i + (1 + \sum_{i=1}^{j-1} \gamma_i)\mathbf{b}_j \in M,$$

since $\gamma_i \in \mathfrak{a}_i$ for all $i < j$. Additionally, a set of representatives of M/M' can be given by $\{\gamma_j \mathbf{b}_j\} \subseteq M'$ with γ_j from a set of representatives of $\mathfrak{a}_j/\mathfrak{p}\mathfrak{a}_j$. Hence $M/M' \simeq \mathfrak{a}_j/\mathfrak{p}\mathfrak{a}_j \simeq \mathcal{O}_K/\mathfrak{p}$.

(Uniformly random sub-module) The number of submodules $M' \subseteq M$ satisfying $M/M' \simeq \mathcal{O}_K/\mathfrak{p}$ corresponds with the number of hyper planes in $M/\mathfrak{p}M$, which equals (by the q-binomial theorem) $\binom{r}{1}_q = \sum_{i=0}^{r-1} q^i$. One can readily verify that the number of M' that Algorithm 1 outputs is indeed $\sum_{i=0}^{r-1} q^i$, and that the way that they are all picked with equal probability.

(Polynomial time) Each of the operations can be reasonably seen to be able to be computed in time polynomial in the input size. We spend some extra words on line 3, where a random representative of $\mathfrak{a}_i/\mathfrak{p}\mathfrak{a}_i$ needs to be chosen. This can be done by computing the Hermite normal form of both $\mathfrak{a}_i$ and $\mathfrak{p}\mathfrak{a}_i$ (after scaling up), take random elements in the finite quotient group (of these two lattices) of order $N(\mathfrak{p}) = q$ (seen as a subgroup of $\mathbb{Z}^d$ with $d = [K : \mathbb{Q}]$) and lift the elements to $\mathfrak{a}_i$. □

2.3.5 Successive minima

It is useful for us to work with two different notions of successive minima, corresponding to linear independence with respect to $\mathbb{Q}$ and, respectively, K.

Definition 2.6. For a $\mathcal{O}_K$-module lattice M of rank r we put

$$\lambda_j(M) = \min\{\lambda \in \mathbb{R}_{>0} \mid \dim_{\mathbb{Q}} \operatorname{span}_{\mathbb{Q}}(B_\lambda \cap M) \geq j\},$$

for $j = 1, \ldots, rd$, where B_λ is the ball of radius λ with respect to the norm on M. In other words, $\lambda_j(M)$ is the minimal λ such that there exist j vectors in M of length at most λ that are $\mathbb{Q}$-linearly independent.

Definition 2.7. For a $\mathcal{O}_K$-module lattice M of rank r we put

$$\lambda_j^K(M) = \min\{\lambda \in \mathbb{R}_{>0} \mid \dim_K \operatorname{span}_K(B_\lambda \cap M) \geq j\},$$

for $j = 1, \ldots, r$, where B_λ is the ball of radius λ with respect to the norm on M. We often call these quantities K-minima.

Definition 2.8. A $\mathcal{O}_K$-module lattice M with K-minima $\lambda_1^K, \ldots, \lambda_r^K$ is α-*balanced* if $\lambda_{i+1}^K/\lambda_i^K \leq \alpha$ for all $1 \leq i < r$.

When comparing the two types of successive minima, we also require the sup-norm successive minima of the underlying ring of integers.

Definition 2.9. Consider $\mathcal{O}_K$ as a $\mathbb{Z}$-lattice through the Minkowski embedding. Define

$$\lambda_j^\infty(\mathcal{O}_K) = \min\{\lambda \in \mathbb{R}_{>0} \mid \dim_{\mathbb{Q}} \operatorname{span}_{\mathbb{Q}}(B_\lambda^\infty \cap \mathcal{O}_K) = j\},$$

for $j = 1, \ldots, r$, where B_λ^∞ is the ball of radius λ with respect to the sup-norm on $K_{\mathbb{R}}$.

The reason for using the sup-norm is the following bound.

Lemma 2.10. *Let L be a module lattice, $x \in L$ and $a \in K_{\mathbb{R}}$. Then*

$$\|ax\| \leq \|a\|_\infty \cdot \|x\|.$$

Proof. Embed L in $K_{\mathbb{R}}^r$. Then the action of $a \in K_{\mathbb{R}}$ is component-wise. □

The successive minima of the ring of integers $\mathcal{O}_K$ can be estimated.

Definition 2.11. Let $\Gamma_K = \sup_L \lambda_d(L)/\lambda_1(L)$, where L ranges over all ideal lattices in K.

Lemma 2.12 ([BPW25, Lemma 2.13])**.** *For any $\mathcal{O}_K$-module lattice L of rank 1, we have:*

(i) $\lambda_d(\mathcal{O}_K)/\sqrt{d} \le \Gamma_K \le \lambda_d^\infty(\mathcal{O}_K) \le |\Delta_K|^{1/d}$.

(ii) If K is a cyclotomic field, then $\Gamma_K = 1$.

(iii) $\lambda_d(L) \le \sqrt{d} \cdot \Gamma_K \cdot \det(L)^{1/d}$.

(iv) $\lambda_1(L) \ge \sqrt{\frac{d}{|\Delta_K|^{1/d}}} \cdot \det(L)^{1/d}$.

The relation between the two types of successive minima is given in the following result.

Lemma 2.13. *For any $1 \le j \le rd$, we have*

$$\lambda^K_{\lceil j/d \rceil}(L) \le \lambda_j(L) \le \Gamma_K \lambda^K_{\lceil j/d \rceil}(L).$$

Proof. Fix (k, i). Let $\lambda = \lambda_{d(k-1)+i}(L)$ and S the set of vectors in L of length at most λ. By definition $\dim_{\mathbb{Q}} \operatorname{span}_{\mathbb{Q}}(S) \ge d(k-1)+i$. But then $\dim_K \operatorname{span}_K(S) \ge \frac{d(k-1)+i}{d} > k-1$ and therefore $\dim_K \operatorname{span}_K(S) \ge k$, so that $\lambda^K_k(L) \le \lambda$: this proves the first inequality.

Let $(u_i)_{i=1}^k$ be K-linearly independent vectors in L of length at most $\lambda^K_k(L)$. For each i, let $(v_{ij})_{j=1}^d$ be $\mathbb{Q}$-linearly independent vectors in $\mathcal{O}_K u_i$ of length at most

$$\lambda_d(\mathcal{O}_K u_i) \le \Gamma_K \lambda_1(\mathcal{O}_K u_i) \le \Gamma_K \lambda^K_k(L).$$

The family $(v_{ij})_{i,j}$ contains dk many $\mathbb{Q}$-linearly independent vectors of length at most $\Gamma_K \lambda^K_k(L)$, hence $\lambda_{d(k-1)+i}(L) \le \lambda_{dk}(L) \le \Gamma_K \lambda^K_k(L)$. □

The n-th successive minima of α-balanced lattices can be bounded by a power of α multiplied by the root determinant of that lattice.

Lemma 2.14. *Let M be an α-balanced $\mathcal{O}_K$-module lattice of rank r. Then*

$$\lambda_{rd}(M) \le \Gamma_K \cdot \sqrt{rd} \cdot \alpha^{r-1} \cdot \det(M)^{1/(rd)}.$$

Proof. We use Minkowski's second theorem [Cas97, Chap. VIII, Thm. 5] and Lemma 2.13, we write $\lambda_j = \lambda_j(M)$ and $n = rd$, to obtain

$$\frac{\det(M)^{1/n}}{\lambda_n} \ge \frac{\sqrt{\pi}}{2 \cdot \Gamma(\frac{n}{2}+1)^{1/n}} \left(\prod_{j=1}^n \frac{\lambda_j}{\lambda_n} \right)^{1/n} \ge \sqrt{e\pi/(4n)} \left(\prod_{j=1}^{rd} \frac{\lambda^K_{\lceil j/d \rceil}}{\Gamma_K \lambda^K_r} \right)^{1/(rd)}$$

$$\ge \sqrt{e\pi/(4n)} \left(\prod_{j=1}^{r} \frac{(\lambda^K_j)^d}{\Gamma_K^d (\lambda^K_r)^d} \right)^{1/(rd)} = \sqrt{e\pi/(4n)} \cdot \frac{1}{\Gamma_K} \cdot \left(\prod_{j=1}^{r} \frac{\lambda^K_j}{\lambda^K_r} \right)^{1/r}$$

$$\ge \sqrt{e\pi/(4n)} \cdot \frac{1}{\Gamma_K} \cdot \left(\prod_{j=1}^{r} \alpha^{-(j-1)} \right)^{1/r} = \sqrt{e\pi/(4n)} \cdot \frac{\alpha^{-(r-1)}}{\Gamma_K}$$

Rewriting and using that $4/(e\pi) < 1$ yields the result. □

We will also use the following simple bound on the balancedness of submodules.

Lemma 2.15. *Let M be an α-balanced rank r module lattice and let $M' \subseteq M$ be an index q sub-module lattice. Then M' is $\alpha \cdot q$-balanced.*

Proof. Suppose, to derive a contradiction, that M' is *not* $\alpha \cdot q$-balanced, i.e., $\frac{\lambda_{i+1}^K(M')}{\lambda_i^K(M')} > \alpha \cdot q$ for some $i \in \{1, \ldots, r-1\}$. Write j for the smallest i satisfying this imbalancedness property.

Write $v_1', \ldots, v_j' \in M'$ for the vectors in M' attaining $\lambda_1^K(M'), \ldots, \lambda_j^K(M')$ and $v_1, \ldots, v_j, v_{j+1}$ for the vectors in M attaining $\lambda_1^K(M), \ldots, \lambda_j^K(M), \lambda_{j+1}^K(M)$.

By definition there exists a $k \in \{1, \ldots, j+1\}$ so that $v_k \notin v_1'\mathcal{O}_K + \ldots + v_j'\mathcal{O}_K$ (which is the module lattice generated by $v_1', \ldots, v_j'$). We claim that $a \cdot v_k + M'$ for $a \in \{0, \ldots, q\}$ are all different cosets in M. Indeed, if two cosets were the same, we would have that $a \cdot v_k \in M'$ for some $a \in \{0, \ldots, q\}$, and hence

$$\lambda_{j+1}^K(M') \leq \|a \cdot v_k\| \leq q \cdot \lambda_k^K(M) \leq q \cdot \lambda_{j+1}^K(M).$$

But then

$$\frac{\lambda_{j+1}^K(M')}{\lambda_j^K(M')} \leq \frac{q \cdot \lambda_{j+1}^K(M)}{\lambda_j^K(M')} \leq \frac{q \cdot \lambda_{j+1}^K(M)}{\lambda_j^K(M)} \leq \alpha \cdot q,$$

which leads to a contradiction.

Hence, indeed, $a \cdot v_k + M'$ for $a \in \{0, \ldots, q\}$ are all different cosets in M, and count to $q+1$. But $|M/M'| = q$, which in turn is a contradiction. Hence, M' must be $\alpha \cdot q$-balanced. □

2.4 Probability

2.4.1 Probability distributions

Definition 2.16. For an n-dimensional Euclidean vector space V and $\mathbf{x} \in V$, we write $\rho_\sigma(\mathbf{x}) := \exp(-\pi\|\mathbf{x}\|^2/\sigma^2)$ for the Gaussian function.

Lemma 2.17 (Gaussian weight lemma)**.** *Let Λ be an n-dimensional full-rank lattice in an n-dimensional Euclidean vector space, let $\mathbf{c} \in$ span(Λ) and $\sigma \geq \sqrt{\frac{\log(2n(1+1/\varepsilon))}{\pi}} \cdot \lambda_n(\Lambda)$ for some $\varepsilon > 0$. Then we have*

$$\sum_{\ell \in \Lambda} \rho_\sigma(\ell + \mathbf{c}) = \rho_\sigma(\Lambda + \mathbf{c}) \in [1-\varepsilon, 1+\varepsilon] \cdot \frac{\sigma^n}{\det(\Lambda)}.$$

Proof. This is a combination of the bound on the smoothing parameter [MR07, Lemma 3.3] and the proof of [MR07, Lemma 4.4]. □

Definition 2.18 (Gaussian distribution)**.** Let V be a Euclidean vector space. For $\sigma \in \mathbb{R}_{>0}$, we denote $\mathcal{G}_{V,\sigma}(x) := \sigma^{-n} \cdot e^{-\pi\|x\|^2/\sigma^2} = \sigma^{-n} \cdot \rho_\sigma(x)$ for the Gaussian distribution over V, where $n = \dim(V)$ and where $\|\cdot\|$ is the length notion over V.

Definition 2.19 (Discrete Gaussian distribution)**.** Let $\Lambda \subseteq V$ be a full-rank lattice in a Euclidean vector space. For $\sigma \in \mathbb{R}_{>0}$, we define the discrete Gaussian over Λ with center $c \in V$ by the rule

$$\mathcal{G}_{\Lambda,\sigma,c}(\ell) := \frac{\mathcal{G}_{V,\sigma}(\ell + c)}{\mathcal{G}_{V,\sigma}(\Lambda + c)} = \frac{\rho_\sigma(\ell + c)}{\rho_\sigma(\Lambda + c)}, \quad \text{for } \ell \in \Lambda,$$

where $\mathcal{G}_{V,\sigma}(\Lambda + c) := \sum_{\ell \in \Lambda} \mathcal{G}_{V,\sigma}(\ell + c)$. In the case that $c = 0$, the center c is omitted in the notation.

Lemma 2.20. *Let $\Lambda \subseteq V$ be a full-rank lattice in a Euclidean vector space. For $\sigma \geq \sqrt{\frac{\log(8n)}{\pi}} \cdot \lambda_n(\Lambda)$ and $\kappa \geq 1/(2\pi)$, we have*

$$\mathop{\mathbb{P}}_{v \leftarrow \mathcal{G}_{\Lambda,\sigma,c}} [\|v - c\| > \sqrt{n} \cdot \kappa \cdot \sigma] \leq 4(\kappa\sqrt{2\pi e})^n \cdot e^{-\pi\kappa^2 n}$$

Proof. We have

$$\begin{aligned}\mathop{\mathbb{P}}_{v\leftarrow\mathcal{G}_{\Lambda,\sigma,c}}[\|v-c\|>\sqrt{n}\cdot\kappa\cdot\sigma] &= \frac{\rho_\sigma((\Lambda+c)\backslash\sqrt{n}\cdot\kappa\cdot\sigma\cdot B_2)}{\rho_\sigma(\Lambda+c)} \leq 2C^n\frac{\rho_\sigma(\Lambda+c)}{\rho_\sigma(\Lambda)}\\ &\leq 2\cdot\frac{1+1/3}{1-1/3}\cdot C^n \leq 4C^n \leq 4(\kappa\sqrt{2\pi e})^n e^{-\pi\kappa^2 n},\end{aligned}$$

where the first inequality follows from [MR07, Lemma 2.10] and the second inequality follows from Lemma 2.17 (with $\varepsilon = 1/3$). Here $C = \kappa\sqrt{2\pi e}\cdot e^{-\pi\kappa^2}$. This yields the claim. □

2.4.2 Statistical distance and the data processing inequality

Definition 2.21 (Statistical distance)**.** Let $(\Omega,\mathcal{S})$ be a measurable space with probability measures P,Q. The statistical distance between P and Q is defined by the rule

$$SD(P,Q) = \sup_{X\in\mathcal{S}}|P(X)-Q(X)|.$$

In the present work we only consider discrete or continuous domains Ω. For a discrete space Ω, we have

$$SD(P,Q) = \frac{1}{2}\sum_{x\in\Omega}|P(x)-Q(x)| =: \frac{1}{2}\|P-Q\|_1.$$

For a continuous space Ω with probability densities P,Q, we have

$$SD(P,Q) = \frac{1}{2}\int_{x\in\Omega}|P(x)-Q(x)| =: \frac{1}{2}\|P-Q\|_1.$$

Often, in this work, due to the equivalence of these notions (up to a constant $\frac{1}{2}$) we will describe closeness of probability distributions in terms of the distance notion $\|\cdot\|_1$, instead of $SD(\cdot,\cdot)$.

The data processing inequality captures the idea that an algorithm (by just processing a single query) cannot increase the statistical distance between two probability distributions. A proof can be found in, for example, [CT06, §2.8].

Proposition 2.22 (Data processing inequality)**.** *Let $(\Omega,\mathcal{S})$ be a measurable space with probability measures P,Q. Let f be a (potentially probabilistic) function on Ω. Then*

$$\|f(P)-f(Q)\|_1 \leq \|P-Q\|_1.$$

Statistical distance is well compatible with conditional events. If two distributions are close, the conditional counterparts are also close, where the statistical distance is multiplied by the probability of the conditioned event happening.

Lemma 2.23. *Let $(\Omega,\mathcal{S})$ be a measurable space with probability measures P,Q. Let $U\in\mathcal{S}$ be an event with non-zero weight for both P and Q. Then*

$$SD(P|_U,Q|_U) \leq 2\cdot P(U)^{-1}\,SD(P,Q),$$

where $P|_U, Q|_U$ denotes P respectively Q conditioned on the event U.

Proof. We have, by the law of conditional probability, writing $p = P(U)$ and $q = Q(U)$,

$$\begin{aligned}SD(P|_U,Q|_U) &= \sup_{X\in\mathcal{S}}\left|\frac{P(X\cap U)}{p}-\frac{Q(X\cap U)}{q}\right|,\\ &= \frac{1}{p}\sup_{X\in\mathcal{S}}\left|P(X\cap U)-\frac{p}{q}\cdot Q(X\cap U)\right|\\ &\leq \frac{1}{p}\sup_{X\in\mathcal{S}}\left(|P(X\cap U)-Q(X\cap U)|+|1-\frac{p}{q}|\cdot Q(X\cap U)\right)\\ &\leq \frac{1}{p}\sup_{X\in\mathcal{S}}|P(X\cap U)-Q(X\cap U)|+\frac{q-p}{p} \leq \frac{2}{p}\cdot SD(P,Q).\end{aligned}$$

□

2.5 Computational problems

We consider the following three types of "shortest vector problems" in lattices.

Problem 2.24 (Shortest Vector Problem (SVP_γ))**.** *Given as input a basis* $\mathbf{B}$ *of a lattice* L *and a* $\gamma \in \mathbb{R}_{\geq 1}$*, the* γ-shortest vector problem *is the computational task of finding a non-zero lattice vector* $x \in L$ *that satisfies* $\|x\| \leq \gamma \cdot \lambda_1(L)$*.*

Problem 2.25 (Shortest Independent Vector Problem (SIVP_γ))**.** *Given as input a basis* $\mathbf{B}$ *of an* n*-dimensional lattice* L *and a* $\gamma \in \mathbb{R}_{\geq 1}$*, the* γ-shortest independent vector problem *is the computational task of finding* $\mathbb{R}$*-linearly independent lattice vectors* $x_1, \dots, x_n \in L$ *that satisfy* $\|x_i\| \leq \gamma \cdot \lambda_n(L)$ *for all* $i \in \{1, \dots, n\}$*.*

The parameter γ in the definitions above is called *approximation factor* and is generally written as a function in the dimension n of the lattice. No known polynomial time algorithm can solve these problems for $\gamma = \mathrm{poly}(n)$. However, they are easy for $\gamma = 2^{O(n)}$: by [LLL82, Proposition 1.12], the LLL algorithm finds a basis (x_i) of L such that $\|x_i\| \leq 2^{(n-1)/2}\lambda_i(L)$ for any i.

2.6 Riemannian geometry, the determinant map, volumes

The space of lattices $X_r(K)$ comes equipped with an invariant probability measure. For computing with this measure, it is useful to work with an explicit realization coming from a Riemannian metric. The latter generalizes the canonical metric for Minkowski space and allows us to compute the volumes of different spaces that show up while proving the Hecke equidistribution theorem. We also consider in this section a way of "splitting" $\mathrm{GL}(r)$ into $\mathrm{SL}(r)$ and $\mathrm{GL}(1)$, as announced in Section 1.3.1.

2.6.1 Riemannian structure

We introduce a Riemannian metric on $\mathrm{GL}_r(K_\mathbb{R})$ and its quotients. For this, we equip the Lie algebra $M_r(K_\mathbb{R})$ of $\mathrm{GL}_r(K_\mathbb{R})$ with the positive definite inner product

$$(x, y) \mapsto \mathrm{tr}_{K_\mathbb{R}/\mathbb{R}}\,\mathrm{tr}({}^t x^* y).$$

This gives $\mathrm{GL}_r(K_\mathbb{R})$ the structure of a Riemannian manifold with a metric that is left-invariant by arbitrary elements and right-invariant by $\mathrm{U}_r(K_\mathbb{R}) \cdot \mathbb{R}_{>0}$. In particular, it defines a volume form μ_{Riem} on $\mathrm{GL}_r(K_\mathbb{R})$ that is a Haar measure and we note that $\mathrm{GL}_r(K_\mathbb{R})$ is unimodular. This also induces a Riemannian metric and measure on the quotient

$$Y_r = \mathrm{GL}_r(K_\mathbb{R}) / \mathrm{U}_r(K_\mathbb{R}) \cdot \mathbb{R}_{>0}. \tag{4}$$

The measure μ_{Riem} further descends to $X_{r,\mathfrak{a}} = \Gamma_\mathfrak{a} \backslash Y_r$ and $X_r(K)$. The probability measure μ on $X_r(K)$ is then equal to $\mu_{\mathrm{Riem}}(X_r(K))^{-1}\mu_{\mathrm{Riem}}$. Throughout this section and much of Section 4, we endow all spaces with the corresponding Riemannian measures and this defines all norms and inner products where the dependence on the space is given as a subscript. Unless specified otherwise, this is the measure implicit in the notation $L^2(X_r)$ and the other L^2-spaces.

The map

$$K_\mathbb{R}^\times / \mathrm{U}_1(K_\mathbb{R}) \to \mathbb{R}^{r_1+r_2}$$

given by $g = (g_v)_v \mapsto \log|\det(g)| = (\log|\det g_v|)_v$ is an isometry of Riemannian manifolds, where for $x = (x_i)_i \in \mathbb{R}^{r_1+r_2}$ we define

$$\|x\|^2 = \sum_{i=1}^{r_1} x_i^2 + 2\sum_{i=r_1+1}^{r_2} x_i^2.$$

Let $H \subset \mathbb{R}^{r_1+r_2}$ be orthogonal to $(1, \dots, 1)$, so that the logarithmic embedding of units lies in H. Let $\pi_H \colon \mathbb{R}^{r_1+r_2} \to H$ denote the orthogonal projection onto H. We obtain an isometry $Y_1 \to H$ given by $g \mapsto \pi_H(\log|\det g|)$.

2.6.2 The determinant map

Let $\Delta\colon Y_r \to Y_1$ be the map induced by the determinant $\mathrm{GL}_r(K_\mathbb{R}) \to K_\mathbb{R}^\times$. For an ideal $\mathfrak{a} \subset \mathcal{O}_K$, this restricts to a map

$$\Delta_\mathfrak{a}\colon X_{r,\mathfrak{a}} \to X_{1,\mathfrak{a}}.$$

Pulling back functions, we obtain an injective map

$$\Delta_\mathfrak{a}^*\colon L^2(X_{1,\mathfrak{a}}) \to L^2(X_{r,\mathfrak{a}})$$

defined by $(\Delta_\mathfrak{a}^* f)(x) = f(\Delta_\mathfrak{a} x)$. We denote the image of the pull-back by

$$L^2_{\mathrm{det}}(X_{r,\mathfrak{a}}) = \Delta_\mathfrak{a}^*(L^2(X_{1,\mathfrak{a}})) \subset L^2(X_{r,\mathfrak{a}}),$$

and, putting all connected components together,

$$L^2_{\mathrm{det}}(X_r) = \bigoplus_{\mathfrak{a}\in \mathrm{Cl}(K)} L^2_{\mathrm{det}}(X_{r,\mathfrak{a}}) = \Delta^*(L^2(X_1)) \subset L^2(X_r).$$

Lemma 2.26. *For non-negative measurable functions $f\colon Y_r \to \mathbb{R}_{\geq 0}$, we have the integration formula*

$$\int_{y\in Y_r} f(y)dy = \frac{1}{r^{r_u/2}} \int_{\delta\in Y_1} \left(\int_{y\in\Delta^{-1}(\delta)} f(y)dy \right) d\delta, \tag{5}$$

and an analogous formula for $X_{r,\mathfrak{a}}$. Integration on the fibers of Δ is done with respect to the restriction of the Riemannian metric.

Proof. At the level of the Lie algebra, notice that the complement of the kernel of the derivative D_Δ of Δ consists of the scalar matrices. Locally, at one place v, the vector $X = \mathrm{diag}(1,\dots,1)$ has length $\sqrt{r}$ in the Riemannian metric. Since $\det(\exp(\lambda X)) = \exp(r\lambda)$, we see that $D_\Delta(X) = r\cdot 1$, where 1 is the unit vector in the Lie algebra of $\mathbb{R}^\times$ or $\mathbb{C}^\times$. These computations now show that the Jacobian of Δ is $\sqrt{r}^{r_u}$. Put another way, Δ is a Riemannian submersion when the metric on Y_1 is scaled by $\frac{1}{\sqrt{r}}$. The statement now follows from the coarea formula (see [Nic11, Thm. 2.1]) applied to Δ. □

It is convenient to have an explicit form of the fibers of Δ. Let $g \in \mathrm{GL}_r(K_\mathbb{R})$ and $\delta = \Delta(g)$. We have

$$\Delta^{-1}(\delta) = \left(\mathrm{SL}_r(K_\mathbb{R})\cdot\mathbb{R}_{>0}/(g\,\mathrm{SU}_r(K_\mathbb{R})g^{-1})\cdot\mathbb{R}_{>0}\right) g \tag{6}$$

and the analogous formula

$$\Delta_\mathfrak{a}^{-1}(\delta) = \left(\Gamma_\mathfrak{a}\backslash\Gamma_\mathfrak{a}\cdot\mathrm{SL}_r(K_\mathbb{R})\cdot\mathbb{R}_{>0}/(g\,\mathrm{SU}_r(K_\mathbb{R})g^{-1})\cdot\mathbb{R}_{>0}\right) g.$$

We shall often encounter the volume of these fibers in computations.

Lemma 2.27. *The volume $\mu_{\mathrm{Riem}}(\Delta_\mathfrak{a}^{-1}(\delta))$ is equal to $\mu_{\mathrm{Riem}}(\Delta_\mathfrak{a}^{-1}(1))$ and is therefore independent of δ.*

Proof. Define $\Gamma^1_\mathfrak{a} = \mathrm{SL}_r(\mathcal{O}_K,\mathfrak{a})$ and notice that a fundamental domain for the left action of $\Gamma^1_\mathfrak{a}$ on $\mathrm{SL}_r(K_\mathbb{R})$ serves as a fundamental domain for the left action of $\Gamma_\mathfrak{a}$ on $\Gamma_\mathfrak{a}\cdot\mathrm{SL}_r(K_\mathbb{R})$, as well. Using that μ_{Riem} is bi-invariant several times, we have that

$$\begin{aligned}\mu_{\mathrm{Riem}}(\Delta_\mathfrak{a}^{-1}(\delta)) &= \mu_{\mathrm{Riem}}\left(\Gamma_\mathfrak{a}\backslash\Gamma_\mathfrak{a}\,\mathrm{SL}_r(K_\mathbb{R})/(g\,\mathrm{SU}_r(K_\mathbb{R})g^{-1})\right)\\ &= \frac{\mu_{\mathrm{Riem}}(\Gamma^1_\mathfrak{a}\backslash\,\mathrm{SL}_r(K_\mathbb{R}))}{\mu_{\mathrm{Riem}}(g\,\mathrm{SU}_r(K_\mathbb{R})g^{-1})} = \mu_{\mathrm{Riem}}(\Delta_\mathfrak{a}^{-1}(1))\end{aligned}$$

for all δ. □

Using the integration formula above, we now construct the orthogonal projection onto $L^2_{\mathrm{det}}(X_r)$. For this, define $\Delta'_{\mathfrak{a}}\colon L^2(X_{r,\mathfrak{a}}) \to L^2(X_{1,\mathfrak{a}})$ by

$$\Delta'_{\mathfrak{a}}(f)(\delta) = \int_{x\in\Delta_{\mathfrak{a}}^{-1}(\delta)} f(x)\,dx.$$

Next, define the operator

$$\pi^{\mathfrak{a}}_{\mathrm{det}} = \mu_{\mathrm{Riem}}(\Delta_{\mathfrak{a}}^{-1}(1))^{-1}\Delta^*_{\mathfrak{a}}\Delta'_{\mathfrak{a}}\colon L^2(X_{r,\mathfrak{a}}) \to L^2(X_{r,\mathfrak{a}}), \tag{7}$$

and let π_{det} be the direct sum of the operators $\pi^{\mathfrak{a}}_{\mathrm{det}}$ over the class group.

Lemma 2.28. *The operator $\pi^{\mathfrak{a}}_{\mathrm{det}}$ is the orthogonal projection onto $L^2_{\mathrm{det}}(X_{r,\mathfrak{a}})$.*

Proof. Let $f \in L^2(X_{r,\mathfrak{a}})$ and $g \in L^2(X_{1,\mathfrak{a}})$. Using the integration formula (5), we have

$$\begin{aligned}
\langle \Delta'_{\mathfrak{a}} f, g\rangle_{X_{1,\mathfrak{a}}} &= \int_{\delta\in X_{1,\mathfrak{a}}} \Delta'_{\mathfrak{a}} f(\delta)\overline{g(\delta)}\,d\delta = \int_{\delta\in X_{1,\mathfrak{a}}} \left(\int_{x\in\Delta_{\mathfrak{a}}^{-1}(\delta)} f(x)dx\right)\overline{g(\delta)}\,d\delta \\
&= \int_{\delta\in X_{1,\mathfrak{a}}} \left(\int_{x\in\Delta_{\mathfrak{a}}^{-1}(\delta)} f(x)\overline{g(\Delta_{\mathfrak{a}}(x))}\,dx\right) d\delta \\
&= \int_{\delta\in X_{1,\mathfrak{a}}} \left(\int_{x\in\Delta_{\mathfrak{a}}^{-1}(\delta)} f(x)\overline{(\Delta^*_{\mathfrak{a}}g)(x)}\,dx\right) d\delta \\
&= r^{\frac{ru}{2}} \int_{x\in X_{r,\mathfrak{a}}} f(x)\overline{(\Delta^*_{\mathfrak{a}}g)(x)}\,dx = r^{\frac{ru}{2}}\langle f, \Delta^*_{\mathfrak{a}}g\rangle_{X_{r,\mathfrak{a}}}.
\end{aligned}$$

Moreover, we compute that

$$\begin{aligned}
\Delta'_{\mathfrak{a}}\Delta^*_{\mathfrak{a}}g(\delta) &= \int_{x\in\Delta_{\mathfrak{a}}^{-1}(\delta)} (\Delta^*_{\mathfrak{a}}g)(x)\,dx = \int_{x\in\Delta_{\mathfrak{a}}^{-1}(\delta)} g(\Delta_{\mathfrak{a}}(x))\,dx \\
&= \int_{x\in\Delta_{\mathfrak{a}}^{-1}(\delta)} g(\delta)\,dx = \mu_{\mathrm{Riem}}(\Delta_{\mathfrak{a}}^{-1}(\delta))g(\delta) = \mu_{\mathrm{Riem}}(\Delta_{\mathfrak{a}}^{-1}(1))g(\delta).
\end{aligned}$$

In other words, we have shown that

$$\Delta'_{\mathfrak{a}}\Delta^*_{\mathfrak{a}} = \mu_{\mathrm{Riem}}(\Delta_{\mathfrak{a}}^{-1}(1))\cdot \mathrm{id}\,.$$

We finally deduce the formula

$$\|\Delta^*_{\mathfrak{a}} f\|^2_{X_r} = \mu_{\mathrm{Riem}}(\Delta_{\mathfrak{a}}^{-1}(1))r^{\frac{-ru}{2}}\,\|f\|^2_{X_1}\,, \tag{8}$$

for any function $f \in L^2(X_1)$, by piecing together the computations above.

We have $\pi^{\mathfrak{a}}_{\mathrm{det}}(L^2(X_{r,\mathfrak{a}})) \subset L^2_{\mathrm{det}}(X_{r,\mathfrak{a}})$ and, by the properties above, $\pi^{\mathfrak{a}}_{\mathrm{det}}$ is self-adjoint and restricts to the identity on $L^2_{\mathrm{det}}(X_{r,\mathfrak{a}})$. □

2.6.3 Distance functions and volumes

Although the Riemannian structure provides a notion of distance, we require two finer ways of measuring it.

Definition 2.29. For $x \in \mathbb{R}^{r_1+r_2}$, let $\|x\|_H = \|\pi_H(x)\|$, and for $g \in \mathrm{GL}_r(K_{\mathbb{R}})$ define

$$\tau(g) = \|\log|\det g|\|^2_H.$$

For $\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$, let $\|\cdot\|_{\mathrm{op}}$ denote the operator norm with respect to the Euclidean norm on $\mathbb{K}^r$. For $g = (g_v)_v \in \mathrm{GL}_r(K_{\mathbb{R}}) = \prod_v \mathrm{GL}_r(K_v)$, define

$$\rho(g) = \max_v \log\max\left(\frac{\|g_v\|_{\mathrm{op}}}{|\det g_v|^{\frac{1}{r}}}, \frac{\|g_v^{-1}\|_{\mathrm{op}}}{|\det g_v^{-1}|^{\frac{1}{r}}}\right).$$

The functions defined above satisfy the following properties. For all $g, h \in \mathrm{GL}_r(K_\mathbb{R})$ we have the inequality $\rho(gh) \leq \rho(g) + \rho(h)$. Moreover, for all $g \in \mathrm{GL}_r(K_\mathbb{R})$, $u \in \mathrm{U}_r(K_\mathbb{R})$ and $a \in K_\mathbb{R}^\times$ we have

$$\rho(g) = \rho(gu) = \rho(ug) = \rho(ag) = \rho(g^{-1})$$

and if $a \in \mathbb{R}_{>0}$ then

$$\tau(g) = \tau(gu) = \tau(ug) = \tau(ag) = \tau(g^{-1}).$$

In particular, ρ and τ both descend to Y_r. One should think of ρ and τ as being a "distance to identity" on the $\mathrm{SL}(r)$ part, respectively on the $\mathrm{GL}(1)$ part. We also define balls for the former as

$$B(t) = \{g \in \mathrm{SL}_r(K_\mathbb{R}) \mid \rho(g) \leq t\}. \tag{9}$$

We now compute the volumes of certain spaces, including the balls defined above and the full space X_r. For this, we use two estimates from [MP21].

Lemma 2.30. *We have*

$$\log \mu_{\mathrm{Riem}}(\mathrm{SU}_r(K_\mathbb{R})) \geq -\frac{d}{4} r^2 \log r.$$

Proof. We apply [MP21, Proposition 11] to lower bound the volume of the local parts, after which we sum over complex and real places. We use the notation a for r in [MP21, Proposition 11], and r for d in [MP21, Proposition 11].

For the real case holds that $a = r/2$ if r is even, and $(r-1)/2$ otherwise. Using the bound $j! \leq j^j$, and using the fact that $m_k \leq r$, we have

$$-\log \mu_{\mathrm{Riem}}(\mathrm{SU}_r(\mathbb{R})) \leq \sum_{k=1}^{a} \log(m_k!) \leq \sum_{k=1}^{a} m_k \log(r) \leq \log(r) r^2/4.$$

Indeed, in the case that r is odd, $m_k = 2k-1$, yielding $\sum_{k=1}^{a} m_k = a^2 \leq r^2/4$. In the case that r is even, $m_k = 2k-1$ except for $m_a = a-1$, for which we can then deduce that $\sum_{k=1}^{a} m_k = (a-1)^2 + (a-1) = a(a-1) = \frac{(r-1)(r-3)}{4} \leq r^2/4$.

For the complex case, we have $a = r-1$ and $m_k = k$, yielding

$$-\log \mu_{\mathrm{Riem}}(\mathrm{SU}_r(\mathbb{C})) \leq \sum_{k=1}^{a} \log(m_k!) \leq \sum_{k=1}^{a} m_k \log(r) \leq \log(r) a(a+1)/2 \leq \log(r) r^2/2$$

Hence, summing over all places, $-\log \mu_{\mathrm{Riem}}(\mathrm{SU}_r(K_\mathbb{R})) \leq d \log(r) r^2/4$, which finishes the proof. □

Lemma 2.31. *Let $\mathbb{K}$ be either $\mathbb{C}$ or $\mathbb{R}$. Then, for $t \leq 1$, we have*

$$I := \int_{(a_i)_i \in \Delta_t^*} \prod_{1 \leq i < j \leq r} \sinh(a_i - a_j)^{[\mathbb{K}:\mathbb{R}]} \geq \left(\frac{t}{4r^2}\right)^{\frac{(r-1)(r[\mathbb{K}:\mathbb{R}]+2)}{2}}$$

where $\Delta_t^* = \{(a_1, \ldots, a_{r-1}) \in \mathbb{R} \mid t > a_1 > \ldots > a_{r-1} > a_r := -\sum_{i=1}^{r-1} a_i > -t\}$.

Proof. We follow the same steps as in the proof of [MP21, Proposition 14], where we use the assumption $t \leq 1$ instead. We write $g = [\mathbb{K} : \mathbb{R}] \in \{1, 2\}$ for conciseness.

We apply [MP21, Lemma 13] with $k = r-1$ to find intervals $[\alpha_i, \beta_i]$ (for $i \in \{1, \ldots, r-1\}$) satisfying the properties (1) - (6) of [MP21, Lemma 13]. For a certain reordering $\sigma \in S_{r-1}$, we put $Q := \prod_{i=1}^{r-1} [t\alpha_{\sigma(i)}, t\beta_{\sigma(i)}]$. By properties (1) and (2) of [MP21, Lemma 13] we can deduce that

$$I := \int_{(a_i)_i \in \Delta_t^*} \prod_{1 \leq i < j \leq r} \sinh(a_i - a_j)^g da_i \geq \int_{(a_i)_i \in Q} \prod_{1 \leq i < j \leq r} \sinh(a_i - a_j)^g da_i.$$

The function $x \mapsto \sinh(x)\exp(-x) = \frac{1-\exp(-2x)}{2}$ is increasing, and we have $\frac{1-\exp(-2x)}{2} \geq x/2$ for $x < 1/2$. Hence, for $x \geq \frac{t}{4r^2}$,

$$\sinh(x) = \frac{1-\exp(-2x)}{2} \cdot \exp(x) \geq \frac{1-\exp(-\frac{t}{2r^2})}{2} \cdot \exp(x) \geq \frac{t}{4r^2} \cdot \exp(x),$$

since $\frac{t}{2r^2} \leq 1/2$. This yields

$$\begin{aligned} I &\geq \left(\frac{t}{4r^2}\right)^{r(r-1)g/2} \int_{(a_i)_i \in Q} \prod_{1 \leq i < j \leq r} \exp(a_i - a_j)^g da_i \\ &\geq \left(\frac{t}{4r^2}\right)^{r(r-1)g/2} \int_{(a_i)_i \in Q} \exp(g \underbrace{\sum_{i<j}(a_i - a_j)}_{\beta}) da_i. \end{aligned}$$

In the proof of [MP21, Proposition 14], we see that $\beta = 2\sum_{i=1}^{r-1}(r-i)a_i$. By properties (3) and (6) of [MP21, Lemma 13] we deduce that $a_i \geq t/4$ for at least $\lfloor r/5 \rfloor$ intervals $[t\alpha_i, t\beta_i]$ (meaning, $\alpha_i \geq 1/4$ for these intervals), and that all intervals have width at least $t/(4r^2)$. Hence,

$$\begin{aligned} I &\geq \left(\frac{t}{4r^2}\right)^{r(r-1)g/2} \int_{(a_i)_i \in Q} \exp(2g \sum_{i<j}(r-i)a_i) da_i \\ &\geq \left(\frac{t}{4r^2}\right)^{r(r-1)g/2} \cdot \left(\frac{t}{4r^2}\right)^{r-1} \cdot \exp(2gt \sum_{i=1}^{\lfloor r/5 \rfloor} i/4) \\ &\geq \left(\frac{t}{4r^2}\right)^{r(r-1)g/2} \cdot \left(\frac{t}{4r^2}\right)^{r-1} \cdot \exp(\frac{gr^2 t}{200}) \geq \left(\frac{t}{4r^2}\right)^{\frac{(r-1)(rg+2)}{2}}, \end{aligned}$$

which is what we wanted to proof. □

Lemma 2.32. *Let $t \leq 1$, and $r \geq 2$. We have*

$$\log \mu_{\mathrm{Riem}}(B(t)) \geq -\log(4r^2/t) \cdot dr^2.$$

Proof. Noting that $\mu_{\mathrm{Riem}}(B(t)) = \prod_\nu I^{(\nu)}$, where $I^{(\nu)} = I$ as in Lemma 2.31 with $\mathbb{K} = K_\nu$ (which is $\mathbb{R}$ or $\mathbb{C}$), we compute (using $\sum_\nu [K_\nu : K] = d$ and $\sum_\nu 1 \leq d$),

$$\begin{aligned} \log \mu_{\mathrm{Riem}}(B(t)) &\geq -\log(4r^2/t) \cdot (r-1) \cdot (d + rd/2) \\ &\geq -\log(4r^2/t) \cdot d \cdot (r-1)(r+2)/2 \geq -\log(4r^2/t) \cdot dr^2. \end{aligned}$$

□

Proposition 2.33. *We have*

$$\mu_{\mathrm{Riem}}(X_r) = \sqrt{d} r^{\frac{r_2+1}{2}} 2^{-\frac{r_2}{2}} \mu_{\mathrm{Riem}}(\mathrm{SU}_r(K_\mathbb{R}))^{-1} h_K R_K |\Delta_K|^{\frac{r^2-1}{2}} \prod_{j=2}^{r} \zeta_K(j).$$

Proof. Let $\mathfrak{a} \subset \mathcal{O}_K$ be an ideal. By the computations and integration formula in Section 2.6.2, we have

$$\begin{aligned} \mu_{\mathrm{Riem}}(X_{r,\mathfrak{a}}) &= \int_{x \in X_{r,\mathfrak{a}}} dx = r^{-\frac{r_u}{2}} \int_{\delta \in X_{1,\mathfrak{a}}} \int_{x \in \Delta_\mathfrak{a}^{-1}(\delta)} d\delta \\ &= r^{-\frac{r_u}{2}} \int_{\delta \in X_{1,\mathfrak{a}}} \mu_{\mathrm{Riem}}(\Delta_\mathfrak{a}^{-1}(\delta)) d\delta \\ &= r^{-\frac{r_u}{2}} \int_{\delta \in X_{1,\mathfrak{a}}} \mu_{\mathrm{Riem}}(\Delta_\mathfrak{a}^{-1}(1)) d\delta \\ &= r^{-\frac{r_u}{2}} \mu_{\mathrm{Riem}}(X_{1,\mathfrak{a}}) \frac{\mu_{\mathrm{Riem}}\left(\mathrm{SL}_r(\mathcal{O}_K, \mathfrak{a}) \backslash \mathrm{SL}_r(K_\mathbb{R})/\mathbb{R}_{>0}\right)}{\mu_{\mathrm{Riem}}(\mathrm{SU}_r(K_\mathbb{R}))}. \end{aligned}$$

By Prasad's formula, we have (see [MP21, Proposition 18], which is also valid in the non-compact case):

$$\mu_{\mathrm{Riem}}\left(\mathrm{SL}_r(\mathcal{O}_K,\mathfrak{a})\backslash \mathrm{SL}_r(K_{\mathbb{R}})/\mathbb{R}_{>0}\right) = r^{\frac{d}{2}}|\Delta_K|^{\frac{r^2-1}{2}}\prod_{j=2}^{r}\zeta_K(j).$$

Finally, we have

$$\mu_{\mathrm{Riem}}(X_{1,\mathfrak{a}}) = \sqrt{d}2^{-\frac{r_2}{2}}R_K.$$

□

Lemma 2.34. *The residue $\zeta_K^*(1)$ of ζ_K at 1 satisfies*

$$\zeta_K^*(1) \leq \left(\frac{e\log|\Delta_K|}{2(d-1)}\right)^{d-1} \leq |\Delta_K|^{\frac{1}{2}}.$$

Proof. The first inequality is [Lou00, Equation (2)]. The second one follows from applying the inequality $\frac{e\log|x|}{|x|} \leq 1$, which holds for all x, to $x = |\Delta_K|^{\frac{1}{2(d-1)}}$. □

Lemma 2.35. *We have*

$$\log(h_K R_K) \leq \log|\Delta_K| + O(1)$$

Proof. Apply Lemma 2.34 and the analytic class number formula. □

Remark 2.36. In the original statement of Louboutin [Lou00, Equation (2)], one can see that, next to $\sqrt{|\Delta_K|}$, the dominant factor is $\left(\frac{e\log|\Delta_K|}{2(d-1)}\right)^{d-1}$ which might be much smaller than $\sqrt{|\Delta_K|}$. Hence, the bound above, though simple, is not tight and might be improved to get a better approximation factor in the main result of this paper.

The results above finally imply a key inequality.

Lemma 2.37. *We have*

$$\log\mu_{\mathrm{Riem}}(X_r) \leq \frac{dr^2}{4}\log r + \frac{r^2}{2}\log|\Delta_K| + O(\log\log|\Delta_K| + dr^2).$$

2.7 Automorphic theory

The purpose of this section is to explain the spectral decomposition of $L^2(\mathbb{X}_r)$ and analyze the action of Hecke operators on the different components. Our main references here are [CU04, Sec. 3.2, Sec. 4.1] and [GH24, Sec. 10].

2.7.1 The spectral decomposition

We recall first that standard parabolic subgroups $P \subset \mathrm{GL}_r$ are in correspondence with partitions $\sum_i r_i = r$. Given such a partition, called $\wp = (r_i)$ for short, the Levi subgroup $M_\wp$ of the corresponding parabolic $P_\wp$ is isomorphic to $\prod_i \mathrm{GL}_{r_i}$ (the group $P_\wp$ is the group of blockwise upper triangular matrices with blocks of sizes given by the partition). We attach to $M_{(r_i)}$ a certain space of characters, denoted by $\mathfrak{a}_{M_\wp}^*$, which we can interpret as a tuple of complex numbers or parameters. We denote the subspace of purely imaginary parameters by $\Im(\mathfrak{a}_{M_\wp}^*)$. If, for each i, we have an irreducible automorphic representation π_i appearing in the discrete spectrum of $L^2(\mathbb{X}_{r_i})$, and $\lambda \in \Im(\mathfrak{a}_{M_\wp}^*)$, then we can construct the induced representation $I(\bigotimes_i \pi_i, \lambda)$, as in [GH24, Sec. 10.1].

A celebrated theorem of Moeglin and Waldspurger describes the discrete spectrum in terms of Speh representations. To introduce the latter, let $N \in \mathbb{Z}_{>0}$ and let s be a divisor of N. There

is a unique standard Levi $M \subset \mathrm{GL}_N$ isomorphic to $\prod_{i=1}^{N/s} \mathrm{GL}_s$. Given a cuspidal automorphic representation σ of GL_s, we can define the Speh representation $\mathrm{Speh}(\sigma, N/s)$ for M (see [GH24, Sec. 10.7]) that occurs in the discrete spectrum of $L^2(\mathbb{X}_N)$.

The spectral theorem of Langlands now states that $L^2(\mathbb{X}_r)$ is a sub-module of

$$\bigoplus_{\wp\colon \sum_i r_i = r} \bigoplus_{s_i | r_i} \widehat{\bigoplus_{\sigma_i}} \int_{\lambda \in \Im(\mathfrak{a}^*_{M_\wp})}^{\oplus} I(\bigotimes_i \mathrm{Speh}(\sigma_i, r_i/s_i), \lambda) d\lambda, \tag{10}$$

where σ_i ranges over cuspidal automorphic representations of $\mathrm{GL}_{s_i}(K)$, and $\int^{\oplus}$ denotes a direct integral decomposition. We can identify the components that make up $L^2_{\mathrm{det}}(\mathbb{X}_r)$ by noting that

$$L^2(\mathbb{X}_1) = \bigoplus_{\chi} \mathbb{C} \cdot \chi,$$

where χ runs over all (unitary) Hecke characters of K, and that $L^2(\mathbb{X}_1)$ is isomorphic to $L^2_{\mathrm{det}}(\mathbb{X}_r)$ by the map Δ^*. It is known that $\mathrm{Speh}(\chi, r)$, for a Hecke character χ, is the one-dimensional representation of $\mathrm{GL}_r(\mathbb{A}_K)$ given by $\chi \circ \det$. Thus, $L^2_{\mathrm{det}}(\mathbb{X}_r)$ is the contribution of the terms corresponding to the trivial partition $r = r$ and $s = 1$ in (10).

2.7.2 Hecke operators

In terms of lattices, the Hecke operator $T_\mathfrak{p}$ corresponds to uniform averaging over submodules $N \subset M$ such that at $M/N \cong \mathcal{O}_K/\mathfrak{p}$ at every module lattice M. More precisely, for a function $f \in L^2(X_r)$, we define

$$T_\mathfrak{p} f(M) = \frac{1}{D_\mathfrak{p}} \sum_{\substack{N \subset M \\ M/N \cong \mathcal{O}_K/\mathfrak{p}}} f(N),$$

where, if $q = N(\mathfrak{p})$, the number of terms in the average is $D_\mathfrak{p} = 1 + q + \ldots + q^{r-1}$.

Interpreting X_r adelically, the operator $T_\mathfrak{p}$ acts only at the place $\mathfrak{p}$. More precisely, let $\pi_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}$ be a uniformizer at $\mathfrak{p}$, and write

$$\mathrm{GL}_r(\mathcal{O}_\mathfrak{p}) \begin{pmatrix} \pi_\mathfrak{p} & 0 & \cdots & 0 \\ 0 & 1 & & \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix} \mathrm{GL}_r(\mathcal{O}_\mathfrak{p}) = \bigsqcup_{g \in R_\mathfrak{p}} \mathrm{GL}_r(\mathcal{O}_\mathfrak{p}) g \tag{11}$$

for some finite set $R_\mathfrak{p}$ (of size $D_\mathfrak{p}$). For a function $f \in L^2(X_r)$ and $x \in \mathrm{GL}_r(\mathbb{A}_K)$ we have

$$T_\mathfrak{p} f(x) = \frac{1}{D_\mathfrak{p}} \sum_{g \in R_\mathfrak{p}} f(xg^{-1}) = \frac{1}{D_\mathfrak{p}} \sum_{g \in R_\mathfrak{p}} g^{-1} \cdot f.$$

This is well-defined because the action (from the right) of $\mathrm{GL}_r(\mathcal{O}_\mathfrak{p})$ is trivial on X_r by definition.

Note that $T_\mathfrak{p} \mathbf{1} = \mathbf{1}$, where $\mathbf{1}$ is the constant 1 function on X_r. We remark also that, by definition, a Hecke operator also acts on the irreducible representations occurring in $L^2(X_r)$. On such representations, it acts by a scalar, the *Hecke eigenvalue*. In particular, it is an endomorphism of $L^2_{\mathrm{det}}(X_r)$.

Let π be an irreducible automorphic representation of $\mathrm{GL}_r(\mathbb{A}_K)$. The representations relevant in our case are unramified at all primes $\mathfrak{p}$, meaning that, they contain nonzero vectors fixed by $\mathrm{GL}_r(\mathcal{O}_\mathfrak{p})$. Clearly, all automorphic representations appearing in the decomposition of $L^2(X_r) \subset L^2(\mathbb{X}_r)$ are unramified. In this case, for every $\mathfrak{p}$ we can attach to π (in fact, to the component $\pi_\mathfrak{p}$ at $\mathfrak{p}$) its *Satake parameters* $\alpha_1, \ldots, \alpha_r \in \mathbb{C}$. These describe the action of the Hecke operators at $\mathfrak{p}$. For instance (see [GH24, (7.2)]), the eigenvalue of $T_\mathfrak{p}$ on π is

$$\frac{1}{D_\mathfrak{p}} q^{\frac{r-1}{2}} \sum_{k=1}^{r} \alpha_k.$$

In our application, we are satisfied with bounding the eigenvalue of $T_{\mathfrak{p}}$ by

$$q^{-(r-1)/2}\sum_{k=1}^{r}\alpha_k,$$

using the formula for $D_{\mathfrak{p}}$.

For example, the Satake parameters of the trivial representation of $\mathrm{GL}_r(K_{\mathfrak{p}})$ are

$$q^{-\frac{r-1}{2}}, q^{-\frac{r-1}{2}+1}, \dots, q^{\frac{r-1}{2}},$$

and this corresponds to the fact that $T_{\mathfrak{p}}$ acts by the scalar 1 on constant functions. However, $T_{\mathfrak{p}}$ acts on most unramified automorphic representations with smaller eigenvalues and this is the source of equidistribution.

2.7.3 Eigenvalue bounds

We now analyze the action of Hecke operators using the explicit spectral decomposition. This is formally contained in the work of Clozel and Ullmo [CU04], who treated the case $K = \mathbb{Q}$. We follow their method and adjust it to cover the general number field case.

Proposition 2.38. *The operator norm of $T_{\mathfrak{p}}$, defined with respect to the L^2-norm on X_r endowed with μ_{Riem}, acting on the orthogonal complement of $L^2_{\mathrm{det}}(X_r) \subset L^2(X_r)$ is bounded by $rq^{-3/8}$.*

Proof. First, it is important to understand the Satake parameters of unramified cuspidal representations π of GL_N, since these are the building blocks of the spectral decomposition. The Generalized Ramanujan Conjecture (GRC) states that, if $\alpha_1, \dots, \alpha_N$ are the Satake parameters of π at $\mathfrak{p}$, then $|\alpha_i| = 1$ for all i. This conjecture seems far out of reach (see [BB13] for a survey), but there are useful bounds towards it.

Let $\theta_N \geq 0$ be the exponent in the best known bound towards GRC, that is,

$$|\alpha_i| \leq q^{\theta_N}$$

for all i. We have (see [BB11]) $\theta_1 = 0$, $\theta_2 \leq 7/64$, $\theta_3 \leq 5/14$, $\theta_4 \leq 9/22$, and more generally $\theta_N \leq 1/2$ for all N.

We can now compute eigenvalues of Hecke operators on the representations occurring in the spectral decomposition (10), as in [CU04, Sec. 4.1]. Let $\mathfrak{p}$ be a prime of K and let $q = N(\mathfrak{p})$. A representation $\mathrm{Speh}(\sigma, m)$ is unramified at $\mathfrak{p}$ if an only if the cuspidal representation σ is. In this case, its Satake parameters at $\mathfrak{p}$ are

$$\alpha_i q^{\frac{m+1}{2}-j},\ i = 1, \dots, s,\ j = 1, \dots, m,$$

where $\alpha_1, \dots, \alpha_s$ are the Satake parameters of σ at $\mathfrak{p}$.

If $I(\otimes_i \pi_i, \lambda)$ contains nonzero $\mathrm{GL}_r(\mathcal{O}_{\mathfrak{p}})$-invariant vectors, then all π_i are unramified at $\mathfrak{p}$ and the Satake parameters of the irreducible sub-quotients of $I(\otimes_i \pi_i, \lambda)$ unramified at $\mathfrak{p}$ are the

$$\alpha_{i,k}\zeta_i$$

where the $\alpha_{i,k}$ are the Satake parameters of the π_i and $|\zeta_i| = 1$ (because $\lambda \in \Im(\mathfrak{a}_M)$ is imaginary). Therefore, the eigenvalue of $T_{\mathfrak{p}}$ acting on the $\mathrm{GL}_r(\mathcal{O}_{\mathfrak{p}})$-fixed points of the representation $I(\otimes_i \mathrm{Speh}(\sigma_i, r_i/s_i), \lambda)$ is bounded in absolute value by

$$\sum_i \sum_{j=1}^{r_i/s_i} \sum_{k=1}^{s_i} q^{\theta_{s_i} + \frac{r_i/s_i+1}{2} - j - \frac{r-1}{2}}.$$

We bound this crudely by

$$rq^{\max(\theta_{s_i}+r_i/2s_i-r/2)}.$$

We now estimate the exponent in various cases. First, note the exceptional case when $i = 1$, $r_1 = r$, and $s_1 = 1$, which occurs when considering representations in $L^2_{\mathrm{det}}(X_r)$. In that case our bound is simply r, which does not give any saving. Excluding this case, we can have for some i that

- $s_i = 1$ and $r_i < r$: the exponent $\theta_1 + r_i/2 - r/2$ is at most $-1/2$;
- $s_i = 2$ (so that $r \geq r_i \geq 2$): the exponent $\theta_2 + r_i/4 - r/2 \leq 7/64 - r/4$ is bounded by $-25/64 \leq -3/8$;[6]
- $s_i \geq 3$ (so that $r \geq r_i \geq 3$): using the general bound $\theta_{s_i} \leq 1/2$, the exponent is at most $\frac{1}{2} + r/6 - r/2 \leq 1/2 - r/3 \leq -1/2$.

This finishes the proof. Note that the first of these cases shows that, even assuming GRC, the best exponent we could hope for in general is $-1/2$. □

In the following, we consider averages of Hecke operators. If $\mathcal{P}$ is a finite subset of the prime ideals of K, we write

$$T_{\mathcal{P}} = \frac{1}{|\mathcal{P}|} \sum_{\mathfrak{p} \in \mathcal{P}} T_{\mathfrak{p}}. \tag{12}$$

For $B \geq 0$, we can define $\mathcal{P}(B)$ as the set of prime ideals with norm at most B. The Extended Riemann Hypothesis implies that

$$|\mathcal{P}(B)| \geq \frac{B}{2 \log B}$$

for $B \geq \max((12 \log|\Delta_K| + 8d + 28)^4, 3 \cdot 10^{11})$, where we recall that d is the degree of K and Δ_K is its discriminant. This was shown in Lemma A.3 of [BDP+20]. We also have the trivial upper bound $|\mathcal{P}(B)| \leq dB$ that follows from unique factorization.

Corollary 2.39. *Let $B \geq \max((12 \log|\Delta_K| + 8d + 28)^4, 3 \cdot 10^{11})$. The operator norm of $T_{\mathcal{P}(B)}$ acting on the orthogonal complement of $L^2_{\mathrm{det}}(X_r) \subset L^2(X_r)$ is bounded by $20 \cdot rd \cdot B^{-3/8} \log(B)$.*

Proof. This follows from the standard technique of splitting the average into dyadic intervals. With $\alpha = -3/8$, we write

$$\sum_{N(\mathfrak{p}) \leq B} N(\mathfrak{p})^{\alpha} \leq \sum_{k=1}^{\log_2(B)-1} \sum_{2^k \leq N(\mathfrak{p}) \leq 2^{k+1}} N(\mathfrak{p})^{\alpha}.$$

The inner sum is at most $d2^{k+1}2^{k\alpha}$ by the trivial upper bound on $\mathcal{P}(B)$. Removing constant factors, the outer sum now becomes a geometric series, namely

$$\sum_{k=1}^{\log_2(B)-1} 2^{k(1+\alpha)} \leq 10B^{1+\alpha},$$

where 10 is large enough considering the size of α.

Plugging in the lower bound for $\mathcal{P}(B)$, Proposition 2.38 implies the upper bound

$$20rd \cdot \frac{\log(B)}{B} \cdot B^{1+\alpha} = 20rd \cdot B^{\alpha} \log(B)$$

on the operator norm of $T_{\mathcal{P}(B)}$. □

[6] We take $-3/8$ here only to make expressions in the rest of the paper cleaner. Any non-trivial bound gives the same qualitative result in this paper.

3 Rounding module lattices

3.1 Introduction

In the worst-case to average-case reduction of the present paper, the average-case stems from a Haar-uniform distribution over the space of module lattices (see Section 2.3.2). Due to the continuity of this latter space, such a uniform distribution cannot be adequately represented by a computer; indeed, computers (or, more formally, Turing machines) can only process module lattices that are represented by rational numbers (bounded in size). We tackle this issue by using a probabilistic algorithm that, for an input module lattice M, outputs a random sample from a specific distribution $\mathcal{D}(M) := \mathrm{Round}^{\mathrm{Perf}}_{\mathrm{Lat}}(M)$ over *rational module lattices*. This algorithm (Algorithm 2) can be seen as a probabilistic way of rounding the input module lattice M to a geometrically close rational module lattice. The average-case distribution considered in this paper can be described by $\mathrm{Round}^{\mathrm{Perf}}_{\mathrm{Lat}}(M)$, where M is sampled Haar-uniform over the space of module lattices.

This rounding algorithm is a generalization of [BDP+20, Algorithm 1] to module lattices. It also closely resembles [FPS22, Algorithm 3.1], with the difference that our version of the rounding algorithm forces the output module to be full-rank and is proven to be Hölder continuous; properties indispensable for the purposes of the current paper.

This specific distribution $\mathrm{Round}^{\mathrm{Perf}}_{\mathrm{Lat}}(M)$ over rational module lattices has special properties in order to indeed resolve the issues coming from the continuity of the module-lattice space. Specifically the distribution $\mathrm{Round}^{\mathrm{Perf}}_{\mathrm{Lat}}$ satisfies

(i) Discreteness, efficiency and rationality: For each M, we have that $\mathrm{Round}^{\mathrm{Perf}}_{\mathrm{Lat}}(M)$ is a random module lattice supported on discrete set S of *rational module lattices*, each of which can be represented by a tuple of rational entries. Additionally, for any module lattice M, almost all of the weight of $\mathrm{Round}^{\mathrm{Perf}}_{\mathrm{Lat}}(M)$ is on a finite set $S' \subseteq S$. Moreover, the algorithm computing a sample from $\mathrm{Round}^{\mathrm{Perf}}_{\mathrm{Lat}}(M)$ is efficient.

(ii) Independence of module representation: The distribution $\mathrm{Round}^{\mathrm{Perf}}_{\mathrm{Lat}}(M)$ does not depend on the choice of pseudo-basis of the module M. This makes $\mathrm{Round}^{\mathrm{Perf}}_{\mathrm{Lat}}$ a map from $X_r(K)$ to the distribution space $L^1(S)$ over the set S of rational modules.

(iii) Preservation of geometry: With high probability, a rational module lattice sample $R \leftarrow \mathrm{Round}^{\mathrm{Perf}}_{\mathrm{Lat}}(M)$ has almost the same geometry as M, meaning that solving respectively SVP, SIVP, etc., on R allows for solving SVP, SIVP, etc., on M (and vice versa).

(iv) Continuity: If M and M' are almost isomorphic, their associated distributions $\mathrm{Round}^{\mathrm{Perf}}_{\mathrm{Lat}}(M)$ and $\mathrm{Round}^{\mathrm{Perf}}_{\mathrm{Lat}}(M')$ are close in total variation distance.

The discreteness, efficiency and rationality makes that any module lattice M can be efficiently "represented" by a computer via the distribution $\mathrm{Round}^{\mathrm{Perf}}_{\mathrm{Lat}}(M)$, even if M itself cannot be. The independence of module representation makes that $\mathrm{Round}^{\mathrm{Perf}}_{\mathrm{Lat}}(-)$ a map truly on modules (and not a pseudo-basis representation thereof). The geometry preservation makes this distribution representation *useful* for the particular context of this paper: SVP-like problems are not (too much) distorted by the distribution representation. Lastly, continuity of $\mathrm{Round}^{\mathrm{Perf}}_{\mathrm{Lat}}$ allows quantifying the effects of *discretization* of the input of $\mathrm{Round}^{\mathrm{Perf}}_{\mathrm{Lat}}$, which will be treated in detail in Section 9.

An intuitive way of thinking about a sample of $\mathrm{Round}^{\mathrm{Perf}}_{\mathrm{Lat}}(M)$ (which is the output distribution of Algorithm 2) is by seeing it as a randomized rounding of the module M to a close, rational module M'. This probabilistic rounding is then done in such a way that the continuity in the module lattice space is transferred to a continuous change of the probability weights on the rational output modules.

The pseudo-algorithm computing the "perfect" rounding distribution $\mathrm{Round}_{\mathrm{Lat}}^{\mathrm{Perf}}(M)$ (Algorithm 2) involves real arithmetic and continuous distributions, and can therefore not be computed by a Turing machine. Instead, we resort to a discrete variant of $\mathrm{Round}_{\mathrm{Lat}}^{\mathrm{Perf}}(M)$, an actual algorithm called $\mathrm{Round}_{\mathrm{Lat}}(M)$, which approximates $\mathrm{Round}_{\mathrm{Lat}}^{\mathrm{Perf}}(M)$ within arbitrarily small statistical distance. The precise description of this discretization can be found in the proof of Lemma 3.3.

The precise main result of this section is the following proposition, in which the properties (i)-(iv) precisely match those just explained.

Proposition 3.1. *There exists an algorithm* $\mathrm{Round}_{\mathrm{Lat}}$ *with balancedness parameter* $\alpha \in \mathbb{R}_{>1}$ *and error parameter* $\varepsilon_0 \in (0, 1/2)$ *that takes* α*-balanced rank* r *module lattices* $(\mathbf{B}_M, \mathbf{I} = (\mathfrak{a}_i)_{i\in[r]})$ *over* K *as input, whose output distribution satisfies, for any* M*,*

$$\|\mathrm{Round}_{\mathrm{Lat}}(M) - \mathrm{Round}_{\mathrm{Lat}}^{\mathrm{Perf}}(M)\| < \varepsilon_0,$$

for a certain perfect distribution $\mathrm{Round}_{\mathrm{Lat}}^{\mathrm{Perf}}(M)$*, and where* $\mathrm{Round}_{\mathrm{Lat}}$ *and* $\mathrm{Round}_{\mathrm{Lat}}^{\mathrm{Perf}}$ *satisfy the following properties.*

(i) The output $(\mathbf{H}_R, (\mathfrak{h}_i)_{i\in[r]})$ *of* $\mathrm{Round}_{\mathrm{Lat}}(M)$ *is a rational module lattice that is bounded in size by* $\mathrm{poly}(\mathrm{size}(\mathbf{B}_M, \mathbf{I}), \log(1/\varepsilon_0))$*. Moreover, the algorithm runs in time* $\mathrm{poly}(\mathrm{size}(\mathbf{B}_M), \max_i \mathrm{size}(\mathfrak{a}_i), \log(1/\varepsilon_0))$*.*

(ii) If $(\mathbf{B}_M, \mathbf{I})$ *and* $(\mathbf{B}'_M, \mathbf{I}')$ *represent the same module, we have that*

$$\mathrm{Round}_{\mathrm{Lat}}^{\mathrm{Perf}}(\mathbf{B}_M, \mathbf{I}) = \mathrm{Round}_{\mathrm{Lat}}^{\mathrm{Perf}}(\mathbf{B}'_M, \mathbf{I}'),$$

meaning that their output distributions are identical.

(iii) For any $N \leftarrow \mathrm{Round}_{\mathrm{Lat}}(M)$ *there exists a full-rank matrix* $Y \in K_{\mathbb{R}}^{r\times r}$ *so that* $M = Y \cdot N$*, which satisfies* $\mathrm{cd}(Y) := \|Y\| \cdot \|Y^{-1}\| \leq 1 + \frac{1}{2n} \leq 2$ *and hence preserves SVP-like problems.*

For example, solving γ*-SVP (resp. SIVP) in* N *allows for solving* 2γ*-SVP (resp. SIVP) in* M*, with probability at least* $1 - \varepsilon_0^{n^4}$*.*

(iv) We have, for any module lattices M, M' *we have*

$$\|\mathrm{Round}_{\mathrm{Lat}}^{\mathrm{Perf}}(M) - \mathrm{Round}_{\mathrm{Lat}}^{\mathrm{Perf}}(M')\|_1 \leq 92n^3 \sqrt[4]{\log(12r/\varepsilon_0)}\sqrt{d(M, M')},$$

where $d(M, M') := \min_\phi(\|\phi - I\|_2, \|\phi^{-1} - I\|_2)$ *if there exists a module isomorphism* $\phi : M \to M'$ *between* M *and* M' *and* $d(M, M') = \infty$ *otherwise.*

Proof. Item (i) is proven in Lemma 3.3, item (ii) in Lemma 3.4, item (iii) in Lemma 3.2 and Lemma 3.6 using $(1 + \frac{1}{8n})(1 + \frac{1}{4n}) \leq (1 + \frac{1}{2n})$ (see also the proof of Lemma 8.3), and item (iv) in Lemma 3.7. □

3.2 The rounding algorithm and its properties

The rounding algorithm of this section is described in Algorithm 2. We now prove the properties listed in the introduction.

The following lemma on the matrix 2-norm and the determinant of the basis $\mathbf{B}_N$ will turn out useful.

Lemma 3.2. *We have, except with probability* $(\varepsilon_0)^{n^4}$*,*

$$\|\mathbf{B}_N\| \leq (1 + \frac{1}{8n})T,\ \|\mathbf{B}_N^{-1}\| \leq (1 + \frac{1}{4n})\frac{1}{T}$$

and

$$|\det(\mathbf{B}_N^{-1})|^{1/n} \leq (1 + \frac{1}{4})T^{-1}$$

Algorithm 2 Rounding a module lattice to a near rational module lattice

Require:

- A balancedness parameter $\alpha \in \mathbb{R}_{\geq 1}$,
- A pseudo-basis $(\mathbf{B}_M, (\mathfrak{a}_i)_{i\in[r]})$ of an α-balanced rank r module lattice M with $\mathfrak{a}_i \subseteq \mathcal{O}_K$.
- An error parameter $\varepsilon_0 \in (0, 1/2)$.

Ensure: A pseudo-basis $(H_R, (\mathfrak{h}_i)_{i\in[r]}))$ of a module lattice R of rank r where H_R has coefficients in K and $\mathfrak{h}_i \subseteq \mathcal{O}_K$ for all $i \in [r]$.

1: Put $\varsigma = 3 \cdot 2^n \cdot \alpha^{r-1} \cdot \Gamma_K \cdot n \cdot \det(M)^{1/n}$ and $T = 8n^4 \cdot \sqrt{\log(12r/\varepsilon_0)} \cdot \varsigma$.
2: **for** $i = 1$ to r **do**
3: Pick $\hat{c} \in \{x \in K_{\mathbb{R}} \mid \|x_\sigma\| = T \text{ for all } \sigma\}$ uniformly. Sample a center
4: Put $c = (\underbrace{0, \dots, 0}_{i-1}, \hat{c}, \underbrace{0, \dots, 0}_{r-i}) \in K_{\mathbb{R}}^r$.
5: Sample $v_i \leftarrow \mathcal{G}_{M,\varsigma,c}$ from the discrete Gaussian (see Definition 2.19) over M with center c. Repeat until v_i is $K_{\mathbb{R}}$-linearly independent of $(v_1, \dots, v_{i-1})$.
6: **end for**
7: Define the free r-module $N = \bigoplus_{i=1}^r \mathcal{O}_K \cdot v_i$; construct its basis $\mathbf{B}_N$ by stacking v_i as columns.
8: **return** the Hermite normal form $(H_R, (\mathfrak{h}_i)_{i\in[r]}))$ of the module R generated by the pseudo-basis $(\mathbf{B}_R := \mathbf{B}_N^{-1}\mathbf{B}_M, (\mathfrak{a}_i)_{i\in[r]})$.

Proof. For conciseness, we write $\mu = \log(2r/\varepsilon_0)$. We start with computing the matrix 2-norm of the matrices $\mathbf{B}_N$ and $\mathbf{B}_N^{-1}$. By the very definition of $\mathbf{B}_N$, we can write $\mathbf{B}_N = T \cdot J - E$, where J is diagonal with on the diagonal entries elements of $\{x \in K_{\mathbb{R}} \mid |x_\sigma| = 1 \text{ for all } \sigma\}$ and where $T \in \mathbb{R}_{>0}$. Hence $\|\mathbf{B}_N\|_2 = \|T \cdot J\| + \|E\| = T + \|E\|$. By the fact that N is constructed by stacking Gaussian samples (see lines 5 and 7), a single component e_{ij} of $E \in K_{\mathbb{R}}^{r\times r}$ must satisfy $e_{ij} \in \{x \in K_{\mathbb{R}} \mid |x_\sigma| \leq n^2 \cdot \mu \cdot \varsigma \text{ for all } \sigma\}$ except with probability (by putting $\kappa = n^{3/2}\mu$), $4(n^{3/2}\mu\sqrt{2\pi e})^n e^{-\pi\mu n^4}$ by Lemma 2.20

Hence *all* of these components satisfy this property except for probability $4n^2 \cdot (n^{3/2}\mu\sqrt{2\pi e})^n e^{-\pi\mu n^4} = (4^{1/n}n^{2/n} \cdot n^{3/2}\mu\sqrt{2\pi e} \cdot e^{-\pi\mu n^3})^n \leq (24\kappa e^{-\pi\kappa^2})^n \leq (e^{-\kappa^2})^n = e^{-\mu n^4} \leq (\varepsilon_0)^{n^4}$ with $\kappa = n^{3/2}\mu \geq 1.3$ (since $\mu = \sqrt{\log(12r/\varepsilon_0)} \geq \sqrt{\log(24)} \approx 1.78$ as $\varepsilon_0 \in (0, 1/2)$). The inequality $24\kappa e^{-\pi\kappa^2} \leq e^{-\kappa^2}$ for $\kappa \geq 1.3$ follows from graphical inspection.

For the remainder of this proof (where we account for the failure probability $(\varepsilon_0)^{n^4}$) we assume that indeed, for all $(e_{ij})_{ij}$, $(e_{ij}) \in \{x \in K_{\mathbb{R}} \mid |x_\sigma| \leq n^2 \cdot \mu \cdot \varsigma \text{ for all } \sigma\}$.

Hence, writing $\delta = n^3 \cdot \mu \cdot \varsigma/T \leq 1/(8n) < 1/2$, we obtain

$$\|\mathbf{B}_N\|_2 \leq T + \|E\|_2 \leq T + \sqrt{\|E\|_1\|E\|_\infty} \leq T + n^3 \cdot \mu \cdot \varsigma = T(1 + \delta)$$

Now for $\mathbf{B}_N^{-1}$, we use that $T^{-1} \cdot J^{-1}\mathbf{B}_N = I - T^{-1}E$. Hence

$$T\|\mathbf{B}_N^{-1}\| = \|T\mathbf{B}_N^{-1} \cdot J\| = \|(I - T^{-1}E)^{-1}\| = \|\sum_{j=0}^{\infty}(T^{-1}E)^j\| \leq 1 + \frac{n^3 \cdot \mu \cdot \varsigma/T}{1 - n^3 \cdot \mu \cdot \varsigma/T}$$
$$\leq 1 + \frac{\delta}{1-\delta} \leq 1 + 2\delta$$

Therefore, $\|\mathbf{B}_N^{-1}\| \leq \frac{1}{T} \cdot (1 + 2\delta)$.

The last computation is on the determinant of $\mathbf{B}_N^{-1}$. We have, by the fact that $\det(J) = 1$,

$$\det(\mathbf{B}_N) = \det(T \cdot J - E) = T^n \det(I - T^{-1}J^{-1}E),$$

for which we have the bound

$$|\det(I - T^{-1}J^{-1}E) - 1| \leq 2n\|T^{-1}J^{-1}E\| = \frac{2n\|E\|}{T} \leq 2n\delta$$

for $\|T^{-1}J^{-1}E\| = \frac{1}{T}\|E\| \leq 1/n$ (see [IR08], together with $(x+1)^n - 1 \leq 2nx$ for $nx \leq 1$). This inequality $\frac{1}{T}\|E\| \leq 1/n$ is clearly satisfied since we assumed that all components of E satisfy $(e_{ij})_{ij}$, $(e_{ij}) \in \{x \in K_{\mathbb{R}} \mid |x_\sigma| \leq n^2 \cdot \mu \cdot \varsigma \text{ for all } \sigma\}$.

Hence,

$$|\det(\mathbf{B}_N^{-1})| = T^{-n}|\det(I - T^{-1}J^{-1}E)| \leq T^{-n}(1 - 2n\delta)^{-1}.$$

Since $\delta = n^3\mu\varsigma/T = 1/(8n)$, we can easily deduce the claims, since $2n\delta \leq 1/4$. □

Lemma 3.3. *The pseudo-algorithm described in Algorithm 2, of which we will call the output distribution* $\mathrm{Round}_{\mathrm{Lat}}^{\mathrm{Perf}}(M)$ *on input* M*, is correct. Furthermore, there exists an algorithm, called* $\mathrm{Round}_{\mathrm{Lat}}$*, that, given* $\varepsilon_0 \in (0, 1/2)$*, and given any rational input* $(\mathbf{B}_M, \mathbf{I})$*, approximates the output distribution* $\mathrm{Round}_{\mathrm{Lat}}^{\mathrm{Perf}}$ *of Algorithm 2 (with the same input) within statistical distance* ε_0 *within bit complexity*

$$\mathrm{poly}(\mathrm{size}(\mathbf{B}_M), \max_i \mathrm{size}(\mathfrak{a}_i), \log(1/\varepsilon_0)).$$

Moreover, any output module R *with pseudo-basis* $(H_R, (\mathfrak{h}_i)_{i\in[r]})$ *of this latter algorithm (*$\mathrm{Round}_{\mathrm{Lat}}$*) satisfies* $\mathrm{size}(H_R), \max_i \mathrm{size}(\mathfrak{h}_i) \leq \mathrm{poly}(\mathrm{size}(\mathbf{B}_M, (\mathfrak{a}_i)_{i\in[r]}), \log(1/\varepsilon_0))$.

Proof. **Correctness.** To prove correctness, we need to show that the output R is a rank r module lattice with coefficients in K. The output R is a rank r module lattice by definition (as it has a pseudo-basis $(\mathbf{B}_R, (\mathfrak{a}_i))$). This is forced by the repeated sampling until linearly independence in line 5. Note that the choice of ς in combination with Lemma 2.14 and the α-balancedness of M implies

$$\varsigma > 3 \cdot 2^n \cdot \sqrt{n} \cdot \lambda_n(M). \tag{13}$$

For the coefficients, we observe instead the matrix $\mathbf{B}_R^{-1} = \mathbf{B}_M^{-1}\mathbf{B}_N \in \mathcal{O}_K^{r\times r}$. Since $v_i \in M$, we can write $v_i = \mathbf{B}_M \cdot w_i$ where $w_i \in \mathfrak{a}_1 \times \cdots \times \mathfrak{a}_r \subseteq \mathcal{O}_K^r$. Hence putting $W = (w_1, \ldots, w_r)$ (where the w_i are columns), we have $\mathbf{B}_N = \mathbf{B}_M W$ and thus $\mathbf{B}_R^{-1} = \mathbf{B}_M^{-1}\mathbf{B}_N = W$. Hence, by the formula for the inverse via the adjugate, we see that $\mathbf{B}_R = \frac{1}{\det_{K_{\mathbb{R}}}(W)}\mathrm{adj}(W)$ which must have coefficients in $\frac{1}{\det_{K_{\mathbb{R}}}(W)}\mathcal{O}_K^{r\times r}$. Hence, $\mathbf{B}_R$ and thus H_R can be represented by rational numbers (in the field K, and hence, by picking any basis of K, by rational numbers in $\mathbb{Q}$). By scaling, one can demand the ideals to be integral, see also the text on Module-HNF in Section 2.3.3.

Approximation of Algorithm 2 with small statistical distance. Next, we prove that the output distribution of Algorithm 2, $\mathrm{Round}_{\mathrm{Lat}}^{\mathrm{Perf}}$, can be approximated by an efficient algorithm $\mathrm{Round}_{\mathrm{Lat}}$ using bit-operations and within statistical distance ε_0. There are two lines in Algorithm 2 that cannot be computed with bit-operations due to their real or infinite nature: Line 3 and line 5. The former, because a computer cannot sample from a uniform ball, and the latter because a computer cannot process arbitrarily large elements of the lattice M.

We resolve the first issue by discretizing the set $\mathcal{C} = \{x \in K_{\mathbb{R}} \mid \|x_\sigma\| = T \text{ for all } \sigma\}$, into the finite set $\ddot{\mathcal{C}}$, in such a way that $\mathcal{C} = \ddot{\mathcal{C}} + F$ with F some fundamental domain satisfying $\|f\| \leq \frac{\varsigma\varepsilon_0^2}{32r^3d}$ for all $f \in F$ (with $r = \mathrm{rank}(M)$ and $d = \deg(K)$). I.e., every element $c \in \mathcal{C}$ can uniquely be written as $c = \ddot{c} + f$ with $\ddot{c} \in \ddot{\mathcal{C}}$ and $f \in F$; with $\mathrm{vol}(F) = \frac{\mathrm{vol}(\mathcal{C})}{|\ddot{\mathcal{C}}|}$. One can efficiently sample in $\ddot{\mathcal{C}}$ by sampling $x \in K_{\mathbb{R}}$ per embedding separately.

Hence, the statistical distance of the two methods of sampling $v_i \leftarrow \mathcal{G}_{M,\varsigma,c}$, with $c = (\underbrace{0, \ldots, 0}_{i-1}, \hat{c}, \underbrace{0, \ldots, 0}_{r-i})$, where $\hat{c} \leftarrow \mathcal{C}$ or $\hat{c} \leftarrow \ddot{\mathcal{C}}$ can then be computed by (where the statistical

distance, or, equivalently, the norm $\|\cdot\|_1$, is over $m \in M$)

$$\left\| \frac{1}{\mathrm{vol}(\mathcal{C})} \int_{\hat{c}\in\mathcal{C}} \mathcal{G}_{M,\varsigma,c} d\hat{c} - \frac{1}{|\ddot{\mathcal{C}}|} \sum_{\hat{c}\in\ddot{\mathcal{C}}} \mathcal{G}_{M,\varsigma,c} \right\|_1 = \left\| \frac{1}{\mathrm{vol}(\mathcal{C})} \int_{f\in F} \sum_{\hat{c}\in\ddot{\mathcal{C}}} \mathcal{G}_{M,\varsigma,c+f} - \mathcal{G}_{M,\varsigma,c} df \right\|_1$$
$$\leq \frac{1}{\mathrm{vol}(\mathcal{C})} \int_{f\in F} \sum_{\hat{c}\in\ddot{\mathcal{C}}} \|\mathcal{G}_{M,\varsigma,c} - \mathcal{G}_{M,\varsigma,c+f}\|_1 df \leq \frac{1}{\mathrm{vol}(\mathcal{C})} \int_{c\in\mathcal{C}} 4\sqrt{\frac{n\|f\|}{\varsigma}} \leq \varepsilon_0/(2r)$$

where the last inequality follows from the result [PS21, Lemma 2.3] by Pellet-Mary and Stehlé. The premise of this result, $\eta_{1/2}(M) \leq \varsigma/2$, follows from [MR07, Lemma 3.3], as $\eta_{1/2}(M) \leq \sqrt{\frac{\log(2n(1+2))}{\pi}} \cdot \lambda_n(M) \leq 2rd\lambda_n(M) \leq \varsigma/2$ (see Equation (13), and where we use that $\sqrt{\log(6x)/\pi} \leq 2x$ for all $x > 0$).

We resolve the second issue by using an algorithm computing an approximation of the discrete Gaussian as in [FPS+23a, Lemma A.7] (see also [GPV08, Theorem 4.1]) with error $\varepsilon_0/(12r)$. This means that, instead of sampling $v_i \leftarrow \mathcal{G}_{M,\varsigma,c}$ in line 5, we sample $v_i \leftarrow \widehat{\mathcal{G}}_{M,\varsigma,c}$ for which

$$\|\widehat{\mathcal{G}}_{M,\varsigma,c} - \mathcal{G}_{M,\varsigma,c}\|_1 < \varepsilon_0/(12r),$$

for which it additionally holds that $\|v_i - c\| \leq \varsigma\sqrt{\log(12r/\varepsilon_0) + 4n}$.

At the end each loop occurrence, at line 5, a v_i is sampled that is a discrete Gaussian *conditioned* on being independent to the earlier samples $(v_1, \ldots, v_{i-1})$. By Lemma A.3, the success probability of a single try of v_i must be bounded from below by $1/3$ (by the fact that $\varsigma > 3 \cdot \sqrt{n} \cdot \lambda_n(M)$, see Equation (13)). Hence, by Lemma 2.23, the statistical distance between the two *conditioned samples* (meaning, repetition until success), must be upper bounded by

$$2 \cdot (1/3)^{-1} \cdot \|\widehat{\mathcal{G}}_{M,\varsigma,c} - \mathcal{G}_{M,\varsigma,c}\|_1 \leq \varepsilon_0/(2r).$$

For fixed input M, write $\mathrm{Round}^{\mathrm{Perf}}_{\mathrm{Lat}}(M)$ for the output distribution of Algorithm 2 over rank r modules represented by $(H_R, (\mathfrak{h}_i)_{i\in[r]})$. And, for the same fixed input, write $\mathrm{Round}_{\mathrm{Lat}}(M)$ for the same output distribution of Algorithm 2 except that $\hat{c}$ is sampled according to a discrete circle and $v_i \leftarrow \widehat{\mathcal{G}}_{M,\varsigma,c}$ is sampled from an approximate discrete Gaussian. Then we have, by the fact that the loop in line 2 consists of r repetitions,

$$\|\mathrm{Round}^{\mathrm{Perf}}_{\mathrm{Lat}}(M) - \mathrm{Round}_{\mathrm{Lat}}(M)\| \leq r \cdot (\varepsilon_0/(2r) + \varepsilon_0/(2r)) = \varepsilon_0$$

Hence, indeed, the output distribution $\mathrm{Round}^{\mathrm{Perf}}_{\mathrm{Lat}}(M)$ of Algorithm 2 can be approximated within statistical distance ε_0. The bound on the run time is shown at the very end of this proof.

Bound on size of H_R and $\mathfrak{h}_i$. Due to the polynomial time algorithm for the Module-HNF by Biasse and Fieker [BF12], it is sufficient to find a polynomial size bound on $\mathbf{B}_R$ in order to bound the sizes of H_R and $\mathfrak{h}_i$, since

$$\mathrm{size}(H_R, (\mathfrak{h}_i)_{i\in[r]}) \leq \mathrm{poly}(\mathbf{B}_R, (\mathfrak{a}_i)_{i\in[r]}).$$

We bound the size of $\mathbf{B}_R \in \frac{1}{\det_{K_\mathbb{R}}(W)} \mathcal{O}_K^{r\times r} \subseteq K_\mathbb{R}^{r\times r}$ (with $W = \mathbf{B}_R^{-1}$, see the beginning of this proof) by proving an upper bound on the length of the vectors it consists of, as well as an upper bound on the (norm of the) denominators of its coefficients.

We have, by a similar computation as in Lemma 3.2 (with $\delta = n^3 \cdot \varsigma \cdot \sqrt{\mu}/T \leq 1/(8n)$, writing $\mu = \sqrt{\log(12r/\varepsilon_0)}$), using that the approximate discrete Gaussian samples indeed always satisfy $e_{ij} \leq n^2 \cdot \sqrt{\log(12r/\varepsilon_0)} \cdot \varsigma = n^2\mu\varsigma$, (contrarily to the perfect discrete Gaussian samples, for which this happens with high probability)

$$\|\mathbf{B}_R\| = \|\mathbf{B}_N^{-1}\mathbf{B}_M\| \leq \|\mathbf{B}_N^{-1}\|\|\mathbf{B}_M\| \leq \frac{1}{T}(1 + 2\delta)\|\mathbf{B}_M\|.$$

Additionally, again, by similar determinant computations as in Lemma 3.2,

$$\begin{aligned}|\det(W)| = |\det(\mathbf{B}_M^{-1}\mathbf{B}_N)| = |\det(M)^{-1}| \cdot |\det(\mathbf{B}_N)| \le \det(M)^{-1} \cdot T(1+2n\delta)\\ \le 2 \cdot \det(M)^{-1} \cdot T.\end{aligned}$$

Since $W \in \mathcal{O}_K^{r\times r}$, we have $\det(W) \in \mathbb{Z}$ and hence we see that $|\det(W)| = |N(\det_{K_\mathbb{R}}(W))| \le 2\det(M)^{-1} \cdot T$.

Hence, the size of $\mathbf{B}_R$ is bounded by $\mathrm{poly}(\mathrm{size}(\mathbf{B}_M), \log(T)) = \mathrm{poly}(\mathrm{size}(\mathbf{B}_M), \log(1/\varepsilon_0))$, which proves the claim.

Run-time. We finish the proof that the approximated algorithm is efficient. For lines 1-6, the efficiency follows from the efficiency of sampling the discrete circle and the efficiency of the approximate discrete Gaussian algorithm as in [FPS+23b, Lemma A.7]. The fact that the sample from the discrete Gaussian is required to be conditioned on being linearly independent of earlier samples, does not give a significant overhead, by Lemma A.3. We can conclude that these lines run in time $\mathrm{poly}(\mathrm{size}(\mathbf{B}_M), \max_i \mathrm{size}(\mathfrak{a}_i), \log(1/\varepsilon_0))$.

An additional note on computing this (approximate) discrete Gaussian, is that before sampling $v_i \leftarrow \hat{\mathcal{G}}_{M,\varsigma,c}$, the basis of M is first LLL-reduced (for this purpose only), in order to have smaller basis elements. This LLL reduction does not need to be module-compatible, and an efficient algorithm to find such an LLL reduced basis for approximate bases is described in [BP89; BK96]. This allows for computing a $\mathbb{Z}$-basis $(m_1, \dots, m_n)$ of the lattice M satisfying $\|m_i\| \le 2^n \lambda_i(M)$ for all $i \in [n]$ [BK96, Corollary 4.1].

Line 7 is just stacking columns and causes no real overhead. The last line, line 8, involves the computation of a Hermite normal form, which can be computed in polynomial time [BF12]. Hence the overall bit-wise approximation algorithm (of Algorithm 2) runs within polynomial time in $\mathrm{size}(\mathbf{B}_M), \mathrm{size}(\mathfrak{a}_i)$. □

Lemma 3.4 (The output distribution $\mathrm{Round}^{\mathrm{Perf}}_{\mathrm{Lat}}$ of Algorithm 2 does not depend on the pseudo-basis representation of M)**.** *Let $\alpha \in \mathbb{R}_{\ge 1}$ and let $\mathrm{Round}^{\mathrm{Perf}}_{\mathrm{Lat}}(\mathbf{B}_M, (\mathfrak{a}_i)_{i\in[r]})$ be the output distribution of Algorithm 2 on input $(\mathbf{B}_M, (\mathfrak{a}_i)_{i\in[r]})$. Let $(\mathbf{B}_M, (\mathfrak{a}_i)_{i\in[r]})$ and $(\mathbf{B}'_M, (\mathfrak{a}'_i)_{i\in[r]})$ be two pseudo-basis representations of an α-balanced module lattice M. Then*

$$\mathrm{Round}^{\mathrm{Perf}}_{\mathrm{Lat}}(\mathbf{B}_M, (\mathfrak{a}_i)_{i\in[r]}) = \mathrm{Round}^{\mathrm{Perf}}_{\mathrm{Lat}}(\mathbf{B}'_M, (\mathfrak{a}'_i)_{i\in[r]})$$

Proof. Since the sample of $v_i \leftarrow \mathcal{G}_{M,\varsigma,c}$ in line 5 is independent on the choice of pseudo-basis of M, the distribution of the free module N in line 7 is also independent on this pseudo-basis choice. Therefore, the module-lattice R is independent of this pseudo-basis choice (but its representation $(\mathbf{B}_R := \mathbf{B}_N^{-1}\mathbf{B}_M, (\mathfrak{a}_i)_{i\in[r]})$ generally not). As the output is the Hermite normal form basis of R (which is unique for each module lattice), the output is indeed independent of the pseudo-basis choice of the module M. □

Lemma 3.5 ($\mathrm{Round}^{\mathrm{Perf}}_{\mathrm{Lat}}$ preserves short-vector problems)**.** *Let R be a module lattice produced as the output of Algorithm 2 with input M. Then, given a vector $v \in R$ satisfying $\|v\| \le \gamma\lambda_1(R)$ (respectively $\|v\| \le \gamma' \det(R)^{1/(dr)}$), the vector $m = \mathbf{B}_N v \in M$ satisfies*

$$\|m\| \le 2\gamma\lambda_1(M) \text{ (respectively } \|m\| \le 2\gamma' \det(M)^{1/(dr)}),$$

with probability at least $1 - (\varepsilon_0)^{n^4}$.

Proof. By Lemma 3.2, we have $\|\mathbf{B}_N\|_2 \le (1 + \frac{1}{8n})T$, $\|\mathbf{B}_N^{-1}\|_2 \le (1 + \frac{1}{4n})\frac{1}{T}$ and $|\det(\mathbf{B}_N^{-1})|^{1/n} \le (1 + \frac{1}{4})T^{-1}$, with probability at least $1 - (\varepsilon_0)^{n^4}$.

Since $\mathbf{B}_N$ is a module isomorphism from R to M (and thus $\mathbf{B}_N^{-1}$ from M to R), we obtain that for any $v \in R\backslash\{0\}$ attaining $\lambda_1(R)$, we have $\mathbf{B}_N v \in M\backslash\{0\}$ and hence

$$\lambda_1(M) \le \|\mathbf{B}_N v\| \le T(1 + 1/(8n))\|v\| = T\left(1 + \frac{1}{8n}\right)\lambda_1(R),$$

and similarly, for $m \in M\backslash\{0\}$ attaining $\lambda_1(M)$,

$$\lambda_1(R) \leq \|\mathbf{B}_N^{-1} m\| \leq \|\mathbf{B}_N^{-1}\| \|m\| \leq \frac{1}{T} \cdot \left(1 + \frac{1}{4n}\right) \cdot \lambda_1(M).$$

After these computations, we turn back to the original task at hand: showing that a short vector in R gives means of computing a short vector of M. Suppose v satisfies $\|v\| \leq \gamma\lambda_1(R)$, i.e., $v = \mathbf{B}_R w$ with $w \in \mathfrak{a}_1 \times \ldots \times \mathfrak{a}_r$. Let now $m = \mathbf{B}_N v = \mathbf{B}_N \mathbf{B}_N^{-1} \mathbf{B}_M w = \mathbf{B}_M w \in M$. Then by the computations on the norms on the matrix, we obtain

$$\|m\| = \|\mathbf{B}_N v\| \leq T(1 + \frac{1}{8n})\|v\| \leq \gamma \cdot T(1 + \frac{1}{8n}) \cdot \lambda_1(R) \leq \gamma \cdot (1 + \frac{1}{8n})(1 + \frac{1}{4n})\lambda_1(M).$$

For the determinant variant, the same type of sequence of inequalities occurs:

$$\begin{aligned}\|m\| = \|\mathbf{B}_N v\| &\leq T(1 + \frac{1}{8n})\|v\| \leq \gamma \cdot T(1 + \frac{1}{8n}) \cdot \det(R)^{1/n} \\ &\leq \gamma \cdot (1 + \frac{1}{8n})(1 + \frac{1}{4}) \cdot \det(M)^{1/n}.\end{aligned}$$

Here we use that $\det(R) = \det(\mathbf{B}_N^{-1}\mathbf{B}_M) = |\det(\mathbf{B}_N)^{-1}||\det(\mathbf{B}_M)| \leq T^{-1}(1 + \frac{1}{4})\det(M)$. Now we use that $(1 + 1/(8n))(1 + 1/(4n)) \leq (1 + 1/(8n))(1 + 1/4) \leq 2$ to obtain the final claim. □

Lemma 3.6 ($\mathrm{Round}_{\mathrm{Lat}}$ preserves short-vector problems)**.** *Let R be the module lattice represented by the output of the approximation $\mathrm{Round}_{\mathrm{Lat}}$ of Algorithm 2 with input M. Then, if $v \in R$ satisfying $\|v\| \leq \gamma\lambda_1(R)$ respectively $\|v\| \leq \gamma' \det(R)^{1/(dr)}$ allows for finding $m \in M$ satisfying*

$$\|m\| \leq 2\gamma\lambda_1(M) \text{ respectively } \|m\| \leq 2\gamma' \det(M)^{1/(dr)},$$

with probability 1.

Proof. This follows from the proof of Lemma 3.5 and the fact that (as can be seen in Lemma 3.3) the tails of the discrete Gaussians are cut in $\mathrm{Round}_{\mathrm{Lat}}$, which takes away the probability that arbitrarily large samples from these Gaussians can cause the short-vector problems not to be preserved. □

Lemma 3.7 ($\mathrm{Round}_{\mathrm{Lat}}^{\mathrm{Perf}}$ is 1/2-Hölder continuous)**.** *Let $\alpha \in \mathbb{R}_{\geq 1}$, $\varepsilon_0 \in (0, 1/2)$ and let M, M' be α-balanced module lattices of rank r. Denote $\mathcal{D}(M)$ for the output distribution of Algorithm 2 on input $(\mathbf{B}_M, (\mathfrak{a}_i)_{i\in[r]})$, a pseudo-basis of M.*

Then we have

$$\|\mathcal{D}(M) - \mathcal{D}(M')\|_1 \leq 92n^3 \cdot \sqrt[4]{\log(12r/\varepsilon_0)}\sqrt{d(M, M')},$$

where $d(M, M') := \min(\|\phi - I\|_2, \|\phi^{-1} - I\|_2)$ if there exists a module isomorphism $\phi : M \to M'$ between M and M' and $d(M, M') = \infty$ otherwise.

Proof. Assume that $M' = \phi M$, where $\phi \in K_{\mathbb{R}}^{r\times r}$ serves as a module isomorphism (and is thus invertible); otherwise the lemma is trivially true. We may without loss of generality assume that $\det(\phi) = 1$ (and hence $\det(M') = \det(M)$), by replacing M' by $\det(\phi)^{-1/(rd)}M'$ and ϕ by $\phi \cdot \det(\phi^{-1/(rd)})$. This holds because Algorithm 2 is scaling-independent, i.e., it does not matter whether M or qM is the input for $q \in \mathbb{R}_{>0}$.

We use that $d(M, M') = \min(\|\phi - I\|_2, \|\phi^{-1} - I\|_2)$ (where M' is scaled so that $\det(M) = \det(M')$). Then, for the same c, the samples $(v_i)_{i\in[r]}$ from $G_{M,\varsigma,c}$ (for Algorithm 2 on input M) and $(\phi v_i)_{i\in[r]}$ from $G_{\phi M,\varsigma,c}$ (for Algorithm 2 on input $M' = \phi M$) lead to the same output module. Indeed, a pseudo-basis of the output module R in the first case can be described by $(\mathbf{B}_R := \mathbf{B}_N^{-1}\mathbf{B}_M, (\mathfrak{a}_i)_{i\in[r]})$ with $\mathbf{B}_N$ is constructed by stacking v_i; whereas in the second case it

can be described by $((\phi\mathbf{B}_N)^{-1}(\phi\mathbf{B}_M), (\mathfrak{a}_i)_{i\in[r]})$, which is equal to the pseudo-basis in the first case since $(\phi\mathbf{B}_N)^{-1}(\phi\mathbf{B}_M) = \mathbf{B}_N^{-1}\mathbf{B}_M$.

Hence, by the data processing inequality, the total variation distance in the output distribution of Algorithm 2 on input M and M' can be bounded above by the total variation distance between $G_{M,\varsigma,c}$ and $\phi^{-1}G_{\phi M,\varsigma,c}$, which are both distributions over M (where we mean with $\phi^{-1}G_{\phi M,\varsigma,c}$ the distribution obtained by multiplying the output of $G_{\phi M,\varsigma,c}$ by ϕ^{-1}).

By rewriting, one obtains that $\phi^{-1}G_{\phi M,\varsigma,c}$ is equal to the distribution $G_{M,\phi^{-1}\varsigma,\phi^{-1}c}$, where $\phi^{-1}\varsigma$ serves as a sort of variance matrix. The probability of sampling v from $G_{M,\phi^{-1}\varsigma,\phi^{-1}c}$ is proportional to $\exp(-\|\phi/\varsigma\cdot(v-\phi^{-1}c)\|^2)$. We use a result from Stehlé and Pellet-Mary [PS21, Lemma 2.4], where we instantiate $\mathbf{S}_1 = \varsigma, \mathbf{S}_2 = \phi^{-1}\varsigma, \mathbf{c}_1 = c$ and $\mathbf{c}_2 = \phi^{-1}c$ in [PS21, Lemma 2.4]; we use here that, by the definition of ς we have $\eta_{1/2}(M) \le \sqrt{\frac{\log(6n)}{\pi}}\lambda_n(M) \le \varsigma$ (see [MR07, Lemma 3.3]) and similarly for M' (see also [PS21, Equation (2.1)]). This yields the following bound:

$$\|G_{M,\phi^{-1}\varsigma,\phi^{-1}c} - G_{M,\varsigma,c}\| \le 4\sqrt{n}\left(\sqrt{\|\mathbf{S}_2^{-1}\mathbf{S}_1 - I_n\|} + \sqrt{\mathbf{S}_2^{-1}(\mathbf{c}_1-\mathbf{c}_2)}\right) \tag{14}$$

$$\le 4\sqrt{n}\left(\sqrt{\|\phi - I\|} + \sqrt{\|\varsigma^{-1}(\phi c - c)\|}\right) \tag{15}$$

$$\le 4\sqrt{n}\sqrt{\|\phi - I\|}(1+\sqrt{nT/\varsigma}) \tag{16}$$

Note, though, that in line 5, instead the samples are *conditional* on being linearly independent of the former samples. By Lemma A.3, the success probability of sampling such v_i being linearly independent to the former samples is at least $1/3$. Hence, by Lemma 2.23 the statistical distance between the *conditioned* Gaussian samples must be upper bounded by

$$2\cdot(1/3)^{-1}\cdot\|G_{M,\phi^{-1}\varsigma,\phi^{-1}c} - G_{M,\varsigma,c}\| \le 24\sqrt{n}\sqrt{\|\phi-I\|}(1+\sqrt{nT/\varsigma}). \tag{17}$$

Hence, for $r \le rd = n$ of such samples, the total variation distance can be bounded by, using that $nT/\varsigma = 8n^5\cdot\mu$ (with $\mu = \sqrt{\log(12r/\varepsilon_0)}$) and $24\sqrt{n}(1+\sqrt{8n^5\cdot\mu}) \le 16n^3\cdot\sqrt{\mu}$ for $n \ge 1$, we obtain a total variation distance of

$$\|\mathcal{D}(M) - \mathcal{D}(M')\|_1 = \|\mathcal{D}(M) - \mathcal{D}(\phi M)\|_1 \le 92n^3\sqrt{\mu}\sqrt{\|\phi - I\|}.$$

By analogously comparing the Gaussians over M' and $\phi^{-1}M' = M$, one arrives at the exact same bound, except that $\|\phi - I\|$ is replaced by $\|\phi^{-1} - I\|$. Hence, replacing $\mu = \sqrt{\log(12r/\varepsilon_0)}$ the claim of the lemma follows. □

4 Self-reducibility in the bulk: analytic tools

The goal of this section is to prove an explicit, quantitative Hecke equidistribution theorem for test functions concentrated at arbitrary lattices. It is one of the main drivers of our reduction, but the result is of independent interest.

First, take a module lattice $L_{z,\mathfrak{a}}$ for $z \in \mathrm{GL}_r(K_{\mathbb{R}})$ and $\mathfrak{a}$ in the class group, as in Section 2.3.2. We define a probability measure on $X_{r,\mathfrak{a}}$, extended trivially to X_r, that is concentrated around $L_{z,\mathfrak{a}}$. It is given by an "initial distribution" function φ_z.

Applying Hecke operators $T_{\mathfrak{p}}$ to φ_z corresponds to randomizing $L_{z,\mathfrak{a}}$ or a geometrically close lattice by taking certain sublattices with index $N(\mathfrak{p})$. As $\mathfrak{p}$ grows large, the measures we obtain spread out to the whole of X_r and start to converge to the uniform probability measure μ. In other words, the sublattices of $L_{z,\mathfrak{a}}$ of large index equidistribute.

For our purposes, it is essential to understand the rate of convergence to the uniform measure. We do so by applying the bounds on Hecke eigenvalues given in Section 2.7, importing the quantitative equidistribution results of [BDP+20], and bounding the L^2-norm of the initial

distribution concentrated around $L_{z,\mathfrak{a}}$. The latter depends heavily on the balancedness of the lattice (recall Definition 2.8).

Theorem 3. *Assume ERH for the L-function of every Hecke character of K of trivial modulus. Let φ_z be the function defined in Definition 4.3, with defining parameters $\sigma \leq 1/\sqrt{d}$ and $t = 1$. Let B, κ be positive parameters such that $\kappa \geq \sigma^{-1}\sqrt{r_u/4\pi}$ and $B \gg \log|\Delta_K| + d$, with large enough implied constant. Recall that $\mathcal{P}(B)$ is the set of prime ideals of K with norm up to B. Assume that the associated lattice $L_{z,\mathfrak{a}}$ is α-balanced. Then*

$$\left\| T_{\mathcal{P}(B)}\varphi_z - \mu_{\mathrm{Riem}}(X_r)^{-1} \cdot \mathbf{1}_{X_r} \right\|_{X_r}^2 \ll \max(r_u(\log r_u)^3, 1/\sigma)^{r_u} \cdot (C_1^2 + e^{-2(\kappa/\sqrt{d})^2}) + (rd)^2 \cdot B^{-3/4}\log(B)^2 \cdot C_2^2,$$

where

$$C_1 = O\left(\frac{\log(B)\log[B^d \cdot |\Delta_K| \cdot (4 + 2\pi\kappa/\sqrt{d})^d]}{\sqrt{B}}\right)$$

and

$$C_2 \leq \exp\left(\frac{r^3 d}{6}\log\alpha + r^2\log|\Delta_K| + \frac{d}{2}\log d + O(r^2 d\log r + \log\log|\Delta_K|)\right).$$

Remark 4.1. For our purposes, Theorem 3 is strong enough when the starting lattice is α-balanced with α at most polynomial in d (see Section 10 for details). In fact, as explained in Section 1.3, we should not expect it to apply to very imbalanced lattices.

4.1 Initial distribution

Define the natural projection

$$\pi_{\mathfrak{a}} \colon Y_r \to X_{r,\mathfrak{a}}. \tag{18}$$

The initial distribution will be the push-forward under $\pi_{\mathfrak{a}}$ of a distribution on Y_r, which we define from its density with respect to μ_{Riem}. The latter is informally constructed by splitting GL_r into SL_r and GL_1 and taking characteristic functions or bump functions on neighborhoods of the identity on each part. For this, we recall the functions ρ and τ from Section 2.6.3, measuring distance on the SL_r and GL_1-parts, respectively.

Let $t > 0$ and $\sigma > 0$. We define $\tilde{f} \in L^2(Y_r)$ by

$$\tilde{f}(x) = \mathbf{1}_{[0,t]}(\rho(x))\exp(-\frac{\pi}{\sigma^2}\tau(x)), \tag{19}$$

and let $I_f = \int_{Y_r} \tilde{f} d\mu_{\mathrm{Riem}}$. Notice that the first factor is the characteristic function of the ball $B(t)$, as defined in 2.6.3. Moreover, $\tilde{f}$ has rapid decay, which implies that all integral manipulations appearing below are valid and there are no convergence issues.

Lemma 4.2. *We have that*

$$I_f = \int_{Y_r} \tilde{f} d\mu_{\mathrm{Riem}} = \frac{\mu_{\mathrm{Riem}}(B(t))}{\mu_{\mathrm{Riem}}(\mathrm{SU}_r(K_{\mathbb{R}}))}\left(\frac{\sigma}{\sqrt{r}}\right)^{r_u}. \tag{20}$$

Proof. Let

$$S \colon K_{\mathbb{R}}^{\times} \to K_{\mathbb{R}}^{\times}\,\mathrm{U}_r(K_{\mathbb{R}})$$

be a section of the determinant $\mathrm{GL}_r(K_{\mathbb{R}}) \to K_{\mathbb{R}}^{\times}$ that takes values in $K_{\mathbb{R}}^{\times}\,\mathrm{U}_r(K_{\mathbb{R}})$. This latter condition is useful for employing the invariance properties of ρ. Using the integration formula

(5), we compute that

$$\begin{aligned}
&\int_{Y_r} \tilde{f}(x)\, d\mu_{\mathrm{Riem}}(x) \\
&= \int_{x\in Y_r} \mathbf{1}_{[0,t]}(\rho(x)) \exp(-\frac{\pi}{\sigma^2}\tau(x))\, dx \\
&= r^{\frac{-r_u}{2}} \int_{\delta\in Y_1} \left(\int_{x\in\Delta^{-1}(\delta)} \mathbf{1}_{[0,t]}(\rho(x)) \exp(-\frac{\pi}{\sigma^2}\tau(x)) dx \right) d\delta.
\end{aligned}$$

Plugging in definitions and using the isometry between Y_1 and H given in section 2.6.1, the expression above equals

$$\begin{aligned}
&r^{\frac{-r_u}{2}} \int_{\delta\in Y_1} \left(\int_{x\in\Delta^{-1}(\delta)} \mathbf{1}_{[0,t]}(\rho(x))\, dx \right) \exp(-\frac{\pi}{\sigma^2}\|\log|\delta|\|_H^2)\, d\delta \\
&= r^{\frac{-r_u}{2}} \int_{\delta\in Y_1} \mu_{\mathrm{Riem}}(B(t)S(\delta)/\operatorname{SU}_r(K_{\mathbb{R}})) \exp(-\frac{\pi}{\sigma^2}\|\log|\delta|\|^2)\, d\delta \\
&= r^{\frac{-r_u}{2}} \int_{\delta\in Y_1} \frac{\mu_{\mathrm{Riem}}(B(t))}{\mu_{\mathrm{Riem}}(S(\delta)\operatorname{SU}_r(K_{\mathbb{R}})S(\delta)^{-1})} \exp(-\frac{\pi}{\sigma^2}\|\log|\delta|\|^2)\, d\delta \\
&= r^{\frac{-r_u}{2}} \int_{x\in H} \frac{\mu_{\mathrm{Riem}}(B(t))}{\mu_{\mathrm{Riem}}(\operatorname{SU}_r(K_{\mathbb{R}}))} \exp(-\frac{\pi}{\sigma^2}\|x\|^2) dx
\end{aligned}$$

The claim follows from a standard formula for the integral of a Gaussian. □

For $z \in Y_r$, notice that $\int_{Y_r} \tilde{f}(z^{-1}x) = I_f$ by invariance of the measure. Thus, writing

$$f_z(x) = I_f^{-1} \tilde{f}(z^{-1}x), \tag{21}$$

we have that $f_z \cdot \mu_{\mathrm{Riem}}$ defines a probability measure on Y_r, concentrated around the point z.

Definition 4.3. Let the *initial distribution* around a point $z \in X_{r,\mathfrak{a}}$ be $\varphi_z = (\pi_{\mathfrak{a}})_* f_z$. Explicitly,

$$\varphi_z(w) = \sum_{\gamma\in \mathrm{GL}_r(\mathcal{O}_K,\mathfrak{a})} f_z(\gamma w), \tag{22}$$

and we note the dependence on $\mathfrak{a}$ and on the two parameters, σ and t, which we leave out of notation for simplicity. It extends trivially to X_r by setting its value to be 0 on all other components.

Lemma 4.4. *The measure $\varphi_z \cdot \mu_{\mathrm{Riem}}$ is a probability measure on X_r.*

Proof. Indeed, we can compute that

$$\int_{X_r} \varphi_z(w)\, d\mu_{\mathrm{Riem}} = \int_{X_{r,\mathfrak{a}}} \varphi_z(w)\, d\mu_{\mathrm{Riem}} = \int_{Y_r} f_z(w)\, d\mu_{\mathrm{Riem}} = 1$$

using the formal integration rule

$$\int_{\Gamma\backslash X} \sum_{\gamma\in\Gamma} f(\gamma x)\, dx = \int_X f(x)\, dx.$$

The latter is often called the unfolding method and is valid in all cases we consider. □

4.1.1 Determinant projection of the initial distribution

We now compute the projection of φ_z onto the space $L^2_{\det}(X_{r,\mathfrak{a}})$ by applying the results in Section 2.6. For this, let $\varphi_{z,1} = \mu_{\mathrm{Riem}}(\Delta_{\mathfrak{a}}^{-1}(1))^{-1}\Delta'_{\mathfrak{a}}\varphi_z$, so that, by (7),

$$\pi_{\det}\varphi_z = \Delta_{\mathfrak{a}}^{*}\varphi_{z,1}. \tag{23}$$

Lemma 4.5. *For the initial distribution defined in (22), we have*

$$\Delta'_{\mathfrak{a}}\varphi_z(\delta) = \sum_{\xi\in\mathcal{O}_K^{\times}} \sigma^{-r_u}\exp(-\frac{\pi}{\sigma^2}\|\log|\delta| + \log|\xi| - \log|\det(z)|\|_H^2). \tag{24}$$

The measure $\Delta'_{\mathfrak{a}}\varphi_z \cdot \mu_{\mathrm{Riem}}$ is a probability measure on $X_{1,\mathfrak{a}}$.

Proof. Recall the description (6) of $\Delta^{-1}(\delta)$ and that

$$\Delta_{\mathfrak{a}}^{-1}(\delta) = \Gamma_{\mathfrak{a}}\backslash\Gamma_{\mathfrak{a}}\Delta^{-1}(\delta).$$

For each $\xi \in \mathcal{O}_K^{\times}$, choose an element $\gamma(\xi) \in \Gamma_{\mathfrak{a}}$ such that $\det(\gamma(\xi)) = \xi$. Using this, we parametrize

$$\Gamma_{\mathfrak{a}}\Delta_{\mathfrak{a}}^{-1}(\delta) = \bigcup_{\xi\in\mathcal{O}_K^{\times}} \gamma(\xi)\Delta_{\mathfrak{a}}^{-1}(\delta).$$

The unfolding method with respect to the measure μ_{Riem} now implies that

$$\begin{aligned}\Delta'_{\mathfrak{a}}\varphi_z(\delta) &= \int_{x\in\Delta_{\mathfrak{a}}^{-1}(\delta)} \varphi_z(x)\,dx = \int_{\Gamma_{\mathfrak{a}}\Delta_{\mathfrak{a}}^{-1}(\delta)} f_z(x)\,dx \\ &= r^{-\frac{r_u}{2}} I_f^{-1} \sum_{\xi\in\mathcal{O}_K^{\times}} \int_{\Delta_{\mathfrak{a}}^{-1}(\delta)} \tilde{f}(z^{-1}\gamma(\xi)x)\,dx.\end{aligned}$$

The same computation as for I_f and the fact that

$$\mu_{\mathrm{Riem}}(z\gamma(\xi)B(t)) = \mu_{\mathrm{Riem}}(B(t))$$

now imply that

$$\int_{\Delta^{-1}(\delta)} \tilde{f}(z^{-1}\gamma(\xi)x)\,dx \quad = \quad \frac{\mu_{\mathrm{Riem}}B(t)}{\mu_{\mathrm{Riem}}(\mathrm{SU}_r(K_{\mathbb{R}}))}\exp(-\frac{\pi}{\sigma^2}\|\log|\delta| \;+\; \log|\xi| \;-\; \log|\det(z)|\|_H^2)$$

Plugging in our formula for I_f, we obtain the formula in the claim. The fact that $\Delta'_{\mathfrak{a}}\varphi_z \cdot \mu_{\mathrm{Riem}}$ defines a probability measure can be checked by standard properties of the Gaussian function. □

4.2 Bound on the norm of the initial distribution

It is essential in our method to have uniform bounds on the norm $\|\varphi_z\|$. We obtain them by first reducing to a problem of counting matrices in $\Gamma_{\mathfrak{a}}$ with certain size constraints that depend on z. We then use techniques based on counting lattice points in balls, where the dependence on the lattice manifests through the appearance of successive minima.

4.2.1 Reduction to a counting problem

We first use generic notation in this section and we specialize later. Let Y be a space equipped with a measure ν. Let Γ be a discrete group acting on Y properly discontinuously. This induces an action of Γ on the space of functions on Y, defined by

$$(\gamma f)(y) = f(\gamma^{-1}y)$$

for $f\colon Y \to \mathbb{R}$, $y \in Y$ and $\gamma \in \Gamma$.

Let $\pi\colon Y \to \Gamma\backslash Y$ be the canonical projection. For a function f on Y we let $\pi_* f$ be the push-forward function on $\Gamma\backslash Y$, i.e. $\pi_* f(x) = \sum_{y\in\pi^{-1}(x)} f(y)$ for $x \in \Gamma\backslash Y$. Assume here that f is measurable and has rapid decay so that all the sums and integrals we consider converge.

Lemma 4.6. *We have* $\|\pi_* f\|^2 = \sum_{\gamma\in\Gamma} \langle f, \gamma^{-1} f\rangle_Y$.

Proof. We compute that

$$\begin{aligned}
\|\pi_* f\|^2 &= \int_{\Gamma\backslash Y} (\pi_* f(x))^2 d\nu(x) = \int_{\Gamma\backslash Y} \Big(\sum_{y\in\pi^{-1}(x)} f(y)\Big)^2 d\nu(x) \\
&= \int_{\Gamma\backslash Y} \sum_{y\in\pi^{-1}(x)} f(y) \sum_{y'\in\pi^{-1}(x)} f(y') d\nu(x) \\
&= \int_{\Gamma\backslash Y} \sum_{y\in\pi^{-1}(x)} f(y) \sum_{\gamma\in\Gamma} f(\gamma y) d\nu(x) \\
&= \int_Y f(y) \sum_{\gamma\in\Gamma} f(\gamma y) d\nu(y) = \sum_{\gamma\in\Gamma} \langle f, \gamma^{-1} f\rangle_Y.
\end{aligned}$$

□

Suppose we have a function $\tau\colon \Gamma \to \mathbb{R}_{\geq 0}$ (measure of size) such that the sets $B_f(t) = \{\gamma \in \Gamma \mid \tau(\gamma) \leq t \text{ and } \langle f, \gamma^{-1} f\rangle_Y \neq 0\}$ are finite. Define $C_f(t) = |B_f(t)|$. In addition, assume that we have a bound of the form

$$|\langle f, \gamma^{-1} f\rangle_Y| \leq F(\tau(\gamma))$$

for some smooth function $F\colon \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$.

Corollary 4.7. *In the notation above, we have*

$$\|\pi_* f\|^2 \leq (F \cdot C_f)(\infty) + \int_0^\infty C_f(t)(-F'(t))\, dt. \tag{25}$$

Proof. Since $C_f(t)$ is clearly monotone, we may use the Riemann–Stieltjes integral to state the inequality

$$\Big| \sum_{\substack{\gamma\in\Gamma \\ \tau(\gamma)\leq T}} \langle f, \gamma^{-1} f\rangle_Y \Big| \leq \sum_{\gamma\in B_f(T)} F(\tau(\gamma)) = \int_0^T F(t)\, dC_f(t),$$

for any $T > 0$. Integration by parts gives

$$\int_0^T F(t)\, dC_f(t) = F(T+)C_f(T+) - F(0-)C_f(0-) - \int_0^T C_f(t)F'(t)\, dt.$$

Finally, assuming the quantities below converge, letting $T \to \infty$, we obtain the claim. □

We now specialize the discussion to $Y = Y_r$ with the measure $\nu = \mu_{\mathrm{Riem}}$, the function $f = f_z$, the discrete subgroup $\Gamma = \mathrm{GL}_r(\mathcal{O}_K, \mathfrak{a})$, and τ as in Definition 2.29. We first compute the function F that gives a bound on the inner products.

Lemma 4.8. *We have that* $\langle f_z, \gamma^{-1} f_z \rangle_Y \leq F(\tau(\gamma))$*, where*

$$F(\tau) = \frac{\mu_{\mathrm{Riem}}(X_r)^2 \mu_{\mathrm{Riem}}(\mathrm{SU}_r(K_{\mathbb{R}}))}{\mu_{\mathrm{Riem}}(B(t))} \left(\frac{\sqrt{r}}{\sigma\sqrt{2}}\right)^{r_u} \exp\left(-\frac{\pi}{2\sigma^2}\tau\right). \tag{26}$$

Proof. We begin with writing explicitly

$$\begin{aligned}
&\langle f_z, \gamma^{-1} f_z \rangle_Y \\
&= \frac{1}{I_f^2} \int_{x \in Y_r} \tilde{f}(z^{-1}x) \tilde{f}(z^{-1}\gamma x)\, d\mu_{\mathrm{Riem}}(x) \\
&= \frac{1}{I_f^2} \int_{x \in Y_r} \mathbf{1}_{[0,t]}(\rho(z^{-1}x)) \mathbf{1}_{[0,t]}(\rho(z^{-1}\gamma x)) \exp\left(-\frac{\pi}{\sigma^2}(\tau(z^{-1}x) + \tau(z^{-1}\gamma x))\right)
\end{aligned}$$

Let $z_H = \pi_H \log|\det z|$ and $\gamma_H = \log|\det \gamma| \in H$. We now estimate the intersection of the balls $zB(t)$ and $\gamma^{-1}zB(t)$ trivially to obtain, using the same techniques as when calculating I_f and $\Delta'_{\mathfrak{a}}\varphi_z$, that

$$\begin{aligned}
&\mu_{\mathrm{Riem}}(X_r) \cdot \langle f_z, \gamma^{-1} f_z \rangle_Y \\
&\leq \frac{1}{I_f^2} \int_{x \in Y_r} \mathbf{1}_{[0,t]}(\rho(z^{-1}x)) \exp\left(-\frac{\pi}{\sigma^2}(\tau(z^{-1}x) + \tau(z^{-1}\gamma x))\right) dx \\
&= \frac{1}{I_f^2 r^{\frac{r_u}{2}}} \int_{\delta \in Y_1} \int_{x \in \Delta^{-1}(\delta)} \mathbf{1}_{[0,t]}(\rho(z^{-1}x)) \exp\left(-\frac{\pi}{\sigma^2}(\tau(z^{-1}x) + \tau(z^{-1}\gamma x))\right) dx\, d\delta \\
&= \frac{1}{I_f^2 r^{\frac{r_u}{2}}} \int_{h \in H} \frac{\mu_{\mathrm{Riem}}(B(t))}{\mu_{\mathrm{Riem}}(\mathrm{SU}_r(K_{\mathbb{R}}))} \exp\left(-\frac{\pi}{\sigma^2}(\|h - z_H\|^2 + \|h + \gamma_H - z_H\|^2)\right) d\delta.
\end{aligned}$$

Focusing in on the integral, we have

$$\begin{aligned}
&\int_{h \in H} \exp\left(-\frac{\pi}{\sigma^2}(\|h - z_H\|^2 + \|h + \gamma_H - z_H\|^2)\right) d\delta \\
&= \int_{h \in H} \exp\left(-\frac{\pi}{\sigma^2}(2\|h - z_H + \tfrac{\gamma_H}{2}\|^2 + \tfrac{1}{2}\|\gamma_H\|^2)\right) d\delta \\
&= \exp\left(-\frac{\pi}{2\sigma^2}\tau(\gamma)\right) \int_{h \in H} \exp\left(-\frac{\pi}{\sigma^2}(2\|h\|^2)\right) d\delta \\
&= \left(\frac{\sigma}{\sqrt{2}}\right)^{r_u} \exp\left(-\frac{\pi}{2\sigma^2}\tau(\gamma)\right).
\end{aligned}$$

We finish by plugging in our formula (20) for I_f. □

To apply our formalism above and obtain a bound for $\|\varphi_z\|$, we are thus left with estimating $C_{f_z}(\tau)$. For this, observe that if $\langle f_z, \gamma^{-1} f_z \rangle_Y \neq 0$, then there exists a point $x \in Y_r$ such that $\rho(z^{-1}x) \leq t$ and $\rho(z^{-1}\gamma x) \leq t$. By the properties of ρ, we deduce that

$$\rho(z^{-1}\gamma z) = \rho(z^{-1}\gamma x x^{-1} z) \leq 2t. \tag{27}$$

We use this in the next section to count the elements γ that contribute to the L^2-norm.

4.2.2 The counting problem

Counting elements of $\Gamma_{\mathfrak{a}}$ lying in $B_{f_z}(\tau)$ can be reduced to counting lattice points in balls. The following lemma is well-known, and we cite a version that features explicit constants.

Lemma 4.9. *If* L *is a lattice of rank* n *and* $R \in \mathbb{R}_{>0}$*, we have*

$$|\{v \in L \mid \|v\| \leq R\}| \leq 2^{n-1} \prod_{i=1}^{n} \left(\frac{2R}{\lambda_i(L)} + 1\right).$$

Proof. This is Theorem 1.5 in [Hen02]. □

Lemma 4.10. *Let $L = L_{z,\mathfrak{a}}$ and let $\tau > 0$. Then*

$$C_{f_z}(\tau) \leq 2^{r^2d-r} \prod_{k=1}^{r} \prod_{i=1}^{rd} \left(2\exp(\tfrac{1}{r}\sqrt{\tau} + 2t) \frac{\lambda_k^K(L)}{\lambda_i(L)} + 1 \right).$$

Proof. Recall that for all $\gamma \in \Gamma = \mathrm{GL}_r(\mathcal{O}_K, \mathfrak{a})$,

$$\tau(\gamma) = \| \log|\det \gamma| \|_H^2 = \| \log|\det \gamma| \|^2,$$

and $C_f(\tau) = |B_f(\tau)|$, where

$$B_f(\tau) = \{\gamma \in \Gamma \mid \tau(\gamma) \leq \tau \text{ and } \langle f, \gamma^{-1} f \rangle_Y \neq 0\}.$$

Let $\gamma \in B_f(\tau)$. Then the non-vanishing of the inner product condition implies that $\rho(z^{-1}\gamma z) \leq 2t$, as in (27). Writing $z = (z_v)_v, \gamma = (\gamma_v)_v$ by viewing $\mathrm{GL}_r(K_\mathbb{R})$ as $\prod_v \mathrm{GL}_r(K_v)$, we have that $\|z^{-1}\gamma z\|_{\mathrm{op}} = \max_v \|z_v^{-1}\gamma_v z_v\|_{\mathrm{op}}$ since for $w \in K_\mathbb{R}^r$ we have $\|w\|^2 = \sum_v [K_v : \mathbb{R}] \|w_v\|^2$. We obtain,

$$\begin{aligned}
\|z^{-1}\gamma z\|_{\mathrm{op}} = \max_v \|z_v^{-1}\gamma_v z_v\|_{\mathrm{op}} &= \max_v \frac{\|z_v^{-1}\gamma_v z_v\|_{\mathrm{op}}}{|\det \gamma_v|^{\frac{1}{r}}} |\det \gamma_v|^{\frac{1}{r}} \\
&\leq \exp\left(\tfrac{1}{r} \log \max_v |\det \gamma_v|\right) \max_v \frac{\|z_v^{-1}\gamma_v z_v\|_{\mathrm{op}}}{|\det \gamma_v|^{\frac{1}{r}}} \\
&= \exp\left(\tfrac{1}{r} \| \log|\det \gamma| \|_\infty\right) \exp(\rho(\gamma)) \\
&\leq \exp\left(\tfrac{1}{r}\sqrt{\tau(\gamma)} + \rho(\gamma)\right) \leq \exp(\tfrac{1}{r}\sqrt{\tau} + 2t),
\end{aligned}$$

using that the L^∞-norm is at most the L^2-norm in finite dimensional spaces. In other words, the operator norm of γ acting on L is at most $\exp(\frac{1}{r}\sqrt{\tau} + 2t)$.

Now let $v_1, \ldots, v_r \in L$ be K-independent with $\|v_k\| \leq \lambda_k^K(L)$. Each $\gamma \in \Gamma$ is uniquely determined by the images of the v_k. In addition, for every $\gamma \in B_f(\tau)$, we have

$$\|\gamma v_k\| \leq \exp(\tfrac{1}{r}\sqrt{\tau} + 2t)\lambda_k^K(L).$$

By Lemma 4.9 the number of vectors in L satisfying this bound is at most

$$2^{rd-1} \prod_{i=1}^{rd} \left(\frac{2\exp(\frac{1}{r}\sqrt{\tau} + 2t)\lambda_k^K(L)}{\lambda_i(L)} + 1 \right).$$

Using this bound for every k leads to the claim. □

Corollary 4.11. *Under the same hypothesis, assuming that $t \geq \frac{1}{4}$ and that L is α-balanced (recall Definition 2.8), we have*

$$C_{f_z}(\tau) \leq \left(8\alpha^{r/6}\right)^{r^2 d} \exp(rd\sqrt{\tau} + 2r^2 dt).$$

Proof. Rewrite the bound of the lemma as

$$C_{f_z}(\tau) \leq 2^{r^2d-r} \prod_{k=1}^{r} \prod_{k'=1}^{r} \prod_{i=1}^{d} \left(2\exp(\tfrac{1}{r}\sqrt{\tau} + 2t) \frac{\lambda_k^K(L)}{\lambda_{d(k'-1)+i}(L)} + 1 \right).$$

Applying Lemma 2.13, we get

$$\begin{aligned}
C_{f_z}(\tau) &\le 2^{r^2d-r}\prod_{k=1}^{r}\prod_{k'=1}^{r}\prod_{i=1}^{d}\left(2\exp(\tfrac{1}{r}\sqrt{\tau}+2t)\frac{\lambda_k^K(L)}{\lambda_{k'}^K(L)}+1\right)\\
&\le 2^{r^2d}(4\exp(\tfrac{1}{r}\sqrt{\tau}+2t))^{dr(r+1)/2}\prod_{k=1}^{r}\prod_{k'=1}^{k-1}\left(4\exp(\tfrac{1}{r}\sqrt{\tau}+2t)\frac{\lambda_k^K(L)}{\lambda_{k'}^K(L)}\right)^d\\
&\le 8^{r^2d}\exp(rd\sqrt{\tau}+2r^2dt)\prod_{k=1}^{r}\prod_{k'=1}^{r}\alpha^{d(k-k')}\\
&\le 8^{r^2d}\exp(rd\sqrt{\tau}+2r^2dt)\alpha^{dr(r^2-1)/6},
\end{aligned}$$

which implies the claim. □

4.2.3 The norm bound

Before proving our bound for $\|\varphi_z\|$, we state a technical lemma that aids computation.

Lemma 4.12. *Let $a, b > 0$. Then*

$$\int_0^\infty \exp(-ax+b\sqrt{x})dx \le \frac{2}{a}\left(2\exp(2b^2/a)+1\right).$$

Proof. Let $x \ge (2b/a)^2$. Then $-ax+b\sqrt{x} \le -\frac{a}{2}x$, so

$$\int_{(2b/a)^2}^\infty \exp(-ax+b\sqrt{x})dx \le \int_{(2b/a)^2}^\infty \exp(-\frac{a}{2}x)dx = \frac{2}{a}\exp(-2b^2/a) \le \frac{2}{a}.$$

On the other hand we have

$$\begin{aligned}
\int_0^{(2b/a)^2} \exp(-ax+b\sqrt{x})dx &\le \int_0^{(2b/a)^2}\exp(b\sqrt{x})dx = 2\int_0^{2b/a} y\exp(by)dy\\
&\le (4b/a)\int_{-\infty}^{2b/a}\exp(by)dy = (4/a)\exp(2b^2/a).
\end{aligned}$$

□

We now sum up all the previous sections, recalling our construction for convenience, and conclude with one of the main estimates in our argument. Namely, we define the function φ_z (see Definition 4.3) starting with data consisting of a matrix $z \in Y_r$, a class group representative $\mathfrak{a}$, the parameter t, which controls how much φ_z localizes in the $\mathrm{SL}(r)$-part, and the parameter σ, which controls how much it localizes in the $\mathrm{GL}(1)$-part. The first two data also define a lattice $L = L_{z,\mathfrak{a}}$. We have the following bound on the L^2-norm of the starting distribution, defined in terms of μ_{Riem}.

Proposition 4.13. *Suppose $L_{z,\mathfrak{a}}$ is α-balanced, and let $1 \le t \le O(1)$ and $\sigma = O(1/\sqrt{d})$. We have*

$$\log\|\varphi_z\|_{X_R} \le \frac{r^3d}{6}\log\alpha + r^2\log|\Delta_K| + \frac{d}{2}\log d + O(r^2d\log r + \log\log|\Delta_K|).$$

Proof. We first prove the more precise bound

$$\|\varphi_z\|^2 \le \frac{\mu_{\mathrm{Riem}}(X_r)^2}{\mu_{\mathrm{Riem}}(B(t))\sigma^{r_u}}\left(\frac{r}{2}\right)^{\frac{r_u}{2}}\left(8e^{2t}\alpha^{r/6}\right)^{r^2d}\left(4\exp\Big(\frac{(2\sigma rd)^2}{\pi}\Big)+2\right).$$

For this, recall from (26) that we have $\langle f_z, \gamma^{-1}f_z\rangle_Y \le F(\tau)$, where

$$F(\tau) = \frac{\mu_{\mathrm{Riem}}(X_r)^2\mu_{\mathrm{Riem}}(\mathrm{SU}_r(K_{\mathbb{R}}))}{\mu_{\mathrm{Riem}}(B(t))}\left(\frac{\sqrt{r}}{\sigma\sqrt{2}}\right)^{r_u}\exp\left(-\frac{\pi}{2\sigma^2}\tau\right).$$

For applying the formal bound (25), we first note that, by Corollary 4.11, the function $C_f(\tau)$ grows like $\exp(\sqrt{\tau})$, whilst $F(\tau)$ decays like $\exp(-\tau)$. This implies that $F(\tau)C_f(\tau)$ vanishes as τ goes to infinity. The same observation shows that $F'(\tau)C_f(\tau)$ exhibits rapid decay and is integrable. Therefore, we obtain that

$$\|\varphi_z\|^2 \leq \int_0^\infty C_f(\tau)(-F'(\tau))d\tau.$$

Ignoring the τ-independent factors in the formula for $F'(\tau)$, we have

$$\int_0^\infty C_f(\tau)\exp\left(-\frac{\pi}{2\sigma^2}\tau\right)\,d\tau \leq \left(8e^{2t}\alpha^{r/6}\right)^{r^2d}\int_0^\infty \exp(-\frac{\pi}{2\sigma^2}\tau + rd\sqrt{\tau})\,d\tau.$$

Lemma 4.12 with $a = \frac{\pi}{2\sigma^2}$ and $b = rd$ now gives

$$\int_0^\infty \exp(-\frac{\pi}{2\sigma^2}\tau + rd\sqrt{\tau})\,d\tau \leq \frac{4\sigma^2}{\pi}\left(2\exp\Big(\frac{(2\sigma rd)^2}{\pi}\Big)+1\right).$$

To finally arrive at the claimed bound, note simply that the factor $\frac{4\sigma^2}{\pi}$ in the previous display and the $\frac{\pi}{2\sigma^2}$ from differentiating F cancel to give a factor of 2.

By the assumption on σ we have

$$4\exp\Big(\frac{(2\sigma rd)^2}{\pi}\Big)+2 = 2^{O(r^2d)}.$$

Introducing the volume computations of Section 2.6.3 to the bound we proved above, we obtain

$$\begin{aligned}
2\log\|\varphi_z\| &\leq 2\log\mu_{\mathrm{Riem}}(X_r) - \log\mu_{\mathrm{Riem}}(B(t)) + \frac{r_u}{2}\log d + \frac{r^3d}{6}\log\alpha + O(r^2d)\\
&\leq \frac{dr^2}{2}\log r + r^2\log|\Delta_K| + O(\log\log|\Delta_K|) + \frac{9}{4}dr^2\log r\\
&+ \frac{r_u}{2}\log d + \frac{r^3d}{6}\log\alpha + O(r^2d) \text{ by Lemmas 2.32 and 2.37}\\
&= r^2\log|\Delta_K| + \frac{d}{2}\log d + \frac{r^3d}{6}\log\alpha + O(r^2d\log r + \log\log|\Delta_K|)
\end{aligned}$$

as claimed, by simplifying the expression using that $r_u \leq d$. □

4.3 Quantitative equidistribution

Recall that we are interested in showing that the measures on X_r, obtained by applying Hecke operators $T_{\mathfrak{p}}$ and averages thereof to the initial probability distribution given by $\varphi_z \cdot \mu_{\mathrm{Riem}}$, converge to the uniform measure μ. To understand the rate of convergence, we need an upper bound on

$$\left\|T_{\mathcal{P}(B)}(\varphi_z - \mu_{\mathrm{Riem}}(X_r)^{-1}\mathbf{1}_{X_r})\right\|_{X_r},$$

where $B > 0$ is some parameter to be chosen later. Here we are using the L^2-norm with respect to μ_{Riem}.

For this, we decompose the function into its projection onto L^2_{det} and its orthogonal complement. Recall that $T_{\mathfrak{p}}$ preserves such decompositions and notice also that the constant function is equal to its projection onto L^2_{det}. We therefore focus first on bounding

$$\left\|T_{\mathcal{P}(B)}(\pi_{\mathrm{det}}\varphi_z - \mu_{\mathrm{Riem}}(X_r)^{-1}\cdot\mathbf{1}_{X_r})\right\|_{X_r}.$$

We now import the results of [BDP+20], which essentially treat Hecke operators on the space $L^2_{\mathrm{det}}(X_r)$. For that, we denote by $T^1_{\mathfrak{p}}$ the Hecke operator on $L^2(X_1)$, which is adelically given by

$$T^1_{\mathfrak{p}} f(x) = f(x\pi_{\mathfrak{p}}^{-1}),$$

where $\pi_{\mathfrak{p}}$ is a uniformizer at $\mathfrak{p}$. This corresponds to the definition of a Hecke operator in [BDP+20, Sec. 3], upon identifying X_1 with the *additive* Arakelov class group Pic^0_K.

Next, we recall that $L^2(X_1) = \prod_{\mathfrak{a}} L^2(X_{1,\mathfrak{a}})$ and that $X_{1,\mathfrak{a}} = X_{1,1}$ for all representatives $\mathfrak{a}$ of the class group. The definition of Hecke operators (see (11)) directly implies that

$$T_{\mathfrak{p}}\Delta^*_{\mathfrak{a}} = \Delta^*_{\mathfrak{a}} T^1_{\mathfrak{p}}. \tag{28}$$

To be precise, we view $L^2(X_{N,\mathfrak{a}})$ embedded in $L^2(X_N)$, for $N = 1, r$, by extending functions by the constant zero function on all other components. Note also that $T_{\mathfrak{p}}$ sends $L^2(X_{N,\mathfrak{a}})$ to $L^2(X_{N,\mathfrak{p}\cdot\mathfrak{a}})$ in this interpretation.

Next, we recall that $\pi_{\mathrm{det}}\varphi_z = \Delta^*_{\mathfrak{a}}\varphi_{z,1}$ (see (23)) and $\mathbf{1}_{X_r} = \Delta^*_{\mathfrak{a}}\mathbf{1}_{X_1}$. Recall from the computation (24) that

$$\langle \varphi_{z,1}, \mathbf{1}_{X_1}\rangle_{X_1} = \mu_{\mathrm{Riem}}(\Delta_{\mathfrak{a}}^{-1}(1))^{-1}.$$

From Section (2.6.3), we gather that

$$\mu_{\mathrm{Riem}}(X_r) = r^{-\frac{r_u}{2}} \cdot \mu_{\mathrm{Riem}}(\Delta_{\mathfrak{a}}^{-1}(1)) \cdot \mu_{\mathrm{Riem}}(X_1).$$

The formula for how norms behave under $\Delta^*_{\mathfrak{a}}$, given in Section 2.6.2, and the Hecke operator compatibility relation 28 now imply that

$$\begin{aligned}
&\left\| T_{\mathfrak{p}}(\pi_{\mathrm{det}}\varphi_z - \mu_{\mathrm{Riem}}(X_r)^{-1}\cdot \mathbf{1}_{X_r})\right\|_{X_r} \\
&= \sqrt{\frac{r^{-\frac{r_u}{2}}\cdot \mu_{\mathrm{Riem}}(\Delta_{\mathfrak{a}}^{-1}(1))\mu_{\mathrm{Riem}}(X_1)}{\mu_{\mathrm{Riem}}(X_r)}}\left\| T^1_{\mathfrak{p}}(\rho_\sigma - \mu_{\mathrm{Riem}}(X_1)^{-1}\mathbf{1}_{X_1})\right\|_{X_1} \\
&= \left\| T^1_{\mathfrak{p}}(\rho_\sigma - \mu_{\mathrm{Riem}}(X_1)^{-1}\mathbf{1}_{X_1})\right\|_{X_1}
\end{aligned} \tag{29}$$

where we write

$$\rho_\sigma(\delta) = \sum_{\xi\in\mathbb{Z}_K^\times} \sigma^{-r_u}\exp(-\frac{\pi}{\sigma^2}\|\log|\delta| + \log|\xi| - \log|\det(z)|\|^2_H).$$

The function ρ_σ is defined on $X_{1,\mathfrak{a}}$ and extended, as usual, to all of X_1 by zero.

We now observe that ρ_σ is the same test function as $\sigma^{r_u}\rho_\sigma\,|^T$ in Section 3.5 of [BDP+20], up to the shift $\delta \mapsto \delta\cdot\det(z)$. Since the right regular representation is unitary, leaves constant functions invariant, and commutes with Hecke operators, we may ignore this shift.

For the next result, we introduce the natural notation

$$T^1_{\mathcal{P}(B)} = \frac{1}{|\mathcal{P}(B)|}\sum_{N(\mathfrak{p})\le B} T^1_{\mathfrak{p}}.$$

Proposition 4.14. *Assume ERH for the L-function of every Hecke character of K of trivial modulus. For positive parameters B, κ, σ such that $\kappa\sigma > \sqrt{r_u/4\pi}$, we have*

$$\left\| T^1_{\mathcal{P}(B)}(\rho_\sigma) - \mu_{\mathrm{Riem}}(X_1)^{-1}\mathbf{1}_{X_1}\right\|^2_{X_1} \ll \max(r_u(\log r_u)^3, 1/\sigma)^{r_u}\cdot(c^2 + e^{-2(\kappa\sigma)^2}),$$

where

$$c = O\left(\frac{\log(B)\log[B^d\cdot|\Delta_K|\cdot(4+2\pi\kappa/\sqrt{d})^d]}{\sqrt{B}}\right).$$

Proof. This is Theorem 3.16 of [BDP+20] with $N = 1$ and a few mild, additional constraints. For convenience, we note here that in loc. cit., n is our d, l is our r_u, s is our σ, r is our κ. Observe also the typo in (6) of loc. cit., where n should be replaced by l.

We use (9) of loc. cit. together with the bounds in the beginning of the proof of Corollary 3.4 in Appendix B of loc. cit. to obtain the bound $r_u(\log r_u)^3$ for $\eta_1(\Lambda_K^*)$, the smoothing number in the notation of that paper. We finish by applying the bound $\beta_{\sqrt{2}\kappa\sigma}^{(r_u)} \leq e^{-2(\kappa\sigma)^2}$ from just before Lemma 2.10 in loc. cit., which is valid under our assumption. □

We continue with the orthogonal complement of $L^2_{\mathrm{det}}(X_r)$. On this space, we use the spectral gap afforded by Corollary 2.39. Putting everything together we prove Theorem 3.

Proof of Theorem 3. As indicated at the beginning of this section, we prove this bound by decomposing the expression in the norm into its projection to L^2_{det} and its orthogonal complement. For the L^2_{det}-part, we recall (29) and the previous result, Proposition 4.14.

Let us temporarily denote $\varphi_z^\perp = \varphi_z - \pi_{\mathrm{det}}\varphi_z$. We are left with bounding $\left\|T^N_{\mathcal{P}(B)}\varphi_z^\perp\right\|$. For this we apply the spectral gap as in Corollary 2.39 to get

$$\left\|T_{\mathcal{P}(B)}\varphi_z^\perp\right\|^2 \ll (rd)^2 \cdot B^{-3/4}\log(B)^2 \cdot \left\|\varphi_z^\perp\right\|^2.$$

We then trivially bound $\left\|\varphi_z^\perp\right\|$ by $\|\varphi_z\|$ and apply Proposition 4.13, the conditions of which are satisfied. □

5 Balancedness of random module lattices

In this section, we prove that μ-random module lattices are balanced (in a weak sense) with high probability: the main result is Theorem 4. We will use the Grayson–Stuhler theory of stability of lattices, from which we recall some definitions (cf. [Gra84; Bos20]). The role of this notion is that it is relatively easy to compute the probability of a random lattice being unstable, and that stable lattices are balanced. We compute this probability using work of Thunder [Thu98], with inspiration from an article of Shapira and Weiss [SW14], whose result we generalize and sharpen. Note that in recent work [GSV+25b; GSV+25a], Gargava, Serban, Viazovska and Viglino prove strong bounds on the shortest vectors of random module lattices; our bounds are weaker but more widely applicable.

Definition 5.1. Let L be a module lattice. The *slope* of L is

$$\mathrm{slope}(L) = \frac{\log\det(L)}{\mathrm{rank}(L)}.$$

Let $t \geq 1$. A sub-module lattice $L' \subset L$ (of arbitrary rank) is *t-destabilising* if

$$\mathrm{slope}(L') \leq \mathrm{slope}(L) - \frac{\log(t)}{\mathrm{rank}(L')},$$

i.e. if

$$(t \cdot \det(L'))^{\frac{1}{\mathrm{rank}(L')}} \leq \det(L)^{\frac{1}{\mathrm{rank}(L)}}.$$

A lattice is *semistable* if it does not contain any t-destabilising sub-module lattices for any $t > 1$, i.e. if

$$\mathrm{slope}(L') \geq \mathrm{slope}(L)$$

for every sub-module lattice $L' \subset L$.

Remark 5.2. The notion of stability we use is with respect to the class of module lattices over a fixed field K. Throughout this section, keeping this remark in mind, we abbreviate the term *sub-module lattice* to simply *sublattice*.

Remark 5.3. Note that if there exists a t-destabilising sublattice L' in L, then there also exists a primitive one of the same rank as L', namely $L'' = W \cap L' \supset L'$ where $W = K \cdot L'$.

Theorem 4. *In the set of (K, r) such that*

- $r \geq 4$, *or*
- $r \geq 3$ *and* $|\Delta_K| \geq 57.5^d$, *or*
- $|\Delta_K| \geq 845^d$,

a μ-random module lattice L is semistable with probability at least $1 - 2^{-\Omega(n \log r)}$.

Now assume $r \leq 3$, and let $\delta = |\Delta_K|^{\frac{1}{d}}$. If $r = 2$, let

$$t = \max\left(1.01\frac{\pi e}{2}\frac{\log \delta}{\delta^{\frac{1}{2}}}, 1\right)^{\frac{d}{2}};$$

if $r = 3$, let

$$t = \max\left(1.01\frac{\pi^3 e}{6}\frac{\log \delta}{\delta}, 1\right)^{\frac{d}{3}};$$

Then a μ-random module lattice L has no t-destabilising sublattice with probability at least $1 - 2^{-\Omega(d)}$.

In all cases, a μ-random module lattice L satisfies

$$\lambda_1(L) \geq \Omega(|\Delta_K|^{-\frac{1}{2d}}) \cdot \det(L)^{\frac{1}{n}} \text{ and } \lambda_n(L) \leq O(n|\Delta_K|^{\frac{1}{2d}}) \cdot \det(L)^{\frac{1}{n}}$$

with probability at least $1 - 2^{-\Omega(n \log r)}$.

Remark 5.4.

1. It would be interesting to know whether there exists families of number fields in which the proportion of semistable lattices of rank 2 (or 3) is not $1 - 2^{-\Omega(d)}$. Such a family should have bounded root discriminant, and, as is visible from our proof, this proportion is directly related to the size of the residue of the Dedekind zeta function of these fields.
2. Our methods meets its limits when the rank r is small and the fields have small root discriminant. Interestingly, the methods of [GSV+25b; GSV+25a] also have limitations in small rank and for families of fields that admits elements of small height. It would be interesting to investigate relations between these limitations.

We break up the proof into several intermediate results. We will use computations by Thunder [Thu98] and we first explain how to relate his adélic computations to our case of interest. For the reader's convenience, we provide the correspondence between notations: Thunder's $K_{\mathbb{A}}$ is our $\mathbb{A}_K$, his n is our r, his d is our k, he writes $[K : \mathbb{Q}]$ for our $d = \deg(K)$, and his χ_t is our $\mathbf{1}_{[0,t]}$. Recall from Section 2.3.2 that to each $A \in \mathrm{GL}_r(\mathbb{A}_K)$ we can attach a module lattice embedded in $K_{\mathbb{R}}^r$, which we will write L_A. Let $k \geq 1$ be an integer. Thunder defines a function

$$f_{r,k} \colon \mathrm{GL}_r(\mathbb{A}_K) \to \mathbb{R}_{>0}.$$

Translated in module lattice language, $f_{r,k}(A)$ is the determinant of the sub-module-lattice $L' \subset L_A$ generated by the first k columns of the basis of L_A determined by A.

Define $G_r = \{A \in \mathrm{GL}_r(\mathbb{A}_K) : \prod_v |\det(A_v)|_v = 1\}$ (corresponding to lattices of determinant 1) and

$$G_{r,k} = \left\{ \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} : A \in G_k, D \in G_{r-k}, B \in M_{k,r-k}(\mathbb{A}_K) \right\}.$$

Then the quotient $\mathrm{GL}_r(K)/\mathrm{GL}_r(K) \cap G_{r,k}$ is in bijection with the set $\mathrm{Gr}_{r,k}(K)$ of k-dimensional subspaces of K^r via $\gamma \mapsto \gamma(K^k \times \{0\}^{r-k})$. Thunder defines

$$c(r,k) = \int_{G_r/G_{r,k}} \mathbf{1}_{[0,1]}(f_{r,k}(A)) d\mu(A).$$

Lemma 5.5. *Let $t \in \mathbb{R}_{\geq 1}$ and $k \in \mathbb{Z}_{\geq 1}$. The measure of the set of module lattices that admit a t-destabilising sublattice of rank k is at most $c(r,k)t^{-r}$.*

Proof. We have

$$\begin{aligned}
& \mu(\{L \in X_r(K) : L \text{ admits a } t\text{-destabilising sublattice of rank } k\}) \\
\leq & \int_{G_r/\mathrm{GL}_r(K)} \left(\sum_{W \in \mathrm{Gr}_{r,k}(K)} \mathbf{1}_{W \cap L_A \text{ is } t\text{-destabilising in } L_A}(A) \right) d\mu(A) \\
= & \int_{G_r/\mathrm{GL}_r(K)} \left(\sum_{\gamma \in \mathrm{GL}_r(K)/\mathrm{GL}_r(K) \cap G_{r,k}} \mathbf{1}_{[0,\frac{1}{t}]}(f_{r,k}(A\gamma)) \right) d\mu(A) \\
= & \int_{G_r/G_{r,k}} \mathbf{1}_{[0,\frac{1}{t}]}(f_{r,k}(A)) d\mu(A) \text{ by [Wei82, Lemma 2.4.2]} \\
= & \ c(r,k)t^{-r} \text{ by [Thu98, Lemma 5]},
\end{aligned}$$

proving the claim. □

For every dimension n, let V_n be the volume of the Euclidean n-ball of radius 1, i.e. $V_n = \frac{\pi^{\frac{n}{2}}}{\Gamma(\frac{n}{2}+1)}$. For every integer $m \geq 1$, let $\zeta_K^*(m)$ denote the leading coefficient of $\zeta_K(s)$ at $s = m$, i.e. $\zeta_K^*(m) = \zeta_K(m)$ for $m \geq 2$ and $\zeta_K^*(1) = \frac{2^{r_1}(2\pi)^{r_2} R_K h_K}{|\Delta_K|^{1/2} w_K}$ by the analytic class number formula (recall Section 2.2 for notation) and define

$$R(m) = \frac{m^{r_u+1} 2^{mr_2} V_m^{r_1} V_{2m}^{r_2}}{\zeta_K^*(m) |\Delta_K|^{m/2}}, \text{ so that } R(1) = \frac{w_K}{h_K R_K}.$$

Lemma 5.6. *For every $0 < k < r$ we have*

$$c(r,k) = \frac{1}{r} \cdot \frac{\prod_{j=1}^{r} R(j)}{\prod_{j=1}^{k} R(j) \prod_{j=1}^{r-k} R(j)}.$$

Proof. First note that for $r > 1$,

$$\frac{1}{r} \cdot \frac{R(r)}{R(1)} = \frac{r^{r_u} 2^{rr_2} V_r^{r_1} V_{2r}^{r_2} h_K R_K}{\zeta_K(r) |\Delta_K|^{r/2} w_K},$$

which is indeed the value of $c(r,1)$ by [Thu98, Lemma 7]. In addition, the RHS of the claimed equality clearly satisfies Thunder's recurrence relation [Thu98, Theorem 3], so the equality holds for every r and k. □

Lemma 5.7. *For every $m \geq 1$ we have*

$$\prod_{j=2}^{m} \zeta_K(j) \leq (2.3)^d.$$

Proof. Since there are at most d prime ideals in $\mathcal{O}_K$ over a rational prime, we have $\zeta_K(j) \le \zeta(j)^d$ for all $j > 1$. It is thus sufficient to prove the inequality for ζ. In addition, since the product increases with m, it is enough to prove the inequality for m large enough. We have

$$\zeta(j) \le 1 + 2^{-j} + \int_2^\infty t^{-j} dt \le 1 + 3 \cdot 2^{-j}.$$

Therefore, for all $m \ge m_0$, we have

$$\sum_{j=m_0}^{m} \log \zeta(j) \le 3 \sum_{j=m_0}^{m} 2^{-j} \le 6 \cdot 2^{-m_0},$$

and thus

$$\prod_{j=2}^{m} \zeta(j) \le \prod_{j=2}^{m_0-1} \zeta(j) \cdot \exp(6 \cdot 2^{-m_0}).$$

For $m_0 = 11$, this gives the claimed inequality. □

Lemma 5.8. *For any function $f\colon [1, +\infty) \to \mathbb{R}$, write $S_m(f) = \sum_{j=1}^{m} f(j)$ for $m \ge 1$ and $S_{r,k}(f) = S_r(f) - S_k(f) - S_{r-k}(f)$ for $r \ge 2$ and $1 \le k < r$.*

1. *For $f(x) = (\frac{x}{2} + 1)\log(\frac{x}{2} + 1)$, we have*
$$S_{r,k}(f) \ge \tfrac{1}{2}k(r-k)\log(\tfrac{r}{2}+1) - \tfrac{1}{4}k(r-k) - \tfrac{13}{8}\log(\tfrac{r}{2}+1) + \tfrac{13}{8}\log(\tfrac{3}{2}) - \tfrac{5}{8}.$$
2. *For $f(x) = \log(\frac{x}{2} + 1)$, we have $S_{r,k}(f) \le (r+2)\log 2 - \frac{11}{12} - \frac{5}{2}\log(\frac{3}{2})$.*
3. *For $f(x) = \frac{1}{\frac{x}{2}+1}$, we have $S_k(f) + S_{r-k}(f) \le 4\log(\frac{r}{4}+1)$.*
4. *For $f(x) = \log\Gamma(\frac{x}{2} + 1)$, we have*
$$S_{r,k}(f) \ge \tfrac{1}{2}k(r-k)\log(\tfrac{r}{2}+1) - \tfrac{3}{4}k(r-k) - r\tfrac{\log 2}{2} - \tfrac{47}{24}\log(r+4) + 1.89.$$
5. *For $f(x) = (x+1)\log(x+1)$, we have*
$$S_{r,k}(f) \ge k(r-k)\log(r+1) - \tfrac{1}{2}k(r-k) - \tfrac{5}{4}\log(r+1) + \tfrac{5}{4}\log 2 - \tfrac{3}{4}.$$
6. *For $f(x) = \log(x+1)$, we have $S_{r,k}(f) \le (r+1)\log 2 + \frac{3}{2}\log 2 - \frac{7}{8}$.*
7. *For $f(x) = \frac{1}{x+1}$, we have $S_k(f) + S_{r-k}(f) \le 2\log(\frac{r}{2}+1)$.*
8. *For $f(x) = \log\Gamma(x+1)$, we have*
$$S_{r,k}(f) \ge k(r-k)\log(r+1) - \tfrac{3}{2}k(r-k) - r\log 2 - \tfrac{17}{12}\log(r+2) - 0.626.$$

Proof. We will repeatedly use Euler–Maclaurin summation in the following form [Coh07, Corollary 9.2.3 and Proposition 9.2.5]: if f is C^4 and both $f^{(2)}$ and $f^{(4)}$ do not change sign on $[1, +\infty)$, then

$$S_m(f) = \int_1^m f(x)dx + \frac{f(1)+f(m)}{2} + R \text{ where } |R| \le \frac{|f'(m) - f'(1)|}{12}.$$

1. We have

$$\begin{aligned} & S_m(f) \\ = \; & (\tfrac{m}{2}+1)^2(\log(\tfrac{m}{2}+1) - \tfrac{1}{2}) - \tfrac{9}{4}(\log(\tfrac{3}{2}) - \tfrac{1}{2}) + \tfrac{1}{2}((\tfrac{m}{2}+1)\log(\tfrac{m}{2}+1) + \tfrac{3}{2}\log(\tfrac{3}{2})) + R \\ = \; & \tfrac{1}{4}(m+2)^2(\log(\tfrac{m}{2}+1) - \tfrac{1}{2}) - \tfrac{9}{4}(\log(\tfrac{3}{2}) - \tfrac{1}{2}) + \tfrac{1}{4}((m+2)\log(\tfrac{m}{2}+1) + 3\log(\tfrac{3}{2})) + R \end{aligned}$$

where

$$|R| \le \tfrac{1}{24}\big(\log(\tfrac{m}{2}+1) - \log(\tfrac{3}{2})\big).$$

We bound

$$\begin{aligned} & (r+2)^2\log(\tfrac{r}{2}+1) - (k+2)^2\log(\tfrac{k}{2}+1) - (r-k+2)^2\log(\tfrac{r-k}{2}+1) \\ \ge\ & (r+2)^2\log(\tfrac{r}{2}+1) - (k+2)^2\log(\tfrac{r}{2}+1) - (r-k+2)^2\log(\tfrac{r}{2}+1) \\ =\ & 2(k(r-k)-2)\log(\tfrac{r}{2}+1) \end{aligned}$$

and

$$\begin{aligned} & (r+2)\log(\tfrac{r}{2}+1) - (k+2)\log(\tfrac{k}{2}+1) - (r-k+2)\log(\tfrac{r-k}{2}+1) \\ \ge\ & (r+2)\log(\tfrac{r}{2}+1) - (k+2)\log(\tfrac{r}{2}+1) - (r-k+2)\log(\tfrac{r}{2}+1) \\ =\ & -2\log(\tfrac{r}{2}+1) \end{aligned}$$

to obtain

$$\begin{aligned} S_{r,k}(f) \ \ge\ & \tfrac{1}{2}(k(r-k)-2)\log(\tfrac{r}{2}+1) - \tfrac{1}{4}(k(r-k)-2) - \tfrac{1}{2}\log(\tfrac{r}{2}+1) \\ & + \tfrac{9}{4}(\log(\tfrac{3}{2}) - \tfrac{1}{2}) - \tfrac{3}{4}\log(\tfrac{3}{2}) - \tfrac{1}{8}(\log(\tfrac{r}{2}+1) - \log(\tfrac{3}{2})) \\ =\ & \tfrac{1}{2}k(r-k)\log(\tfrac{r}{2}+1) - \tfrac{1}{4}k(r-k) - \tfrac{13}{8}\log(\tfrac{r}{2}+1) + \tfrac{13}{8}\log(\tfrac{3}{2}) - \tfrac{5}{8}. \end{aligned}$$

2. We have

$$S_m(f) = (m+2)\big(\log(\tfrac{m}{2}+1) - 1\big) - 3(\log(\tfrac{3}{2}) - 1) + \tfrac{1}{2}\log(\tfrac{m}{2}+1) + \tfrac{1}{2}\log(\tfrac{3}{2}) + R$$

where

$$|R| \le \tfrac{1}{12}(\tfrac{1}{3} - \tfrac{1}{m+2}) \le \tfrac{1}{36}.$$

We bound

$$\begin{aligned} & (r+2)\log(\tfrac{r}{2}+1) - (k+2)\log(\tfrac{k}{2}+1) - (r-k+2)\log(\tfrac{r-k}{2}+1) \\ \le\ & (r+2)\log(\tfrac{r}{2}+1) - 2(\tfrac{r}{2}+2)\log(\tfrac{r}{4}+1) \\ \le\ & (r+2)\log(\tfrac{2r+4}{r+4}) \\ \le\ & (r+2)\log 2 \end{aligned}$$

and

$$\tfrac{1}{2}\log(\tfrac{r}{2}+1) - \tfrac{1}{2}\log(\tfrac{k}{2}+1) - \tfrac{1}{2}\log(\tfrac{r-k}{2}+1) \le 0.$$

We get

$$S_{r,k}(f) \le (r+2)\log 2 + 2 + 3(\log(\tfrac{3}{2}) - 1) - \tfrac{1}{2}\log(\tfrac{3}{2}) + \tfrac{1}{12} = (r+2)\log 2 - \tfrac{11}{12} - \tfrac{5}{2}\log(\tfrac{3}{2}).$$

3. We have

$$S_m(f) \le \int_0^m \frac{dt}{\frac{t}{2}+1} = 2\log(\tfrac{m}{2}+1),$$

and therefore

$$S_k(f) + S_{r-k}(f) \le 2\log(\tfrac{k}{2}+1) + 2\log(\tfrac{r-k}{2}+1) \le 4\log(\tfrac{r}{4}+1).$$

4. We use the following bound [Alz97, Theorem 8]: for all $y > 0$ we have

$$(y - \tfrac{1}{2})\log(y) - y + \tfrac{\log(2\pi)}{2} < \log\Gamma(y) < (y - \tfrac{1}{2})\log(y) - y + \tfrac{\log(2\pi)}{2} + \tfrac{1}{12y}.$$

Summing the various contributions, we get

$$\begin{aligned} & S_{r,k}(f) \\ \geq\ & \tfrac{1}{2}k(r-k)\log(\tfrac{r}{2}+1) - \tfrac{1}{4}k(r-k) - \tfrac{13}{8}\log(\tfrac{r}{2}+1) + \tfrac{13}{8}\log(\tfrac{3}{2}) - \tfrac{5}{8} - (r+2)\tfrac{\log 2}{2} \\ & + \tfrac{11}{24} + \tfrac{5}{4}\log(\tfrac{3}{2}) - \tfrac{1}{2}k(r-k) - \tfrac{1}{3}\log(\tfrac{r}{4}+1) \\ \geq\ & \tfrac{1}{2}k(r-k)\log(\tfrac{r}{2}+1) - \tfrac{3}{4}k(r-k) - r\tfrac{\log 2}{2} - \tfrac{47}{24}\log(r+4) + 1.89. \end{aligned}$$

5. We have

$$S_m(f) = \tfrac{1}{2}(m+1)^2\big(\log(m+1) - \tfrac{1}{2}\big) - 2(\log 2 - \tfrac{1}{2}) + \tfrac{1}{2}(m+1)\log(m+1) + \log 2 + R$$

where

$$|R| \leq \tfrac{1}{12}\big(\log(m+1) - \log 2\big).$$

We bound

$$\begin{aligned} & (r+1)^2\log(r+1) - (k+1)^2\log(k+1) - (r-k+1)^2\log(r-k+1) \\ \geq\ & (r+1)^2\log(r+1) - (k+1)^2\log(r+1) - (r-k+1)^2\log(r+1) \\ =\ & (2k(r-k)-1)\log(r+1) \end{aligned}$$

and

$$\begin{aligned} & (r+1)\log(r+1) - (k+1)\log(k+1) - (r-k+1)\log(r-k+1) \\ \geq\ & (r+1)\log(r+1) - (k+1)\log(r+1) - (r-k+1)\log(r+1) \\ =\ & -\log(r+1) \end{aligned}$$

to obtain

$$\begin{aligned} S_{r,k}(f) \ \geq\ & (k(r-k) - \tfrac{1}{2})\log(r+1) - \tfrac{1}{4}(2k(r-k)-1) + 2(\log 2 - \tfrac{1}{2}) - \tfrac{1}{2}\log(r+1) \\ & - \log 2 - \tfrac{1}{4}\big(\log(r+1) - \log 2\big) \\ =\ & k(r-k)\log(r+1) - \tfrac{1}{2}k(r-k) - \tfrac{5}{4}\log(r+1) + \tfrac{5}{4}\log 2 - \tfrac{3}{4}. \end{aligned}$$

6. We have

$$S_m(f) = (m+1)\big(\log(m+1) - 1\big) - 2(\log 2 - 1) + \tfrac{1}{2}\log(m+1) + \tfrac{1}{2}\log 2 + R$$

where

$$|R| \leq \tfrac{1}{12}(\tfrac{1}{2} - \tfrac{1}{m+1}) \leq \tfrac{1}{24}.$$

We bound

$$\begin{aligned} & (r+1)\log(r+1) - (k+1)\log(k+1) - (r-k+1)\log(r-k+1) \\ \leq\ & (r+1)\log(r+1) - 2(\tfrac{r}{2}+1)\log(\tfrac{r}{2}+1) \\ \leq\ & (r+1)\log(\tfrac{2r+2}{r+2}) \\ \leq\ & (r+1)\log 2 \end{aligned}$$

and

$$\log(r+1) - \log(k+1) - \log(r-k+1) \leq 0.$$

We get

$$S_{r,k}(f) \leq (r+1)\log 2 + \tfrac{3}{2}\log 2 - 1 + \tfrac{1}{8} = (r+1)\log 2 + \tfrac{3}{2}\log 2 - \tfrac{7}{8}.$$

7. We have

$$S_m(f) \leq \int_0^m \frac{dt}{t+1} = \log(m+1),$$

and therefore

$$S_k(f) + S_{r-k}(f) \leq \log(k+1) + \log(r-k+1) \leq 2\log(\tfrac{r}{2}+1).$$

8. Summing the various contributions, we get

$$\begin{aligned} & S_{r,k}(f) \\ \geq\ & k(r-k)\log(r+1) - \tfrac{1}{2}k(r-k) - \tfrac{5}{4}\log(r+1) + \tfrac{5}{4}\log 2 - \tfrac{3}{4} - (r+1)\log 2 \\ & -\tfrac{3}{2}\log 2 + \tfrac{7}{8} - k(r-k) - \tfrac{1}{6}\log(\tfrac{r}{2}+1) \\ \geq\ & k(r-k)\log(r+1) - \tfrac{3}{2}k(r-k) - r\log 2 - \tfrac{17}{12}\log(r+2) - 0.626. \end{aligned}$$

□

Proposition 5.9. *Let $t \in \mathbb{R}_{\geq 1}$ and $k \in \mathbb{Z}_{\geq 1}$. The measure $P_{r,k,t}$ of the set of module lattices that admit a t-destabilising sublattice of rank k satisfies*

$$\begin{aligned} P_{r,k,t} \ &\leq\ \frac{\zeta_K^*(1)}{r\cdot|\Delta_K|^{\frac{k(r-k)}{2}}} \cdot \left(\binom{r}{k}\frac{\prod_{j=2}^{k}\zeta(j)\prod_{j=2}^{r-k}\zeta(j)\prod_{j=1}^{r}V_j}{\prod_{j=1}^{k}V_j\prod_{j=1}^{r-k}V_j}\right)^{r_1} \\ &\quad \cdot \left(\binom{r}{k}2^{k(r-k)}\frac{\prod_{j=2}^{k}\zeta(j)^2\prod_{j=2}^{r-k}\zeta(j)^2\prod_{j=1}^{r}V_{2j}}{\prod_{j=1}^{k}V_{2j}\prod_{j=1}^{r-k}V_{2j}}\right)^{r_2} \cdot t^{-r} \\ &\leq\ \frac{\zeta_K^*(1)}{|\Delta_K|^{\frac{k(r-k)}{2}}}\left(0.8\cdot(r+4)^2\cdot 2^{\frac{3r}{2}}\cdot\left(\frac{28.2}{r+2}\right)^{\frac{k(r-k)}{2}}\right)^{r_1} \\ &\quad \cdot\left(53\cdot(r+2)^2\cdot 4^r\cdot\left(\frac{28.2}{r+1}\right)^{k(r-k)}\right)^{r_2}\cdot t^{-r}. \end{aligned}$$

Proof. From Lemma 5.6, write

$$c(r,k) = \frac{\zeta_K^*(1)}{r}\binom{r}{k}^{r_u+1}\left(\frac{\pi^{\frac{r_1}{2}}(2\pi)^{r_2}}{|\Delta_K|^{\frac{1}{2}}}\right)^{k(r-k)} Z G_1^{r_1} G_2^{r_2}$$

where

$$Z = \frac{\prod_{j=2}^{k}\zeta_K(j)\prod_{j=2}^{r-k}\zeta_K(j)}{\prod_{j=2}^{r}\zeta_K(j)},$$

$$G_1 = \frac{\prod_{j=1}^{k}\Gamma(\frac{j}{2}+1)\prod_{j=1}^{r-k}\Gamma(\frac{j}{2}+1)}{\prod_{j=1}^{r}\Gamma(\frac{j}{2}+1)}$$

and

$$G_2 = \frac{\prod_{j=1}^{k}\Gamma(j+1)\prod_{j=1}^{r-k}\Gamma(j+1)}{\prod_{j=1}^{r}\Gamma(j+1)}.$$

By Lemma 5.7 we have $Z \leq (2.3)^{2d} = (2.3)^{2r_1}(2.3)^{4r_2}$. By Lemma 5.8, we have

$$G_1 \leq \exp(-\tfrac{1}{2}k(r-k)\log(\tfrac{r}{2}+1) + \tfrac{3}{4}k(r-k) + r\tfrac{\log 2}{2} + \tfrac{47}{24}\log(r+4) - 1.89)$$

and

$$G_2 \leq \exp(-k(r-k)\log(r+1) + \tfrac{3}{2}k(r-k) + r\log 2 + \tfrac{17}{12}\log(r+2) + 0.626).$$

Using the trivial bound $\binom{r}{k} \leq 2^r$ and putting the terms together gives the result. □

We now quantify the fact that semistable lattices are balanced. This bound is implicitly present in the proof of [Gra84, Theorem 5.1].

Lemma 5.10. *Let L be a module lattice of rank r and let $t \geq 1$.*

1. *If L does not admit a t-destabilising sublattice of rank 1, then*

$$\lambda_1(L) > t^{-\frac{1}{d}}|\Delta_K|^{-\frac{1}{2d}}\det(L)^{\frac{1}{n}}.$$

2. *If L does not admit a t-destabilising sublattice of rank $n-1$, then*

$$\lambda_n(L) < nt^{\frac{1}{d}}|\Delta_K|^{\frac{1}{2d}}\det(L)^{\frac{1}{n}}.$$

If L is semistable then $\lambda_1(L) \geq |\Delta_K|^{-\frac{1}{2d}}\det(L)^{\frac{1}{n}}$ and $\lambda_n(L) \leq n|\Delta_K|^{\frac{1}{2d}}\det(L)^{\frac{1}{n}}$.

Proof.

1. We prove the contrapositive. Suppose that the bound is not satisfied, and let $x \in L$ be such that
$$\|x\| \leq t^{-\frac{1}{d}}|\Delta_K|^{-\frac{1}{2d}}\det(L)^{\frac{1}{n}}.$$
Then the rank 1 sublattice $L' = \mathcal{O}_K x$ satisfies
$$\det(\mathcal{O}_K x) = \|x\|^d|\Delta_K|^{1/2} \leq t^{-1}\det(L)^{\frac{1}{r}},$$
so that L' is t-destabilising.

2. Assume L does not admit a t-destabilising sublattice of rank $n-1$, then $L^\vee$ does not admit a t-destabilising sublattice of rank 1. By the first part of the lemma, we have
$$\lambda_1(L^\vee) > t^{-\frac{1}{d}}|\Delta_K|^{-\frac{1}{2d}}\det(L)^{-\frac{1}{n}}.$$
Finally, Banaszczyk's theorem [Ban93, Theorem (2.1)] gives
$$\lambda_n(L) < nt^{\frac{1}{d}}|\Delta_K|^{\frac{1}{2d}}\det(L)^{\frac{1}{n}}.$$

If L is semistable, then both inequalities hold for every $t > 1$, yielding the result by letting $t \to 1$. □

Piecing together the results above, we prove the main result of this section.

Proof of Theorem 4. We will use the notation of Proposition 5.9.

First suppose that $r \geq 225$ and take $t = 1$. Applying Lemma 2.34, we can bound

$$\frac{\zeta_K^*(1)}{|\Delta_K|^{\frac{k(r-k)}{2}}} \leq \frac{1}{|\Delta_K|^{\frac{k(r-k)-1}{2}}} \leq 1.$$

We also bound

$$\begin{aligned} & 0.8 \cdot (r+4)^2 \cdot 2^{\frac{3r}{2}} \cdot \Big(\frac{28.2}{r+2}\Big)^{\frac{k(r-k)}{2}} \\ \leq\ & 0.8 \cdot (r+4)^2 \cdot 2^{\frac{3r}{2}} \cdot \Big(\frac{28.2}{r+2}\Big)^{\frac{r-1}{2}} \text{ since } r+2 > 28.2 \\ \leq\ & O(r^{\frac{5}{2}}) \cdot \Big(\frac{2^3 \cdot 28.2}{r+2}\Big)^{\frac{r}{2}} \\ \leq\ & O(r^{\frac{5}{2}}) \cdot \Big(\frac{225.6}{r+2}\Big)^{\frac{r}{2}} \\ =\ & 2^{-\Omega(r \log r)}, \end{aligned}$$

and similarly

$$\begin{aligned} & 53 \cdot (r+2)^2 \cdot 4^r \cdot \Big(\frac{28.2}{r+1}\Big)^{k(r-k)} \\ \leq\ & 53 \cdot (r+2)^2 \cdot 4^r \cdot \Big(\frac{28.2}{r+1}\Big)^{r-1} \\ \leq\ & O(r^3) \cdot \Big(\frac{4 \cdot 28.2}{r+1}\Big)^{r} \\ =\ & 2^{-\Omega(r \log r)}, \end{aligned}$$

so that in those cases we indeed have $P_{r,k,1} \leq 2^{-\Omega(dr \log r)}$.

Now for $4 \leq r \leq 224$, we apply the Odlyzko–Serre bound [Poi77]:

$$|\Delta_K| \geq (A^{r_1} B^{2r_2})^{1+o(1)} \text{ as } d \to \infty,$$

where $A = 4\pi \exp(1+\gamma)$, $B = 4\pi \exp(\gamma)$ and γ is Euler's constant. For each such r, each $0 < k < r$ and $t = 1$, we evaluate the explicit formula for the first bound in Proposition 5.9, inserting $A^{-\frac{k(r-k)-1}{2}}$ in the r_1 term and $B^{-k(r-k)+1}$ in the r_2 term, and we check that both expressions are strictly less than 1. This proves that for each such r and k, we have $P_{r,k,1} = 2^{-\Omega(d)}$.

Now assume $r = 2$. The bound from Proposition 5.9 is

$$P_{2,1,t} \leq \frac{1}{2} \cdot \frac{\zeta_K^*(1)}{|\Delta_K|^{\frac{1}{2}}} \pi^{r_1} (2\pi)^{r_2} t^{-2}.$$

Using Lemma 2.34 we bound

$$\zeta_K^*(1) |\Delta_K|^{-\frac{1}{2}} \leq \left(\frac{e \log |\Delta_K|}{2(d-1)}\right)^{d-1} |\Delta_K|^{-\frac{1}{2}} \leq \left(\frac{e}{2} \frac{d}{d-1} \frac{\log \delta}{\delta^{\frac{1}{2}}}\right)^{d-1}.$$

We obtain

$$P_{2,1,t} \leq \left((1+o(1)) \frac{\pi e}{2} \frac{\log \delta}{\delta^{\frac{1}{2}}}\right)^{d-1} \cdot O(t^{-2}).$$

For the stated choice of t, this is $2^{-\Omega(d)}$. When $\delta \geq 845$, we have $t = 1$.

Finally, assume $r = 3$. The bound from Proposition 5.9 is

$$P_{3,k,t} \leq \frac{1}{3} \cdot \frac{\zeta_K^*(1)}{|\Delta_K|} \left(\frac{\pi^3}{3}\right)^{r_1} \left(\frac{\pi^6}{18}\right)^{r_2} t^{-3}.$$

Using Lemma 2.34 again we bound

$$\zeta_K^*(1) |\Delta_K|^{-1} \leq \left(\frac{e}{2} \frac{d}{d-1} \frac{\log \delta}{\delta}\right)^{d-1}.$$

We obtain

$$P_{3,k,t} \leq \left((1+o(1))\frac{\pi^3 e}{6}\frac{\log\delta}{\delta}\right)^{d-1} \cdot O(t^{-3}).$$

For the stated choice of t, this is $2^{-\Omega(d)}$. When $\delta \geq 57.5$, we have $t = 1$.

We obtain the last statement by applying Lemma 5.10 and noting that the values of t for $r = 2$ and $r = 3$ satisfy $t^{\frac{1}{d}} = O(1)$. □

6 Cutting cusps: reduction to the flare

The goal of this section is to prove Theorem 5 below, which reduces worst-case SIVP instances to SIVP in lattices which are (mildly) balanced.

Theorem 5 (Reduction to the flare)**.** *Let L be an $\mathcal{O}_K$-module lattice of rank r, and $\gamma \geq 1$. There is a polynomial time reduction from $\gamma \cdot (1+\varepsilon)^{r-1}$-SIVP in L to γ-SIVP in at most r module lattices $L_1, \ldots, L_t$, where each L_i is of rank r and $\Gamma_K^2 2^{\frac{3}{2}(rd-1)}$-balanced, and $\varepsilon < \frac{d}{2^{(rd+1)/2}}$.*

We proceed in two steps. In Section 6.1, we prove that if the given lattice L is very imbalanced (it is *in the cusp*), then a polynomial time lattice-basis reduction like LLL can detect gaps between the successive minima, and exploit them to split L into lattices of smaller dimension with smaller gaps. In order to preserve the dimension, we then show in Section 6.2 that SIVP in these lattices of smaller dimension reduces to SIVP in lattices of the original dimension, but now with balancedness guarantees: they are now *in the flare*.

6.1 Splitting imbalanced lattices into smaller dimensions

To reduce to (mildly) balanced lattices, we start by showing in Lemma 6.1 that large gaps between successive minima can be detected in polynomial time. Once we know where such a gap is, we show in Lemma 6.2 how to find generators of the "denser" sublattice (reaching all first minima up to the gap). Then, in Lemma 6.3, we show how SIVP in the original lattice reduces to SIVP in this denser sublattice, and in a lattice of complementary dimension. Essentially, this splits the original lattice around the gap, resulting in two lattices of smaller dimension and with one fewer (large) gap.

Finally, Lemma 6.5 applies this splitting recursively, resulting in a collection of lattices of smaller dimension with no remaining (large) gap.

Lemma 6.1. *There is a polynomial time algorithm such that the following holds. Let L be an $\mathcal{O}_K$-module lattice of rank r, with successive K-minima $\lambda_1^K, \ldots, \lambda_r^K$. Given $\alpha > 0$ and a basis of L, the algorithm either asserts that $\lambda_{i+1}^K/\lambda_i^K \leq \alpha\Gamma_K 2^{rd-1}$ for all i, or returns an index k such that $\lambda_{k+1}^K/\lambda_k^K > \alpha$.*

Proof. Let $(u_i)_{i=1}^{rd}$ be a family of linearly independent vectors in L with $\|u_i\| = \lambda_i = \lambda_i(L)$. One can compute in polynomial time an LLL-reduced basis $(b_i)_i$ of L. By [LLL82, Proposition 1.12] for any i we have

$$\|b_i\| \leq 2^{(rd-1)/2}\lambda_i.$$

The algorithm searches for an index j such that $\|b_{j+d}\|/\|b_j\| > \alpha\Gamma_K 2^{(rd-1)/2}$, and if it exists, returns $k = \lceil j/d \rceil$. If there is no such j, the algorithm asserts that $\lambda_{i+1}^K/\lambda_i^K \leq \alpha\Gamma_K 2^{rd-1}$ for all i. We prove correctness in two parts:

- Assume a valid j is found. We have

$$\frac{\lambda_{k+1}^K}{\lambda_k^K} \geq \frac{\lambda_{j+d}}{\Gamma_K \lambda_j} \geq \frac{\|b_{j+d}\|}{2^{(rd-1)/2}\Gamma_K\|b_j\|} > \alpha,$$

  as expected.

- Assume there exists an index k such that $\lambda_{k+1}^K/\lambda_k^K > \beta 2^{(rd-1)/2}$. Let j be the largest index reaching $\lambda_j = \lambda_k^K$ (in particular, $\lceil j/d \rceil = k$). Applying Lemma 2.13, we obtain

$$\frac{\|b_{j+d}\|}{\|b_j\|} \geq \frac{\lambda_{j+d}}{2^{(rd-1)/2}\lambda_j} \geq \frac{\lambda_{k+1}^K}{2^{(rd-1)/2}\lambda_k^K} > \beta.$$

  The contraposition, with $\beta = \alpha\Gamma_K 2^{(rd-1)/2}$, states that if the algorithm finds no valid index j, then $\lambda_{i+1}^K/\lambda_i^K \leq \alpha\Gamma_K 2^{rd-1}$ for all i.

This proves that the algorithm has the claimed property. □

Lemma 6.2. *There is a polynomial time algorithm such that the following holds. Let L be an $\mathcal{O}_K$-module lattice of rank r, with successive K-minima $\lambda_1^K, \ldots, \lambda_r^K$. Given a basis of L and an index k such that $\lambda_{k+1}^K/\lambda_k^K > \Gamma_K 2^{(rd-1)/2}$, the algorithm returns a basis of the unique primitive sub-module $L' \subset L$ of rank k with $\lambda_i^K(L') = \lambda_i^K$ for all $i \leq k$.*

Proof. One can compute in polynomial time an LLL-reduced basis $(b_i)_i$ of L. Let j be the smallest index such that $\mathrm{span}_K(b_1, \ldots, b_j)$ has K-rank k (in particular, $j \leq (k-1)d + 1$). For any $i \leq j$, we have

$$\|b_i\| \leq 2^{(rd-1)/2}\lambda_i \leq 2^{(rd-1)/2}\lambda_j \leq \Gamma_K 2^{(rd-1)/2}\lambda_{\lceil j/d \rceil}^K \leq \Gamma_K 2^{(rd-1)/2}\lambda_k^K < \lambda_{k+1}^K.$$

Let $V = \mathrm{span}_K(x \in L \mid \|x\| < \lambda_{k+1}^K)$. The vectors $(b_1, \ldots, b_j)$ are all in V. Therefore, $\mathrm{span}_K(b_1, \ldots, b_j)$ is a K-subspace of V of K-rank k. By definition of λ_{k+1}^K, the space V has K-rank at most k, and we deduce that $(b_1, \ldots, b_j)$ generates V. From this generating set of V and the provided basis of L, we can deduce a basis of the sub-module $L' = L \cap V$ in polynomial time, which proves the lemma. □

Lemma 6.3. *Suppose L is an $\mathcal{O}_K$-module lattice of rank r, with successive K-minima $\lambda_1^K, \ldots, \lambda_r^K$. Let k be an index such that $\beta = \lambda_{k+1}^K/\lambda_k^K > \Gamma_K 2^{(rd-1)/2}$. Then, given k, there is a polynomial time reduction from $\gamma \cdot (1+\varepsilon)$-SIVP in L to γ-SIVP in two module lattices of rank k and $r-k$, with $\varepsilon = \frac{d\Gamma_K}{2\beta} < \frac{d}{2^{(rd+1)/2}}$.*

Proof. From Lemma 6.2, one can compute in polynomial time a basis of the unique sub-module $L' \subset L$ of rank k with $\lambda_i^K(L') = \lambda_i^K$ for all $i \leq k$.

Let $(u_i)_{i=1}^{rd}$ be a family of linearly independent vectors in L with $\|u_i\| = \lambda_i$. Let us start with finding a good basis of L'. Applying the γ-SIVP oracle to L' we can find $w_i \in L'$ such that $\|w_i\| \leq \gamma\lambda_{kd}(L')$. By Lemma 2.13, we have

$$\lambda_{kd}(L') \leq \Gamma_K \lambda_k^K(L') \leq \Gamma_K \lambda_k^K \leq (\Gamma_K/\beta)\lambda_{k+1}^K \leq (\Gamma_K/\beta)\lambda_{rd}.$$

We deduce $\|w_i\| \leq \gamma(\Gamma_K/\beta)\lambda_{rd}$. In particular, $\|w_i\| < \gamma\lambda_{rd}$.

Let us now complete $(w_i)_{i=1}^{kd}$ to a good basis of L. Let $V = \mathrm{span}_K(L)$ and $W = \mathrm{span}_K(L')$, and consider the orthogonal projection $\pi : V \to W^\perp$. Then, $L_\pi = \pi(L)$ is a module lattice of rank $r-k$. We have $\|\pi(u_i)\| \leq \|u_i\| = \lambda_i$. Applying the γ-SIVP oracle to L_π we can find $z_i \in L$ such that $0 < \|\pi(z_i)\| \leq \gamma\lambda_{(r-k)d}(L_\pi) \leq \gamma\lambda_{rd}$. We can assume each z_i to be reduced with respect to the basis $(w_i)_i$ of W, so $z_i = \pi(z_i) + \sum_i \mu_i w_i$ with $|\mu_i| < 1/2$. Recall that $\|w_i\| \leq \gamma(\Gamma_K/\beta)\lambda_{rd}$, so

$$\begin{aligned}\|z_i\| \leq \|\pi(z_i)\| + \sum_i |\mu_i|\|w_i\| &\leq \gamma\lambda_{rd} + (d/2)\gamma(\Gamma_K/\beta)\lambda_{rd} \\ &= \gamma\left(1 + \frac{d\Gamma_K}{2\beta}\right)\lambda_{rd}.\end{aligned}$$

Therefore, $(w_1, \ldots, w_{kd}, z_1, \ldots, z_{(r-k)d})$ is a solution of $\gamma \cdot (1+\varepsilon)$-SIVP for L. □

Lemma 6.4. *Suppose L is an $\mathcal{O}_K$-module lattice of rank r. There is a polynomial time algorithm which either asserts that L is $\Gamma_K^2 2^{\frac{3}{2}(rd-1)}$-balanced, or reduces $\gamma \cdot (1+\varepsilon)$-SIVP in L to γ-SIVP in two module lattices L_1 and L_2 with $\mathrm{rank}_K(L_1) + \mathrm{rank}_K(L_2) = r$ and $\mathrm{rank}_K(L_i) < r$, with $\varepsilon < \frac{d}{2^{(rd+1)/2}}$.*

Proof. This is a combination of Lemma 6.1 (detecting gaps) and Lemma 6.3 (exploiting gaps). □

Lemma 6.5 (Reduction to balanced lattices of smaller dimension)**.** *Let L be an $\mathcal{O}_K$-module lattice of rank r, and $\gamma \geq 1$. There is a polynomial time reduction from $\gamma \cdot (1+\varepsilon)^{r-1}$-SIVP in L to γ-SIVP in at most r module lattices $L_1, \ldots, L_t$, with*

- $\varepsilon < \frac{d}{2^{(rd+1)/2}}$,
- $\sum_{i=1}^t \mathrm{rank}_K(L_i) = r$,
- *each L_i is $\Gamma_K^2 2^{\frac{3}{2}(\mathrm{rank}_K(L_i)d-1)}$-balanced.*

Proof. This follows from a recursive application of Lemma 6.4, and the fact that a rank-1 lattice is necessarily Γ_K-balanced (hence $\Gamma_K^2 2^{\frac{3}{2}(d-1)}$-balanced). The recursion has depth at most $r-1$ since the quantity $\sum_{i=1}^t \mathrm{rank}_K(L_i) = r$ is constant and t can only increase. □

6.2 Back to the original dimension

The previous section shows how to reduce SIVP in an imbalanced lattice into SIVP instances in balanced lattices, but these lattices have smaller dimension. We would like the computational reduction to preserve the dimension. Reducing the dimension sounds good in practice, but *a priori*, there could exist r such that the average case in dimension $r-1$ is harder than the average case in dimension r. To resolve this concern, in this section, we prove that SIVP is lattices of smaller dimension reduces to SIVP in lattices of the original dimension r.

Lemma 6.6 (Increasing the dimension)**.** *Suppose L is an α-balanced $\mathcal{O}_K$-module lattice of rank $k < r$. There is a polynomial time reduction from γ-SIVP in L to γ-SIVP in a $\max(\alpha, \sqrt{k}, \sqrt{d} \cdot \Gamma_K)$-balanced $\mathcal{O}_K$-module lattice of rank r.*

Proof. Let $O = \mathcal{O}_K^{r-k}$ be the orthogonal $\mathcal{O}_K$-lattice of rank $r-k$. Let $x > 0$ and $M = L \oplus xO$. Let us prove that with $x = \det(L)^{\frac{1}{kd}}$, we have that M is $\max(\alpha, \sqrt{kd}, \Gamma_K)$-balanced, and $\lambda_{rd}(M) \leq \lambda_{kd}(L)$. We have

$$\lambda_1^K(L) = \lambda_1(L) \leq \sqrt{kd} \det(L)^{\frac{1}{kd}} = \sqrt{kd} \cdot x,$$

and

$$x = \det(L)^{\frac{1}{kd}} \leq \left(\prod_{i=1}^{kd} \lambda_i(L) \right)^{\frac{1}{kd}} \leq \lambda_{kd}(L) \leq \Gamma_K \lambda_k^K(L).$$

Since $\lambda_1(x\mathcal{O}_K) = x\sqrt{d}$, we deduce that $\lambda_1^K(L)/\sqrt{k} \leq \lambda_1(x\mathcal{O}_K) \leq \sqrt{d} \cdot \Gamma_K \lambda_k^K(L)$. Since M is an orthogonal sum of L and copies of $x\mathcal{O}_K$, we deduce that M is $\max(\alpha, \sqrt{k}, \sqrt{d} \cdot \Gamma_K)$-balanced. From $x \leq \lambda_{kd}(L)$, we deduce that $\lambda_{rd}(M) \leq \lambda_{kd}(L)$. Therefore, a solution of γ-SIVP for M, projected orthogonally down to L, is a solution of γ-SIVP for L. □

We now have all the ingredients to prove the main result of this section.

Proof of Theorem 5. This is the composition of Lemma 6.5 and Lemma 6.6, and the fact that

$$\max\left(\Gamma_K^2 2^{\frac{3}{2}(\mathrm{rank}_K(L_i)d-1)}, \sqrt{\mathrm{rank}_K(L_i)}, \sqrt{d} \cdot \Gamma_K \right) \leq \Gamma_K^2 2^{\frac{3}{2}(rd-1)}.$$

□

7 Reduction from the flare to the bulk

We will use Section 4 and Section 5 to show that we have an algorithm, based on Hecke equidistribution, that can handle α-balanced module lattices L with $\log \alpha \ll \log d$. Section 6 shows that we can reduce to module lattices that are α-balanced with $\alpha \ll \Gamma_K^2 \cdot 2^{O(d)}$. There remains a gap between these two regimes. Thus, we are left with further reducing from lattices not too high in the cusp, with α exponential in d, to those in the bulk, where α is only polynomial in d. We informally call this "intermediate" part of the space of module lattices the *flare*, see Figure 1.

The strategy is the following. Take an α-balanced lattice L with α at most 2^d, for simplicity. Thus, the range where the gaps $\lambda_{i+1}^K(L)/\lambda_i^K(L)$ could lie is $[1, 2^d]$. We split this range into dyadic intervals, of which there are only d many, and *guess* in which of these the first gap $\lambda_2^K(L)/\lambda_1^K(L)$ lies. Assuming the correct guess, we apply a Hecke operator, that is, we randomly consider a certain type of sublattice of index p, where p lies in the respective dyadic interval. With high probability, because $p \ll \lambda_2^K(L)/\lambda_1^K(L)$, taking such a sublattice only increases the length of the shortest vector and the result has a first gap $\lambda_2^K(L)/\lambda_1^K(L)$ of size $\asymp 1$. Morally, the other successive minima are not impacted, but in practice we prove that they are only potentially multiplied by a polynomial in d.

Having reduced the first gap, we continue with the second, and so forth. However, one must use different Hecke operators for this. For instance, if $\lambda_1^K \asymp \lambda_2^K \asymp p^{-1}\lambda_3^K$, then we wish to increase the volume of a rank 2 dense sublattice, taking care not to reopen the first gap. This can be achieved by considering another family of sublattices as above, with a different structure inside L. Following all steps up to the last gap, with high probability, we can obtain a sublattice with gaps bounded by a polynomial in d, depending on r.

At the level of Hecke operators, closing all gaps conceptually uses an entire set of generators for the local Hecke algebra. We also note that this procedure is expensive in terms of the rank r, but provides a good algorithm in terms of d.

7.1 Closing one gap

The following implements the idea that, given a gap in the successive minima, carefully choosing a sublattice in terms of the size of that gap can effectively *close* or shrink it. It is the main tool of this section.

Lemma 7.1. *Let L be a module lattice of rank r with $\lambda_1^K, \dots, \lambda_r^K$ its K-minima. Assume that there exists $n \in \mathbb{Z}$, $n \geq 2$, such that $\lambda_{k+1}^K \geq n\lambda_k^K$ for some $k < r$. Let M be the primitive sub-module of rank k containing the vectors of length at most λ_k^K. Assume that $L_n \subset L$ is a sub-module of rank r such that L/L_n is isomorphic to $(\mathcal{O}_K/n\mathcal{O}_K)^k$ and nM is primitive in L_n. Then*

$$\lambda_i^K(L_n) = n\lambda_i^K, \quad i = 1, \dots, k,$$

and

$$\lambda_i^K \leq \lambda_i^K(L_n) \leq \left(1 + \frac{\Gamma_K\sqrt{kd}}{2}\right)\lambda_i^K, \quad i = k+1, \dots, r.$$

Proof. We start by noting that M is well-defined. Indeed, since $\lambda_{k+1}^K > \lambda_k^K$, the vectors of length up to λ_k^K have a K-span of dimension k. We can now define M to be the maximal sub-module of rank k containing these vectors and we recall Definition 2.4.

Since nM is primitive in L_n, we can find a sub-module $M' \subset L_n$ such that $L_n = nM \oplus M'$. We have $L_n \subset M \oplus M' \subset L$ and, computing indices, we find that $L = M \oplus M'$.

For any $i \in \{1, \dots k\}$, we clearly have the inequality $\lambda_i^K(L_n) \leq n\lambda_i^K(L)$. To prove the inverse inequality, assume that there exist K-independent vectors $w_1, \dots, w_i \in L_n$ with lengths strictly smaller than $n\lambda_i^K(L)$. The lengths of $w_1, \dots, w_i$ are also strictly smaller than $\lambda_{k+1}^K(L)$,

by assumption. Therefore, by definition of the successive minima, the K-span of these vectors is included in the K-span of M. We can therefore deduce that

$$\mathrm{span}_K(w_1, \dots w_i) \subset K \cdot M = K \cdot nM.$$

Next, because nM is primitive in L_n, we have

$$K \cdot nM \cap L_n = nM.$$

It follows that the vectors $w_1, \dots, w_i$ lie in nM. Dividing by n, we obtain i K-linearly independent vectors $w_1/n, \dots, w_i/n$ in $M \subset L$. Since n is a rational number, their lengths are simply $\|w_1\|/n, \dots, \|w_i\|/n$. These are strictly smaller than $\lambda_i^K(L)$ by assumption, so we reach a contradiction.

We now consider the other successive minima. Let $(u_i)_{i \leq r}$ be a K-linearly independent family of vectors in L with $u_i = v_i + w_i$, where $v_i \in M$, $w_i \in M'$, and $\|u_i\| = \lambda_i^K$ for each $i \in \{1, \dots, r\}$. In particular, $u_i \in M$ if $i \leq k$.

For each $i > k$, let $v_i' \in nM$ be the closest vector to v_i, so that

$$\|v_i' - v_i\| \leq \mathrm{cov}(nM) \leq \frac{\sqrt{kd}}{2}\lambda_{kd}(nM) \leq \Gamma_K \frac{\sqrt{kd}}{2} n\lambda_k^K \leq \Gamma_K \frac{\sqrt{kd}}{2}\lambda_i^K,$$

where M is the covering radius of a lattice M and we use the inequality given in [MG02, Thm. 7.9]. Let $u_i' = v_i' + w_i \in L_n$. By construction, $(u_1, \dots, u_k, u_{k+1}', \dots, u_r')$ are K-linearly independent. Furthermore,

$$\|u_i'\| = \|v_i' + w_i'\| \leq \|v_i' - v_i'\| + \|v_i + w_i'\| \leq \Gamma_K \frac{\sqrt{kd}}{2}\lambda_i^K + \lambda_i^K,$$

which proves the result. □

In the previous lemma, we consider specific sublattices L_n of L, formed by scaling a fixed submodule M, containing short vectors, by n. Conversely, we now consider how many sublattices with the same structure can be formed this way. We first start with n replaced by a prime ideal.

Lemma 7.2. *The number of sublattices $L' \subset L$ such that $L/L' \cong (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)^k$ is given by*

$$\frac{(1-q^r)\cdots(1-q^{r-k+1})}{(1-q)\cdots(1-q^k)},$$

where $q = |F| = N(\mathfrak{p})$. Out of these, given a fixed primitive sub-module $M \subset L$ of rank k, the number of sublattices L' such that $\mathfrak{p}M$ is primitive in L' is

$$q^{k(r-k)}.$$

Proof. Any sublattice L' as in the statement satisfies $\mathfrak{p}L \subset L' \subset L$. As such, they correspond bijectively to subspaces of dimension $r-k$ of the vector space $L/\mathfrak{p}L \cong F^r$ over the field $F := \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$. It is well-known that the number of such subspaces is given by the Gaussian binomial coefficient, by definition given by the formula in the first part of the lemma.

For the second part of the lemma, recall that $\mathfrak{p}M$ is primitive in L' if and only if $L' \cap \mathrm{span}(\mathfrak{p}M) = \mathfrak{p}M$, as in Definition 2.4. Since M is also primitive in L, we have

$$L' \cap \mathrm{span}(\mathfrak{p}M) = L' \cap L \cap \mathrm{span}(M) = L' \cap M.$$

Thus, we are counting L' as above such that $L' \cap M = \mathfrak{p}M$.

If $L' \cap M = \mathfrak{p}M$, then $L' \cap (M + \mathfrak{p}L) = (L' \cap M) + \mathfrak{p}L$ (since $\mathfrak{p}L \subset L'$), so $L' \cap (M + \mathfrak{p}L) = \mathfrak{p}L$. In other words, the images of L' and M inside the vector space $L/\mathfrak{p}L$ should have trivial intersection.

Conversely, if $L' \cap (M + \mathfrak{p}L) = \mathfrak{p}L$, then $L' \cap M \subset \mathfrak{p}L$. Since $\mathfrak{p}L = \mathfrak{p}M + \mathfrak{p}M'$ for some sub-module M' by primitivity, we can also deduce that $\mathfrak{p}L \cap M = \mathfrak{p}M$, since $\mathfrak{p}M$ is primitive in L. Therefore, $L' \cap M \subset \mathfrak{p}L \cap M \subset \mathfrak{p}M$ and the reverse inclusion is obvious.

Let $V = L/\mathfrak{p}L$ and U be the image of M inside V, a subspace of dimension $k = \operatorname{rank} M$. The previous paragraphs show that the sublattices L' as in the statement are in bijection with $(r-k)$-dimensional subspaces $W \subset V$ that intersect trivially with U. We can study these using the action of $\mathrm{GL}_r(F)$ on $(r-k)$-dimensional subspaces (the Grassmannian). Indeed, we can choose a basis $e_1, \ldots, e_r$, such that $(e_{r-k+1}, \ldots, e_r)$ forms a basis for U. Then any $(r-k)$-dimensional subspace of V can be given as $\operatorname{span}(ge_1, \ldots, ge_{r-k})$ for some $g \in \mathrm{GL}_r(F)$.

The stabilizer of $W_0 := \operatorname{span}(e_1, \ldots, e_{r-k})$ under this action is given by the subgroup

$$H = \left\{ g = \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \mid A \in \mathrm{GL}_{r-k}(F), D \in \mathrm{GL}_k(F), B \in \mathcal{M}_{r-k,k}(F) \right\}.$$

Let now $W = g \cdot W_0$ be some $(r-k)$-dimensional subspace. Write

$$g = \begin{pmatrix} S & T \\ U & V \end{pmatrix}$$

as a block matrix, analogously to the description of H, and suppose we multiply g from the right by an element

$$\begin{pmatrix} A & 0 \\ 0 & \mathrm{id} \end{pmatrix} \in H.$$

This would replace S by $S \cdot A$ and we can therefore assume that S is in column echelon form (by Gauss elimination), that is, in lower triangular shape.

Assume now that $W \cap U = 0$. This implies that, if $S = (s_{ij})_{1 \le i,j \le r-k}$, then $s_{r-k,r-k} \neq 0$. Otherwise, since S is lower triangular, we would have the vector $g \cdot e_{r-k}$ in the intersection $W \cap U$. Multiplying by another matrix in H, we can assume that $s_{r-k,r-k} = 1$ (we are working over a field) and that the rest of the last row of S is zero. The same argument now reiterates to show that $s_{r-k-1,r-k-1} \neq 0$, and so on, allowing us to assume that $S = \mathrm{id}_{r-k}$.

In this form, we can multiply g from the right by

$$\begin{pmatrix} \mathrm{id} & -T \\ 0 & \mathrm{id} \end{pmatrix} \in H$$

and reduce to $T = 0$. This now implies that V must be invertible and another multiplication by an element of H allows us to assume that $V = \mathrm{id}_k$.

We have thus found representatives

$$g = \begin{pmatrix} \mathrm{id} & 0 \\ U & \mathrm{id} \end{pmatrix}$$

for all $(r-k)$-dimensional subspaces W such that $W \cap U = 0$. It is easy to see that these form a system of representatives (one for each coset of H). Since $U \in \mathcal{M}_{k,r-k}(F)$ is free, we have $q^{k(r-k)}$ such representatives. □

Lemma 7.3. *Let $p \in \mathbb{Z}$ be a prime and suppose we have the decomposition $p\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{p}_i$ (where we allow ramification). Let L be a module lattice of rank r over K with a given primitive sub-module M of rank k. For every $i \in \{0, \ldots, g\}$, compute L_i inductively and probabilistically as follows:*

- *define $L_0 = L$;*
- *given L_i, define L_{i+1} as a random sub-module of L_i such that $L_i/L_{i+1} \cong (\mathcal{O}_K/\mathfrak{p}_i\mathcal{O}_K)^k$.*

The lattice L_g contains pM as a primitive sub-module with probability at least $1 - d/(p-1)$.

Proof. We use Lemma 7.2 at each stage, with M equal to $M, \mathfrak{p}_1 M, \mathfrak{p}_1\mathfrak{p}_2 M, \ldots, pM$, successively. Let $q_i = N(\mathfrak{p}_i)$. At step i, the probability of the required outcome is

$$\frac{q_i^{k(r-k)}(q_i-1)\cdots(q_i^k-1)}{(q_i^r-1)\cdots(q_i^{r-k+1}-1)} \geq \frac{(q_i-1)\cdots(q_i^k-1)}{q_i\cdots q_i^k}$$

where we estimated $q_i^j - 1 \leq q_i^j$ in the denominator. It is now easy to see (e.g. inductively) that

$$\frac{(q_i-1)\cdots(q_i^k-1)}{q_i\cdots q_i^k} = \prod_{i=1}^{k}\left(1-\frac{1}{q^i}\right) \geq 1 - \sum_{i=1}^{k}\frac{1}{q^i} \geq 1 - \frac{1}{q-1}.$$

Writing $q_i = p^{\alpha_i}$, multiplying these bounds together and applying the same reasoning as above, we obtain the bound

$$\prod_{i=1}^{g}\left(1-\frac{1}{p^{\alpha_i}-1}\right) \geq 1 - \sum_{i}\frac{1}{p^{\alpha_i}-1} \geq 1 - \frac{d}{p-1},$$

using that $\alpha_i \geq 1$ and that $g \leq d$. □

Putting everything together, we obtain the gap-decreasing algorithm.

Proposition 7.4. *Let L be a rank r module lattice over a degree d number field K, with K-minima $\lambda_1^K, \ldots, \lambda_r^K$. Suppose that $\lambda_{k+1}^K \geq p\lambda_k^K$ for some prime p and $k < r$. The algorithm described in Lemma 7.3 then produces, with probability at least $1 - d/(p-1)$, a full-rank sub-module $L' \subset L$ of covolume p^{dk}, such that, if μ_i^K are its K-minima, then*

$$\mu_i^K = p\lambda_i^K, \quad i = 1, \ldots, k,$$

and

$$\lambda_i^K \leq \mu_i^K \leq \left(1 + \frac{\Gamma_K\sqrt{kd}}{2}\right)\lambda_i^K, \quad i = k+1, \ldots, r.$$

7.2 Reduction to balanced lattices

We now describe and analyze an algorithm for closing all gaps of a lattice. It is adequate for reducing SIVP for lattices with gaps of size 2^d to SIVP for lattices with gaps of polynomial size in d.

Theorem 6. *Let M be a $\mathbb{Z}_K$-module of rank $r > 1$; and let $t \in \mathbb{N}_{>2}$ be a parameter that satisfies $2^t \geq \left(1 + \frac{\Gamma_K\sqrt{r\cdot d}}{2}\right)^{r-1} \cdot \max_j \frac{\lambda_{j+1}^K(M)}{\lambda_j^K(M)}$. Then, with probability at least $(2t)^{-(r-1)}$, Algorithm 3 outputs a sub-module $N \subset M$ such that, for some primes $p_1, \ldots, p_{r-1}$ at most 2^t,*

- $\det(N) = \det(M) \cdot \prod_{i=1}^{r-1} p_i^{di}$.
- $\frac{\lambda_{i+1}^K(N)}{\lambda_i^K(N)} \leq 4d \cdot \left(1 + \frac{\Gamma_K\sqrt{i\cdot d}}{2}\right)$ *for all* $1 \leq i \leq r-1$.
- $\lambda_i^K(N) \leq \prod_{j=1}^{i-1}\left(1 + \frac{\Gamma_K\sqrt{j\cdot d}}{2}\right) \cdot \left(\prod_{s=i}^{r-1} p_s\right) \cdot \lambda_i^K(M)$. *for all* $1 \leq i \leq r$.

Moreover, this algorithm runs in polynomial time in the size of its input.

Algorithm 3 Finding a balanced sublattice

Require: A module lattice M of rank r, and a parameter $t \in \mathbb{N}_{>1}$.
Ensure: A sub-module $N \subset M$.

1: Put $N_0 = M$.
2: **for** $i = 1$ to $r - 1$ **do**
3: Pick $g_i \in \{2^1, 2^2, 2^3, \ldots, 2^t\}$ uniformly random. 'Guess the gap'
4: **if** $g_i \leq 4d$ **then**
5: Put $p_i = 1$ and $N_i = N_{i-1}$.
6: **else**
7: Pick a prime p_i satisfying $g_i/2 \leq p_i \leq g_i$.
8: Decompose $p_i = \prod_{j=1}^{g} \mathfrak{p}_j$ over K (with possible ramification).
9: Put $P_i := N_{i-1}$.
10: **for** $j = 1$ to g **do**
11: Take a random sub-module $P_j \subset P_{j-1}$ satisfying $P_{j-1}/P_j \simeq (\mathbb{Z}_K/\mathfrak{p}_j)^i$.
12: **end for**
13: Put $N_i = P_g$.
14: **end if**
15: **end for**
16: **return** $N := N_{r-1}$.

Proof. In this section, we use the notation

$$\gamma_i^K(L) = \frac{\lambda_{i+1}^K(L)}{\lambda_i^K(L)}$$

for a module lattice L and $i = 1, \ldots, r-1$. These signify the gaps between the K-successive minima.

For the first item, note that in the i-th step of the algorithm, $|P_{j-1}/P_j| = N(\mathfrak{p}_j)^i$. Hence, $|N_{i-1}/N_i| = \prod_{j=1}^{g} N(\mathfrak{p}_j)^i = p^{di}$ (with $d = [K : \mathbb{Q}]$). Therefore, taking the product over i yields $|N/M| = |N_r/N_0| = \prod_{i=1}^{r-1} p_i^{di}$, which gives the claim.

For the second item, recall the notation $\gamma_i^K(N') = \lambda_{i+1}^K(N')/\lambda_i^K(N')$ for any module N'. We follow the algorithm through steps $i = 1$ to $r-1$. We say that the 'gap guessing' in step 3 (of the i-th loop) is successful whenever either $g_i/2 \leq \gamma_i^K(N_{i-1}) \leq 2 \cdot g_i$. This happens with probability at least $1/t$. After choosing a prime p_i, as in step 5 and step 7, note that $1 \leq \gamma_i^K(N_{i-1})/p_i \leq 4d$ in this successful case.

Assume now that we are in the non-trivial case of $g_i > 4d$ and, thus, $p_i \geq g_i/2$. According to Corollary 7.4, with probability at least $1 - d/(p_i - 1) \geq 1/2$, the module N_i satisfies $\lambda_t^K(N_i) = p_i \lambda_t^K(N_{i-1})$ for $t \leq i$ and $\lambda_t^K(N_i) \leq \kappa_i \lambda_t^K(N_{i-1})$ for $t > i$, where we write $\kappa_i = 1 + \frac{\Gamma_K \sqrt{i \cdot d}}{2}$ for brevity. This is also true in the trivial case of $g_i \leq 4d$, where $p_i = 1$, with probability 1.

We assume for the rest of the proof that we are indeed in such a successful 'gap guessing' case, for all i. The probability computation follows at the end of this proof.

For all $\ell < i$, we have

$$\gamma_\ell^K(N_i) = \frac{\lambda_{\ell+1}^K(N_i)}{\lambda_\ell^K(N_i)} = \frac{\lambda_{\ell+1}^K(N_{i-1})}{\lambda_\ell^K(N_{i-1})} = \gamma_\ell^K(N_{i-1})$$

whereas for $\ell = i$, we have

$$\gamma_i^K(N_i) = \frac{\lambda_{i+1}^K(N_i)}{\lambda_i^K(N_i)} \leq \frac{\kappa_i \lambda_{i+1}^K(N_{i-1})}{p_i \lambda_i^K(N_{i-1})} = \frac{\kappa_i}{p_i} \cdot \gamma_i^K(N_{i-1}).$$

By induction, one can then conclude that

$$\gamma_i^K(N) = \gamma_\ell^K(N_{i-1}) = \frac{\kappa_i}{p_i} \cdot \gamma_i^K(N_{i-1}) \le 4d \cdot \kappa_i = 4d \cdot \left(1 + \frac{\Gamma_K \sqrt{i \cdot d}}{2}\right)$$

since we assumed that $\gamma_i^K(N_{i-1})/p_i \le 4d$.

For the bound on $\lambda_i^K(N)$, we use Corollary 7.4 again: $\lambda_j^K(N_i) = p_i \lambda_j^K(N_{i-1})$ for $j \le i$ and $\lambda_j^K(N_i) \le \kappa_i \lambda_j^K(N_{i-1})$ for $j > i$. Therefore,

$$\lambda_i^K(N) = \lambda_i^K(N_{r-1}) = \left(\prod_{s=i}^{r-1} p_s\right) \cdot \lambda_i^K(N_{i-1}) \le \left(\prod_{s=i}^{r-1} p_s\right) \cdot \left(\prod_{j=1}^{i-1} \kappa_j\right) \lambda_i^K(N_0),$$

which proves the third item.

As promised, we finish with the probability claim. For the entire algorithm to be successful, both the 'gap guessing' and the 'gap closing' should be successful in each of the i-steps. These success probabilities are $1/t$ and at least $1/2$, respectively. Since these are independent events, taking the product takes the overall success probability, yielding $(2t)^{-(r-1)}$. □

Corollary 7.5. *Let M be an $\mathcal{O}_K$-module lattice of rank $r > 1$, and $\gamma \ge 1$. Suppose M is α-balanced. Let $c_K = 1 + \frac{\Gamma_K \sqrt{r \cdot d}}{2}$. There is a polynomial time reduction which, given M and α, reduces $(c_K^{r-1} \cdot \gamma)$-SIVP in M to γ-SIVP in a rank-r module lattice N, where N is $(4d \cdot c_K)$-balanced with probability*

$$p = (2(r-1)\log_2(c_K) + 2\log_2(\alpha))^{-(r-1)}.$$

Proof. Let $t = (r-1)\log_2(c_K) + \log_2(\alpha)$. Algorithm 3 finds a sub-module $N \subseteq M$ satisfying the properties of Theorem 6 with probability

$$p = (2t)^{-(r-1)} = (2(r-1)\log_2(c_K) + 2\log_2(\alpha))^{-(r-1)}.$$

In that event, the module N is $(4d \cdot c_K)$-balanced. Furthermore, we have

$$\lambda_r^K(N) \le \prod_{j=1}^{r-1} \left(1 + \frac{\Gamma_K \sqrt{j \cdot d}}{2}\right) \cdot \lambda_r^K(M) \le c_K^{r-1} \lambda_r^K(M),$$

so a solution of γ-SIVP for N provides a solution of $(c_K^{r-1} \cdot \gamma)$-SIVP for M. □

Theorem 7 (Reduction to the bulk)**.** *Let $c_K = 1 + \frac{\Gamma_K \sqrt{r \cdot d}}{2}$, and $\varepsilon = \frac{d}{2^{(rd+1)/2}}$. Let O be an oracle which solves γ-SIVP for $(4d \cdot c_K)$-balanced rank-r module lattices. There is a randomized polynomial time algorithm which given access to O, solves $(c_K^{r-1} \cdot (1+\varepsilon)^{r-1} \cdot \gamma)$-SIVP with probability at least $1/2$. The expected number of oracle calls is $\mathrm{poly}_r(\log|\Delta_K|)$.*

Proof. Consider a rank-r module lattices or which we wish to solve $(c_K^{r-1} \cdot (1+\varepsilon)^{r-1} \cdot \gamma)$-SIVP. By Theorem 5, the problem reduces to $t \le r$ instances of $(c_K^{r-1} \cdot \gamma)$-SIVP in α-balanced module lattices, with $\alpha = \Gamma_K^2 2^{\frac{3}{2}(rd-1)}$. Let $k \in \mathbb{Z}_{>0}$ be a parameter to be tuned later. To each of these t instances, apply the reduction of Corollary 7.5 independently k times (and solve them using the oracle O), and keep the smallest response. For each of the t instances, the probability that the best-of-k solutions is small enough is $1 - (1-p_0)^k$ with

$$p_0 = (2(r-1)\log_2(c_K) + 2\log_2(\alpha))^{-(r-1)}$$

is the success probability from Corollary 7.5. The probability that all t instances are solved successfully is $(1-(1-p_0)^k)^t$. We have $(1-(1-p_0)^k)^t > 1/2$ if and only if $k > \frac{\log_2(1-2^{-1/t})}{\log_2(1-p_0)}$.

For $0 < x < 1$, we have $0 < x/2 < -\log(1-x)$, and for any $t \geq 1$, we have $-\log(1-2^{-1/t}) < 1 + \log(t)$, so

$$\frac{\log_2(1-2^{-1/t})}{\log_2(1-p_0)} = \frac{\log(1-2^{-1/t})}{\log(1-p_0)} < \frac{-2\log(1-2^{-1/t})}{p_0} \leq \frac{2+2\log(t)}{p_0}.$$

In particular, choosing $k > \frac{2+2\log(t)}{p_0} = \mathrm{poly}_r(\log(\Gamma_K), d) = \mathrm{poly}_r(\log|\Delta_K|)$, we obtain a probability of success of at least $1/2$. □

8 Sampling

8.1 Road map

In the following two sections we tackle two challenges. The first one regards *how* to sample an element in $\mathrm{GL}_r(K_\mathbb{R})$ with respect to the distribution f_z as in Section 4.1, assuming real arithmetic and uniform samples from $[0,1]$. In other words, how can the distribution f_z be "built" from known distributions. This is the subject of section Section 8.

On actual computers (or Turing machines), though, no real arithmetic and uniform samples are possible, so the natural second challenge then consists of showing that *discretization* does not impact much the final distribution of this paper's algorithm. This is the subject of Section 9. We now elaborate more on the first of these two challenges.

We note that Section 8 is more of an expository section, making clear the building blocks of the initial distribution f_z, whereas Section 9 contains the precise procedure of sampling from a finite discretized version $\mathcal{D}_z$ of f_z; and the proof that these two are close in some precise sense. In both Section 8 and Section 9 we use column notation for matrices and vectors.

Sampling in $\mathrm{GL}_r(K_\mathbb{R})$ according to f_z.

We will crucially rely on the fact that we can decompose

$$\mathrm{SL}_r(K_\mathbb{R}) = \mathrm{SU}_r(K_\mathbb{R}) \cdot \mathrm{diag}^0(K_\mathbb{R}) \cdot \mathrm{SU}_r(K_\mathbb{R})$$

where $\mathrm{diag}^0(K_\mathbb{R})$ are the determinant 1 diagonal matrices with coefficients in $K_\mathbb{R}$, and that the Haar-measure of a function g on $\mathrm{SL}_r(K_\mathbb{R})$ is dictated by the restriction of g on the completions K_ν in $K_\mathbb{R} = \prod_\nu K_\nu$; which is given by the rule [MP21, Proposition 10]

$$c \int_{(k_1,k_2)\in \mathrm{SU}_r(K_\nu)^2} \int_{a\in\Delta^*} \prod_{1\leq i<j\leq r} \sinh(a_i - a_j)^{[K_\nu:\mathbb{R}]} g(k_1 \exp(a) k_2) dk_1 da dk_2$$

where we mean with $\exp(a)$ the $r \times r$ diagonal matrix $\mathrm{diag}(e^{a_1}, \ldots, e^{a_r})$ and where $\Delta^* = \{(a_1, \ldots, a_{r-1}) \in \mathbb{R}^{r-1} \mid a_1 > \ldots > a_{r-1} > -\sum_{i=1}^{r-1} a_i\}$ and $a_r = -\sum_{i=1}^{r-1} a_i$; and where $c \in \mathbb{R}_{>0}$ is a normalization constant only depending on r and $[K_\nu : \mathbb{R}]$.

By Equations (19) and (21) and Definition 2.29, the matrix norm part (ρ) and the determinant part (τ) are independent; and both ρ and τ are invariant under $\mathrm{SU}_r(K_\mathbb{R})$. Hence, we proceed as in Algorithm 4.

Remark 8.1. As explained in Section 4.1, the initial distribution will be defined as a push-forward of a distribution on Y_r (see Equation (4) and Equation (18)) under the projection $\pi_\mathfrak{a}$. The choice of the left quotient $\mathrm{GL}_r(\mathcal{O}_K, \mathfrak{a}) = \mathrm{Aut}(\mathcal{O}_K^{r-1} \oplus \mathfrak{a})$ in the definition of $X_{r,\mathfrak{a}}$ in Equation (3) is arbitrary and done there for conciseness.

In the present section we let this quotient instead depend on the pseudo-basis $(\mathbf{B}, \mathbf{I})$ of the input module lattice M, where $\mathbf{I} = (\mathfrak{a}_1, \ldots, \mathfrak{a}_r)$ and $\mathbf{B} \in \mathrm{GL}_r(K_\mathbb{R})$. In other words, we rather define

$$X_{r,\mathbf{I}} = \mathrm{Aut}(\mathfrak{a}_1 \oplus \ldots \oplus \mathfrak{a}_r) \backslash \mathrm{GL}_r(K_\mathbb{R}) / (\mathrm{U}_r(K_\mathbb{R}) \cdot \mathbb{R}_{>0}),$$

and send (the coset of) $z := \mathbf{B} \in Y_r$ to (the coset of) $z = \mathbf{B}$ in $X_{r,\mathbf{I}}$, which then corresponds to the module lattice M.

Note that the other class group components of $X_r(K)$ as in Equation (2) may be chosen arbitrarily as long as the full class group is covered.

In the present section, we will also see the distribution f_z on Y_r (see Equation (4)) as a distribution on $\mathrm{GL}_r(K_\mathbb{R})$ and vice versa. This will not lead to confusion, since the support of f_z consists of modules that all have the same absolute determinant, and since for any m in the support of f_z, the entirety of $m \cdot U_r(K_\mathbb{R})$ has equal density.

Algorithm 4 Computing a sample from f_z in $\mathrm{GL}_r(K_\mathbb{R})$

Require:

- A pseudo-basis $(\mathbf{B}, \mathbf{I})$ of a rank r module lattice M,
- $\sigma > 0$, a Gaussian parameter,
- $t \in \mathbb{R}_{>0}$ a width parameter for the diagonal.

Ensure: A pseudo-basis of a module lattice R of rank r.

1: Sample $h \in H \simeq \{h' \in \prod_\nu \mathbb{R} \mid \sum_\nu [K_\nu : \mathbb{R}] \cdot h'_\nu = 0\}$ according to a Gaussian distribution with parameter σ (as in Equation (19)), where H is the hyper plane where the logarithmic units live in.

2: Put $M_h = \mathrm{diag}(e^{h/r}, \ldots, e^{h/r}) \in \mathrm{GL}_r(K_\mathbb{R})$. Note that $\log|\det(M_h)| = h$ and thus $\tau(M_h) = \|h\|^2$. We denote $M_h^{(\nu)}$ for the ν-th component of M_h in the decomposition $\mathrm{GL}_r(K_\mathbb{R}) = \prod_\nu \mathrm{GL}_r(K_\nu)$.

3: For each place ν separately, sample $a^{(\nu)} = (a_1, \ldots, a_{r-1}, a_r)$ with $(a_1, \ldots, a_{r-1}) \in \Delta^*$ from the distribution

$$c' \int_{a \in \Delta^*} \prod_{1 \le i < j \le r} \sinh(a_i - a_j)^{[K_\nu : \mathbb{R}]} 1_{[0,t]}(\rho(\exp(a)) da. \tag{30}$$

Also sample $k_1^{(\nu)}, k_2^{(\nu)} \in \mathrm{SU}_r(K_\nu)$ uniformly (which is possible because it is a compact group) and put (for each ν separately) $g^{(\nu)} := k_1^{(\nu)} \exp(a^{(\nu)}) M_h^{(\nu)} k_2^{(\nu)}$, where $\exp(a)$ is the $r \times r$ diagonal matrix $\mathrm{diag}(e^{a_1}, \ldots, e^{a_r})$.

4: Assemble the $g := (g^{(\nu)})_\nu \in \prod_\nu \mathrm{GL}_r(K_\nu)$ component-wise.

5: **return** $(g \cdot \mathbf{B}, \mathbf{I})$;

That Algorithm 4 indeed yields the desired distribution f_z for $z := \mathbf{B}$, is the object of Lemma 8.2. Note that, computationally, there are three distributions for which a sampling procedure is required. One, the Gaussian distribution on $h \in H$, which is already treated in an earlier work [BDP+20] and will therefore only come up in this work in the section about discretization (Section 9.5). Two, the uniform distribution on $\mathrm{SU}_r(K_\nu)$, which can be computed by assembling uniform distributions on spheres in the shape of Householder transformations. This is treated in Section 8.3. Three, the distribution on Δ^* as in Equation (30), which can be seen as a distribution on a polytope Δ_t^*. We will sample from this distribution by a rejection sampling procedure where the proposal distribution is the uniform distribution on some polytope Δ_t^*. This is treated in Section 8.4.

8.2 Sampling according to the density f_z in $\mathrm{SL}_r(K_\mathbb{R})$

Lemma 8.2. *For any input pseudo-basis $(\mathbf{B}, I)$, the pseudo-algorithm described in Algorithm 4 indeed samples $g \leftarrow \mathrm{GL}_r(K_\mathbb{R})$ according to the distribution f_z as in Section 4.1, with $z = \mathbf{B}$.*

Proof. By the definition of f_z in Equation (21), it enough to show that $g \in \mathrm{GL}_r(K_\mathbb{R})$ as in line 4 of Algorithm 4 is distributed with density $I_f^{-1}\tilde{f}$. The definition of $\tilde{f}$ Equation (19) reads

$$\tilde{f}(x) = 1_{[0,t]}(\rho(x)) \exp(-\frac{\pi}{\sigma^2}\tau(x)),$$

where ρ and τ are defined in Definition 2.29. By the very definition of $\tilde{f}$, the determinant-part and the SL_r-part are *independent* (due to the product in the density function) and can hence be sampled independently.

We focus for now on sampling the SL_r-part, i.e., elements $g \in \mathrm{SL}_r(K_\mathbb{R})$ for which $\det(g) = 1 \in K_\mathbb{R}$ (i.e. 1 at each local component). We decompose $g = (g_\nu)_\nu$ via the isomorphism $\mathrm{SL}_r(K_\mathbb{R}) \simeq \prod_\nu \mathrm{SL}_r(K_\nu)$ from which we can directly see that $\deg(g_\nu) = 1 \in K_\nu$ for all ν. Hence, for $g \in \mathrm{SL}_r(K_\mathbb{R})$,

$$\tilde{f}(g) = 1 \iff (\|g_\nu\|_{\mathrm{op}} \leq t \text{ and } \|g_\nu^{-1}\|_{\mathrm{op}} \leq t \text{ for all } \nu)$$

For each g_ν, we have a unique decomposition $g_\nu = u_\nu d_\nu v_\nu$ with $u_\nu, v_\nu \in \mathrm{SU}_r(K_\nu)$ and $d_\nu \in D_r(\mathbb{R})$ of ordered diagonal matrices (i.e., $\mathrm{diag}(d_1, \ldots, d_r)$ with $d_1 > \ldots > d_r$) of determinant 1.

The Haar measure of a function h on $\mathrm{SL}_r(K_\nu)$ is given by [MP21, Proposition 10]

$$c \int_{(k_1,k_2)\in \mathrm{SU}_r(K_\nu)^2} \int_{a\in\Delta^*} \prod_{1\leq i<j\leq r} \sinh(a_i - a_j)^{[K_\nu:\mathbb{R}]} h(k_1 \exp(a) k_2)\, dk_1\, da\, dk_2$$

for some constant c; here $\exp(a)$ is the r-dimensional diagonal matrix $\mathrm{diag}(e^{a_i})$ with $a_r = -\sum_{i=1}^{r-1}$. Substituting $\tilde{f}$ for h, using that $\rho(g_\nu) = \rho(u_\nu d_\nu v_\nu) = \rho(d_\nu)$ and hence $\tilde{f}(k_1 \exp(a) k_2) = 1_{[0,t]}(\max_{i=1}^r |a_i|)$, we can deduce the following.

Sampling, for all ν, $k_\nu^{(1)}, k_\nu^{(2)} \in \mathrm{SU}_r(K_\nu)$ independently and uniformly, and sampling $a_\nu \in \Delta_t^* := \{a_\nu \in \mathbb{R}^{r-1} \mid t > a_1 > \ldots > a_{r-1} > a_r > -t\}$ with $a_r = -\sum_{i=1}^{r-1} a_i$ according to the distribution

$$c' \prod_{1\leq i<j\leq r} \sinh(a_i - a_j)^{[K_\nu:\mathbb{R}]} d$$

yields a $g_\nu := k_\nu^{(1)} \exp(a_\nu) k_\nu^{(2)} \in \mathrm{SL}_r(K_\nu)$ such that the combination $g = (g_\nu)_\nu$ (via $\mathrm{SL}_r(K_\mathbb{R}) \simeq \prod_\nu \mathrm{SL}_r(K_\nu)$) is (Haar) distributed according to $\tilde{f}$ given a unit determinant. Here, c' is defined such that $c' \int_{a\in\Delta_t^*} \prod_{1\leq i<j\leq r} \sinh(a_i - a_j)^{[K_\nu:\mathbb{R}]} da$ integrates to 1.

By sampling $h \leftarrow H$ according to a Gaussian $\mathcal{G}_{\sigma,H}$, defining

$$M_h = \mathrm{diag}(e^{h/r}, \ldots, e^{h/r}) \in \mathrm{GL}_r(K_\mathbb{R})$$

and denoting $M_h^{(\nu)}$ for the ν-th component of M_h in the decomposition $\mathrm{GL}_r(K_\mathbb{R}) = \prod_\nu \mathrm{GL}_r(K_\nu)$, subsequently putting $g_\nu := k_\nu^{(1)} \exp(a_\nu) M_h^{(\nu)} k_\nu^{(2)}$ and combining $g = (t_\nu)_\nu \in \mathrm{GL}_r(K_\mathbb{R})$ we see that g is distributed according to $\tilde{f}$ (with varying determinant). □

Lemma 8.3. *Let $t, \sigma > 0$ be parameters of Algorithm 4, and let $\varepsilon_1 \in (0,1)$ an error parameter. Let $(\mathbf{B}, \mathbf{I})$ be a pseudo-basis of an α-balanced module lattice M. Then, with probability at least $1 - \varepsilon_1$, the output $(g \cdot \mathbf{B}, \mathbf{I})$ of Algorithm 4 is $(e^{2t+2\sigma\cdot\sqrt{2d\log(2d/\varepsilon_1)}} \cdot \alpha)$-balanced.*

Proof. We have that g is of the shape $g = k_1 \cdot \delta \cdot M_h \cdot k_2$ with $k_1, k_2 \in \mathrm{SU}_r(K_\mathbb{R})$ and M_h and δ diagonal matrices (over K) as in Algorithm 4. Hence, by replacing $(\mathbf{B}, \mathbf{I})$ by $(k_2^{-1}\mathbf{B}, \mathbf{I})$ (which does not change the balancedness of $\mathbf{B}$, as k_2 is unitary), we may assume k_2 is the identity. With the same argument, as we only consider the balancedness properties of $(g \cdot \mathbf{B}, \mathbf{I})$, which are the same as those of $(k_1^{-1} \cdot g \cdot \mathbf{B}, \mathbf{I})$, we may assume k_1 is the identity as well.

Let now write $t = \delta \cdot M_h$. Our aim is to relate the successive minima of M and of tM. We can deduce, by taking $\{m_1, \ldots, m_j\}$ the first j successive minima of M, that

$$\lambda_j^K(tM) \leq \max_i \|tm_i\| \leq \|t\| \cdot \|m_j\| \leq \|t\| \cdot \lambda_j^K(M).$$

In a similar fashion, by taking $\{tm'_1, \ldots, tm'_j\}$ the first j successive minima of tM, with $m'_i \in M$,

$$\lambda_j^K(M) \leq \max_i \|t^{-1}tm'_i\| \leq \|t^{-1}\| \cdot \|tm'_j\| \leq \|t^{-1}\|\lambda_j^K(tM).$$

Hence, for all j,

$$\|t^{-1}\|^{-1} \leq \frac{\lambda_j^K(tM)}{\lambda_j^K(M)} \leq \|t\|,$$

and so

$$\frac{\lambda_{j+1}^K(tM)}{\lambda_j^K(tM)} \leq \frac{\|t\|\lambda_{j+1}^K(M)}{\|t^{-1}\|^{-1}\lambda_j^K(M)} \leq \|t\|\|t^{-1}\| \cdot \frac{\lambda_{j+1}^K(M)}{\lambda_j^K(M)}.$$

In other words, if M is α-balanced, tM must be $(\mathrm{cd}(t) \cdot \alpha)$-balanced, where $\mathrm{cd}(t) = \|t\|\|t^{-1}\|$ is the conditioning number of t.

Since $t = \delta \cdot M_h$, we can use the exact same computations as in the proof of Proposition 9.1, except for the fact that h, in the specific continuous distribution of line 1 of Algorithm 4, is bounded by $\sigma \cdot \sqrt{2d\log(2d/\varepsilon_1)}$ with probability ε_1 for any $\varepsilon_1 \in (0,1)$, by Lemma A.8. Therefore, $\mathrm{cd}(t) = \mathrm{cd}(\delta) \cdot \mathrm{cd}(M_h) \leq e^{2t} \cdot e^{2\sigma \cdot \sqrt{2d\log(2d/\varepsilon_1)}}$, except with probability ε_1. This finishes the proof. □

8.3 Uniform sampling over $\mathrm{SU}_r(K_\mathbb{R})$

In the following lemma, we explain how we can sample uniformly in $\mathrm{SU}_r(K_\mathbb{R})$ if we are allowed to use samples from $\mathcal{U}([0,1])$, the uniform distribution over $[0,1]$.

We do this by first decomposing $\mathrm{SU}_r(K_\mathbb{R}) = \prod_\nu \mathrm{SU}_r(K_\nu)$ where K_ν is the completion of K at the place ν, i.e., $K_\nu = \mathbb{R}$ if ν is real and $\mathbb{C}$ otherwise. Hence sampling a uniformly distributed element from $\mathrm{SU}_r(K_\mathbb{R})$ reduces to sampling uniformly distributed elements from $\mathrm{SU}_r(\mathbb{C})$ and $\mathrm{SU}_r(\mathbb{R})$. As uniformly sampling in these two special orthogonal groups can be tackled similarly, we focus on the $\mathbb{R}$-variant: $\mathrm{SU}_r(\mathbb{R})$.

For sampling in $\mathrm{SU}_r(\mathbb{R})$, we note that (roughly speaking, via fibrations) $\mathrm{SU}_r(\mathbb{R}) \simeq \prod_{j=2}^r S^{j-1}(\mathbb{R})$, where S^{r-1} is the unit sphere in $\mathbb{R}^r$. Indeed, by applying a linear transformation T that sends the first column (an element of $S^{r-1}(\mathbb{R})$) of a $U \in \mathrm{SU}_r(\mathbb{R})$ to the unit vector $\mathbf{e}_1$, we immediately deduce that the bottom-right block of TU lies in $\mathrm{SU}_{r-1}(\mathbb{R})$. The decomposition of $\mathrm{SU}_r(\mathbb{R})$ then follows by induction. So, we can conclude that uniform sampling in $\mathrm{SU}_r(\mathbb{R})$ reduces to uniform samples in spheres.

To uniformly sample in $S^r(\mathbb{R})$, we apply inverse transform sampling by writing the coordinates of $S^r(\mathbb{R})$ in angular coordinates $(\theta_1, \ldots, \theta_r)$. By an adequate sampling of these $(\theta_1, \ldots, \theta_r)$ one then obtains a uniform distribution on $S^r(\mathbb{R})$.

Lemma 8.4. *Let $r \geq 1$. Then there is a procedure that allows to compute a uniform sample in $S^r(\mathbb{R})$ given r uniform samples $(u_1, \ldots, u_r)$ from $\mathcal{U}([0,1])$.*

Proof. We start by defining a map, which described the sphere in spherical coordinates [Blu60],

$$[0, 2\pi] \times [0, \pi]^{r-1} \mapsto S^r(\mathbb{R}),\ (\theta_1, \ldots, \theta_r) \mapsto x := f(\theta_1, \ldots, \theta_r)$$

by the rule

$$x_j = f_j(\theta) := \left(\prod_{k=j}^r \sin(\theta_j)\right) \cos(\theta_{j-1})$$

where we put $\theta_0 := 0$. We seek a distribution $\mathcal{D}$ on $[0, 2\pi] \times [0, \pi]^{r-1}$ such that $f(\theta)$ is uniformly distributed on $S^r(\mathbb{R})$ for $\theta \leftarrow \mathcal{D}$. We put

$$\rho_j(\theta) := \begin{cases} \frac{1}{\sqrt{\pi}} \frac{\Gamma(\frac{j+1}{2})}{\Gamma(\frac{j}{2})} \sin^{j-1}(\theta) & \text{if } j > 1 \\ \frac{1}{2\pi} & \text{if } j = 1 \end{cases}.$$

And define the distribution $\rho(\theta) := \prod_{j=1}^{r} \rho_j(\theta_j)$. This is indeed a distribution, since by the reduction formulae for definite integrals over powers of sines, we have[7], for $j > 1$,

$$\int_0^\pi \sin^{j-1}(\theta) d\theta = \begin{cases} \frac{2(j-2)!!}{(j-1)!!} & \text{if } j \text{ is even} \\ \frac{(j-2)!!}{(j-1)!!} \cdot \pi & \text{if } j \text{ is odd} \end{cases}$$

By the fact that $\Gamma(k+1/2) = \frac{(2k-1)!!}{2^k}\sqrt{\pi}$ and $\Gamma(k) = (k-1)!$, we see that,

$$\frac{\Gamma(\frac{j+1}{2})}{\Gamma(\frac{j}{2})} = \begin{cases} \frac{(2k-1)!!\sqrt{\pi}}{2^k \cdot (k-1)!} = \frac{(2k-1)!!\sqrt{\pi}}{2\cdot(2k-2)!!} = \frac{(j-1)!!\sqrt{\pi}}{(j-2)!!\cdot 2} & \text{for } j = 2k \text{ is even} \\ \frac{(k-1)!2^{k-1}}{\sqrt{\pi}(2k-3)!!} = \frac{(2k-2)!!}{(2k-3)!!\sqrt{\pi}} = \frac{(j-1)!!}{(j-2)!!\sqrt{\pi}} & \text{for } j = 2k-1 \text{ is odd.} \end{cases}$$

Hence, indeed, $\rho_j(\theta)$ is a distribution, and so is $\rho(\theta)$.

Under the function $f : [0, 2\pi] \times [0, \pi]^{r-2}$ this distribution changes into a distribution τ over $S^r(\mathbb{R})$. Our aim is to prove that this latter distribution τ is uniform.

For $A \subseteq S^r(\mathbb{R})$, we have, by the substitution formula for integrals and the inverse function theorem,

$$\int_{\theta \in f^{-1}(A)} \rho(\theta) d\theta = \int_{a \in A} \rho(f^{-1}(a)) |D(f^{-1})(a)| da \tag{31}$$

$$= \int_{a \in A} \rho(f^{-1}(a)) |D(f)(f^{-1}(a))|^{-1} da \tag{32}$$

hence $\tau(a) = \rho(f^{-1}(a))|D(f)(f^{-1}(a))|^{-1}$ is the density function on $a \in S^r(\mathbb{R})$. It is a fact [Blu60, p. 66] that the Jacobian of the spherical coordinates defined by f is equal to

$$D(f)(\theta) := \prod_{j=1}^{r} \sin^{j-1}(\theta_j),$$

and hence, for all $a \in S^r(\mathbb{R})$, we have $\rho(f^{-1}(a)) = c|D(f)(f^{-1}(a))|$ for some constant $c \in \mathbb{R}_{>0}$. This means that $\tau(a) = \rho(f^{-1}(a))|D(f)(f^{-1}(a))|^{-1}$ is constant, and hence is equal to the uniform distribution.

One now obtains a uniform sample $a \in S^r(\mathbb{R})$ by the following procedure:

1. Sample $(u_1, \ldots, u_r) \in [0, 1]^r$ uniformly.
2. Compute $F_j(x) = \int_0^x \rho_j(\theta) d\theta$ either symbolically or numerically.
3. Compute $\theta_j = F_j^{-1}(u_j)$ for all j. Note that, by the inverse transform sampling principle, θ_j is now distributed with density function ρ_j.
4. Compute $x := f(\theta_1, \ldots, \theta_r) \in S^r(\mathbb{R})$.
5. Then $x \in S^r(\mathbb{R})$ is uniformly distributed.

□

Lemma 8.5 (Uniform sampling in SU_r)**.** *There is a procedure that transforms the $(r-1)$-tuple of uniform samples $(u_2, \ldots, u_r) \in \prod_{j=2}^{r} S^{j-1}(\mathbb{R})$ into a uniform sample from $\mathrm{SU}_r(\mathbb{R})$.*

Likewise, there is a procedure that transforms that r-tuple of uniform samples $(u_1, \ldots, u_r) \in \prod_{j=1}^{r} S^{2j-1}(\mathbb{R})$ into a uniform sample from $\mathrm{SU}_r(\mathbb{C})$

[7] Here, !! denotes the double factorial, which equals $n!! := \prod_{j=0}^{\lfloor n/2 \rfloor}(n-2j)$.

Proof. We start with the proof of the first statement, which we prove by induction (where we use $\mathrm{SU}_1(\mathbb{R}) = \{1\}$). So, we assume we have a sample of $\mathrm{SU}_{r-1}(\mathbb{R})$, using uniform samples $(u_2, \ldots, u_{r-1}) \in \prod_{j=2}^{r-1} S^{j-1}(\mathbb{R})$.

Since the (oriented) sphere $S^{r-1}(\mathbb{R})$ is a homogeneous space for $\mathrm{SU}_r(\mathbb{R})$, and we have the following fiber bundle [Ste99, p. I.7.6]

$$SU_{r-1}(\mathbb{R}) \to \mathrm{SU}_r(\mathbb{R}) \to S^{r-1}(\mathbb{R}),$$

we can assemble a uniform sample in $\mathrm{SU}_r(\mathbb{R})$ by combining a uniform sample in $S^{r-1}(\mathbb{R})$ and $\mathrm{SU}_{r-1}(\mathbb{R})$ as follows.

We construct such $A \in \mathrm{SU}_r(\mathbb{R})$ by the following procedure. First, sample $a \in S^{r-1}(\mathbb{R})$ uniformly. This $a \in \mathbb{R}^r$ satisfies $\|a\| = 1$. Create a Householder transformation $H_a = I - 2vv^\top \in U_r(\mathbb{R})$ that sends a to e_n; that is, put $v = \frac{a-e_n}{\|a-e_n\|}$.

Sample $B \in SU_{r-1}(\mathbb{R})$ uniformly and put

$$A' := \begin{bmatrix} B & 0 \\ 0 & -1 \end{bmatrix}.$$

That is, the last row and the last column of A' consists of zeroes, except for $A'_{11} = -1$. Then, output $A := H_a A'$.

By construction, $\det(A) = \det(H_a)\det(A') = -\det(H_a)\det(B) = 1$ since Householder transformations have determinant -1. Hence $A \in \mathrm{SU}_r(\mathbb{R})$.

For the second statement, about $\mathrm{SU}_r(\mathbb{C})$, can be proven similarly, but instead with the spheres S^{2j-1}, via the fiber bundle (for $r \geq 2$) [Ste99, p. I.7.10]

$$SU_{r-1}(\mathbb{C}) \to SU_r(\mathbb{C}) \to S^{2r-1}(\mathbb{R}).$$

Note that $\mathrm{SU}_1(\mathbb{C}) \simeq S^1(\mathbb{R})$. The uniform sample from $\mathrm{SU}_r(\mathbb{C})$ is then constructed by sampling $a \in S^{2r-1}(\mathbb{R})$ uniformly, and seeing it as a vector in $\mathbb{C}^r$ of norm 1. Subsequently, compute the Householder transformation $H_a = I - 2vv^*$ with $v = \frac{a-e_1}{\|a-e_n\|}$ (note the difference between v^* and $v^\top$ between the complex and the real case). We sample $B \in SU_{r-1}(\mathbb{C})$ uniformly and put

$$A' := \begin{bmatrix} B & 0 \\ 0 & -1 \end{bmatrix},$$

and define $A := H_a A'$. By similar computations, we deduce that A is a uniform sample in $\mathrm{SU}_r(\mathbb{C})$. □

Definition 8.6. For $\theta \in \prod_{j=2}^{r} S^{j-1}(\mathbb{R})$ we denote by $U_\theta \in \mathrm{SU}_r(\mathbb{R})$ the real unitary matrix associated with θ defined by the procedure in Lemma 8.5. Abusing notation, for $\theta \in \prod_{j=1}^{r} S^{2j-1}(\mathbb{R})$ we also denote by $U_\theta \in \mathrm{SU}_r(\mathbb{C})$ the complex unitary matrix associated with θ defined by the procedure in Lemma 8.5.

8.4 Sampling from $1_{[0,t]}(\rho(\exp(a)))$ over the diagonal

8.4.1 The target distribution

The goal in the following text is to derive a procedure to sample determinant one diagonal matrices over K_ν with operator norm (from ρ) bounded by some number $t \in \mathbb{R}_{>0}$, according to the marginal distribution inherited from the Haar measure on $\mathrm{SL}_r(K_\nu)$, as in Equation (30).

This precisely coincides with sampling $(a_1, \ldots, a_r) \in \mathbb{R}$ with $a_1 > \ldots > a_{r-1} > a_r$ and $a_r = -\sum_{i=1}^{r-1} a_i$, satisfying $\max_j |a_j| < t$, according to the Haar measure on the diagonal in

$\mathrm{SL}_r(\mathbb{K})$ with $\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$. This distribution can be shown ([MP21, Proposition 10] where we locally instantiate $d := r$ and $e := 1$, see [MP21, Section 4]) to have density

$$g(a_1, \ldots, a_{r-1}) = \begin{cases} c \cdot \prod_{1 \le i < j \le r} \sinh(a_i - a_j)^{[\mathbb{K}:\mathbb{R}]} & \text{for } |a_i| < t \\ 0 & \text{elsewhere} \end{cases} \tag{33}$$

where $c \in \mathbb{R}_{>0}$ is a constant such that g is indeed a density (with unit integral). We will write $\bar{g} = c^{-1} g = \prod_{1 \le i < j \le r} \sinh(a_i - a_j)^{[\mathbb{K}:\mathbb{R}]}$ (restricted to $|a_i| < t$) for the unnormalized function.

8.4.2 Rejection sampling

In rejection sampling (e.g., [Dev86, Section II.3]), there are two distributions: a target distribution, from which we actually would like a sample, and a proposal distribution, for which we are already able to find samples. By adequately, with a certain probability depending on the sampled value, reject samples from the proposal distribution, we arrive at a sample procedure for the target distribution.

In the case at hand, the target distribution has density function g as in Equation (33), whereas we choose as the proposal distribution the *uniform distribution* on the simplex defined by $(a_1, \ldots, a_r)$. Such a rejection sampling procedure then reads as follows.

1. Compute an upper bound $M \ge \max_{|a_i| < t} \bar{g}(a_1, \ldots, a_{r-1})$ on $\bar{g} = c^{-1} g$.
2. Sample $a = (a_1, \ldots, a_{r-1}) \in \Delta_t^*$ uniformly from the set

$$\Delta_t^* = \{(a_1, \ldots, a_{r-1}) \in \mathbb{R} \mid t > a_1 > \ldots > a_{r-1} > a_r := -\sum_{i=1}^{r-1} a_i > -t\}.$$

   and reject with probability $1 - \frac{\bar{g}(a_1, \ldots, a_{r-1})}{M}$.
3. If a is rejected, re-sample (go to line 2); if not, output a.

In line 2 the algorithm is expected to reject a with probability $\frac{1}{\mathrm{vol}(\Delta_t^*)} \int_{a \in \Delta_t^*} \left(1 - \frac{c^{-1} g(a)}{M}\right) da = 1 - \frac{1}{cM}$ and hence accepts a with probability $(cM)^{-1}$. So one can deduce that the expected number of uniform samples from Δ_t^* this algorithm needs, provided that $t \le 1$, is

$$O(cM) = O(\max_a g(a)) = O\left((16r^2)^{\frac{r(r-1)[\mathbb{K}:\mathbb{R}]}{2}} \cdot \left(\frac{4r^2}{t}\right)^{r-1}\right) = e^{O(r^2 \log r)} \cdot t^{-(r-1)},$$

by the later Lemma 8.7 in Section 8.4.4.

8.4.3 Uniform sampling on the polytope Δ_t^*

Our aim is to uniformly sample in the polytope

$$\Delta_t^* = \{(a_1, \ldots, a_{r-1}) \in \mathbb{R} \mid t > a_1 > \ldots > a_{r-1} > a_r := -\sum_{i=1}^{r-1} a_i > -t\}.$$

We apply the change of variables $y_i = \frac{t - a_i}{2t}$ for $i \in \{1, \ldots, r-1\}$ that bijectively and linearly transforms Δ_t^* in the set

$$S = \{(y_1, \ldots, y_{r-1}) \in \mathbb{R} \mid 0 < y_1 < \ldots < y_{r-1} \le 1, \sum_{i=1}^{r-1} y_i > \frac{r-2}{2} \text{ and } y_{r-1} + \sum_{i=1}^{r-1} y_i < \frac{r}{2}\}. \tag{34}$$

Indeed, $\sum_{i=1}^{r-1} y_i = \sum_{i=1}^{r-1} \frac{t-a_i}{2t} = \frac{r-1}{2} - \frac{1}{2t}\sum_{i=1}^{r} a_i > \frac{r-1}{2} - \frac{t}{2t} = \frac{r-2}{2}$ and

$$y_{r-1} + \sum_{i=1}^{r-1} y_i = \frac{t-a_{r-1}}{2t} + \sum_{i=1}^{r-1} \frac{t-a_i}{2t} = \frac{r}{2} - \frac{1}{2t}\underbrace{\left(a_{r-1} + \sum_{i=1}^{r-1} a_i\right)}_{>0} < \frac{r}{2}.$$

This set S satisfies $S \subseteq \Delta^0 = \{(y_1, \ldots, y_{r-1}) \in \mathbb{R} \mid 0 < y_1 < \ldots < y_{r-1} \leq 1\}$, a filled simplex. A procedure for sampling in Δ^0 exists [Dev86, §I.4.3, p. 17] by sampling $r-1$ uniform distributions $U_1, \ldots, U_{r-1}$ and sorting them $U_{(1)} \leq U_{(2)} \leq \ldots \leq U_{(r-1)}$.

We now sample y from Δ^0 in this way, and reject if $y \notin S$. We aim to compute a lower bound on the success probability of this rejection sampling procedure. Surely, if $y_1 > \frac{(r-2)}{2(r-1)}$ we have $\sum_{i=1}^{r-1} y_i > \frac{(r-2)}{2}$. Also, if $y_{r-1} < 1/2$, we must have $y_{r-1} + \sum_{i=1}^{r-1} y_i < \frac{r}{2}$. Hence,

$$\begin{aligned}
\frac{\mathrm{vol}(S)}{\mathrm{vol}(\Delta^0)} &\geq \mathop{\mathbb{P}}_{y \leftarrow \mathcal{U}(\Delta^0)}\left[y_1 > \frac{(r-2)}{2(r-1)} \text{ and } y_{r-1} < 1/2\right] \\
&= \mathbb{P}\left[\min_{i=1,\ldots,r-1} U_i > \frac{(r-2)}{2(r-1)} \text{ and } \max_{i=1,\ldots,r-1} U_i < 1/2\right] \\
&= \mathbb{P}\left[\max_{i=1,\ldots,r-1} U_i < 1/2 \;\middle|\; \min_{i=1,\ldots,r-1} U_i > \frac{(r-2)}{2(r-1)}\right] \cdot \mathbb{P}\left[\min_{i=1,\ldots,r-1} U_i > \frac{(r-2)}{2(r-1)}\right]
\end{aligned}$$

where U_i are iid uniform distributions over $[0,1]$. We have

$$\mathbb{P}\left[\min_{i=1,\ldots,r-1} U_i > \frac{(r-2)}{2(r-1)}\right] = \left(1 - \frac{(r-2)}{2(r-1)}\right)^{r-1} = \left(\frac{1}{2} + \frac{1}{2(r-1)}\right)^{r-1}$$

whereas we can compute the conditional probability by defining U_i' being uniform in $[\frac{(r-2)}{2(r-1)}, 1]$:

$$\mathbb{P}\left[\max_{i=1,\ldots,r-1} U_i < 1/2 \;\middle|\; \min_{i=1,\ldots,r-1} U_i > \frac{(r-2)}{2(r-1)}\right] = \mathbb{P}[\max_{i=1,\ldots,r-1} U_i' < 1/2] = \left(\frac{\frac{1}{2} - \frac{(r-2)}{2(r-1)}}{1 - \frac{(r-2)}{2(r-1)}}\right)^{r-1}$$

$$= \left(\frac{\frac{1}{2(r-1)}}{\frac{1}{2} + \frac{1}{2(r-1)}}\right)^{r-1}$$

Hence,

$$\frac{\mathrm{vol}(S)}{\mathrm{vol}(\Delta^0)} \geq (2(r-1))^{-(r-1)}. \tag{35}$$

So, the expected number of uniform samples from $[0,1]$ required to compute a uniform sample in Δ_t^* via this rejection procedure, is

$$O((2(r-1))^{(r-1)}) = e^{O(r \log r)}.$$

8.4.4 Bound on the maximum of g

Lemma 8.7. *For $t \leq 1$, we have*

$$\|\bar{g}\|_\infty \leq (4t)^{r(r-1)}, \qquad \|g\|_\infty \leq (16r^2)^{\frac{r(r-1)[\mathbb{K}:\mathbb{R}]}{2}} \cdot \left(\frac{4r^2}{t}\right)^{r-1}$$

and

$$Lip(g) \leq \frac{r^2}{t} \cdot (16r^2)^{\frac{r(r-1)[\mathbb{K}:\mathbb{R}]}{2}} \cdot \left(\frac{4r^2}{t}\right)^{r-1}$$

Proof. For the first bound we compute, using $|a_i - a_j| \leq 2t < 2$.

$$\bar{g} = \prod_{i<j} \sinh(a_i - a_j)^{[\mathbb{K}:\mathbb{R}]} \leq 2^{r(r-1)/2} \cdot \prod_{i<j} (a_i - a_j)^{[\mathbb{K}:\mathbb{R}]} \leq (4t)^{r(r-1)[\mathbb{K}:\mathbb{R}]/2} \leq (4t)^{r(r-1)}$$

For the second bound we use the lower bound on the integral I in Lemma 2.31. Hence, we can bound g by (since $|a_i - a_j| < 2t < 2$)

$$\begin{aligned} g &= I^{-1} \prod_{i<j} \sinh(a_i - a_j)^{[\mathbb{K}:\mathbb{R}]} \leq I^{-1} \cdot (4t)^{r(r-1)[\mathbb{K}:\mathbb{R}]/2} \\ &\leq (16r^2)^{\frac{r(r-1)[\mathbb{K}:\mathbb{R}]}{2}} \cdot \left(\frac{4r^2}{t}\right)^{r-1}. \end{aligned}$$

For the bound on the Lipschitz constant, we bound the derivative of g on Δ_t^*.

$$\frac{\partial g}{\partial a_k} = I^{-1} \frac{\partial}{\partial a_k} \prod_{1 \leq i < j \leq r} \sinh(a_i - a_j)^{[\mathbb{K}:\mathbb{R}]}$$

$$= I^{-1} \prod_{\substack{1 \leq i < j \leq r \\ k \neq i, k \neq j}} \sinh(a_i - a_j)^{[\mathbb{K}:\mathbb{R}]} \frac{\partial}{\partial a_k} \prod_{\substack{1 \leq i < j \leq r \\ i = k \text{ or } j = k}} \sinh(a_i - a_j)^{[\mathbb{K}:\mathbb{R}]}$$

We proceed with the right-hand side of above expression, which equals

$$= \frac{\partial}{\partial a_k} \prod_{i=1}^{k-1} \sinh(a_i - a_k)^{[\mathbb{K}:\mathbb{R}]} \prod_{j=k+1}^{r} \sinh(a_k - a_j)^{[\mathbb{K}:\mathbb{R}]}$$

$$= \left(-\sum_{i=1}^{k-1} [\mathbb{K} : \mathbb{R}] \frac{\cosh(a_i - a_k)}{\sinh(a_i - a_k)} + \sum_{j=k+1}^{r} [\mathbb{K} : \mathbb{R}] \frac{\cosh(a_i - a_k)}{\sinh(a_i - a_k)} \right) \prod_{i=1}^{k-1} \sinh(a_i - a_k)^{[\mathbb{K}:\mathbb{R}]} \prod_{j=k+1}^{r} \sinh(a_k - a_j)^{[\mathbb{K}:\mathbb{R}]}$$

Hence

$$\frac{\partial g}{\partial a_k} = \left(-\sum_{i=1}^{k-1} [\mathbb{K} : \mathbb{R}] \frac{\cosh(a_i - a_k)}{\sinh(a_i - a_k)} + \sum_{j=k+1}^{r} [\mathbb{K} : \mathbb{R}] \frac{\cosh(a_i - a_k)}{\sinh(a_i - a_k)} \right) g$$

Since $a_i - a_j < 2t < 2$, we see that $\sinh(a_i - a_j) \leq 4t$ and $\cosh(a_i - a_j) < 2$, for all $i < j$. Hence, we can bound

$$\begin{aligned} \| \frac{\partial g}{\partial a_k} \|_\infty &\leq 2I^{-1}(r-1)[\mathbb{K} : \mathbb{R}](4t)^{[\mathbb{K}:\mathbb{R}]\frac{(r-1)r}{2} - 1} \leq 4r \cdot \frac{1}{4t} \cdot I^{-1} \cdot (4t)^{[\mathbb{K}:\mathbb{R}]\frac{(r-1)r}{2}} \\ &\leq \frac{r}{t} \cdot (16r^2)^{\frac{r(r-1)[\mathbb{K}:\mathbb{R}]}{2}} \cdot \left(\frac{4r^2}{t}\right)^{r-1} \end{aligned}$$

Now, $\mathrm{Lip}(g) \leq r \max_k \| \frac{\partial g}{\partial a_k} \|_\infty \leq \frac{r^2}{t} \cdot (16r^2)^{\frac{r(r-1)[\mathbb{K}:\mathbb{R}]}{2}} \cdot \left(\frac{4r^2}{t}\right)^{r-1}$, which is what we wanted to prove. □

9 Discretization

9.1 Introduction

In Section 8 we described how to sample from the continuous distributions that occur in the random walk procedure of the current work. On an actual computer (or Turing machine), none of these continuous distributions can be computed. Instead, we will compute discretized versions of these, which, in the end, will lead to a distribution $\mathcal{D}$ on a finite subset $S \subseteq \mathrm{GL}_r(K_\mathbb{R})$ instead of the distribution $\tilde{f}$.

The discreteness of the distribution $\mathcal{D}$ on S and the continuity of the distribution $\tilde{f}$ on $\mathrm{GL}_r(K_{\mathbb{R}})$ cause them to be incomparable at first glance. However, the full random walk procedure of this paper comes with a randomization framework and at the end the rounding algorithm (see Section 3). The output of the rounding algorithm (and thus of the entire random walk procedure) is a *distribution* in $L^1(X)$ over some discrete set of module lattices X.

For $g \in \mathrm{GL}_r(K_{\mathbb{R}})$ (where g is sampled, for example, from $\mathcal{D}$ or from $\tilde{f}$), we can write the output of the entire random walk procedure of this paper on input g as $\psi(g) \in L^1(X)$.

In order to show that the output distribution of the entire random walk procedure on input $g \leftarrow \tilde{f}$ differs not much from if we instead had taken the input $g \leftarrow \mathcal{D}$ (on the finite set S), it is sufficient to show that

$$\mathop{\mathbb{E}}_{g \xleftarrow{\tilde{f}} \mathrm{GL}_r(K_{\mathbb{R}})}[\psi_g] = \int_g \psi_g \tilde{f}(g) dg \approx \sum_{g \in S} \psi_g \mathcal{D}(g) = \mathop{\mathbb{E}}_{g \xleftarrow{\mathcal{D}} S}[\psi_g]$$

where both on the right side and the left side is a distribution over X, i.e., a function in $L^1(X)$, which is "averaged" over all possible g. Here the "$\approx$" sign means that we want the two distributions to be close in statistical distance.

We will show that indeed these average end distributions are close in statistical distance. We show this by changing the continuous distributions into discretized analogues one by one. So, writing $\mathcal{D}_0 = \tilde{f}$, and $\mathcal{D}_1$ for the distribution in which in $\tilde{f}$ the left-multiplied uniform distribution on $\mathrm{SU}_r(K_\nu)$ (for all ν) is discretized, $\mathcal{D}_2$ for which additionally the $a \in \Delta^*$ are discretized, $\mathcal{D}_3$ for which additionally $h \in H$ is discretized, and $\mathcal{D}_4 = \mathcal{D}$ for which additionally the right-multiplied uniform distribution on $\mathrm{SU}_r(K_\nu)$ are discretized; this latter is equal to $\mathcal{D}$ because then all is discretized. We will show that

$$\mathop{\mathbb{E}}_{g \xleftarrow{\tilde{f}} \mathrm{GL}_r(K_{\mathbb{R}})}[\psi_g] \approx \mathop{\mathbb{E}}_{g \leftarrow \mathcal{D}_1}[\psi_g] \approx \mathop{\mathbb{E}}_{g \leftarrow \mathcal{D}_2}[\psi_g] \approx \mathop{\mathbb{E}}_{g \leftarrow \mathcal{D}_3}[\psi_g] \approx \mathop{\mathbb{E}}_{g \leftarrow \mathcal{D}_4}[\psi_g].$$

For each of the continuous distributions we will show how to discretize them appropriately and how it impacts this final distribution. The discretization of the uniform distribution on the "left-multiplied" $\mathrm{SU}_r(K_\nu)$ is treated in Section 9.7, the discretization of $a \in \Delta^*$ in Section 9.6, the discretization of $h \in H$ in Section 9.5 and, as it is very similar, the discretization of the "right-multiplied" $\mathrm{SU}_r(K_\nu)$ also in Section 9.7.

9.2 Result

The self-reduction of this paper on an input module lattice consists of two ingredients. The first one is a random walk procedure that both changes the input module lattice slightly geometrically and takes random prime power index sub-module lattices of it. The second ingredient is a rounding procedure, called $\mathrm{Round}_{\mathrm{Lat}}$, that allows for efficiently computing a rational module lattice close to the input module lattice, with the virtue that the specific input pseudo-basis representation is hidden: only its module-lattice structure is known.

The random walk procedure on the space of module lattices involves random processes that can be divided into a *discrete* random process and a *continuous* random process. The discrete random process consists of choosing a random prime ideal and taking a random sub-module with quotient group isomorphic to the corresponding residue field, whereas the continuous one involve sampling from the continuous distribution f_z for $z \in Y_r$.

Recall that random process of taking submodules as above corresponds to the Hecke operator $T_{\mathcal{P}}$, defined in (12). Although $T_{\mathcal{P}}$ is defined on the space of lattices X_r, we also use $T_{\mathcal{P}}$ to denote the same process at the level of pseudo-bases, as in Algorithm 1, by choosing coset representatives to average over. This should not lead to confusion, as it commutes with the push-forward through the projection $Y_r \to X_{r,\mathfrak{a}}$. Recall also the rounding algorithm $\mathrm{Round}_{\mathrm{Lat}}$, defined in Algorithm 2, taking in parameters ε_0 and a balancedness parameter α.

Let $z = (\mathbf{B}, \mathbf{I})$ be the input corresponding to a module lattice L. We define f_z and φ_z by slight abuse of notation, as in Remark 8.1, and in all that follows we interpret f_z and φ_z as distributions by meaning literally $f_z\mu_{\mathrm{Riem}}$ and $\varphi_z\mu_{\mathrm{Riem}}$, respectively.

The output distribution of the random walk procedure on input z is given by $T_{\mathcal{P}}f_z$, which a priori depends on the choice of pseudo-basis. If we additionally also apply the rounding algorithm, we get the output distribution $\mathrm{Round}_{\mathrm{Lat}}(T_{\mathcal{P}}f_z)$. Since the the output of $\mathrm{Round}_{\mathrm{Lat}}$ is independent of pseudo-bases with high probability (see Proposition 3.1), we can identify this distribution with $\mathrm{Round}_{\mathrm{Lat}}(T_{\mathcal{P}}\varphi_z)$.

Similarly, for any other distribution $\mathcal{D}_z$ on Y_r, we denote by $\mathrm{Round}_{\mathrm{Lat}}(T_{\mathcal{P}}\mathcal{D}_z)$ for the distribution that results if we took a sample from $\mathcal{D}_z$ instead of f_z and then subsequently applied taking random sub-module and the rounding representation algorithm.

The goal of this section is to show that for all reasonably balanced module lattices z, there exists an efficiently computable *finite* distribution $\mathcal{D}_z$ such that $\mathrm{Round}_{\mathrm{Lat}}(T_{\mathcal{P}}\mathcal{D}_z)$ is statistically close to $\mathrm{Round}_{\mathrm{Lat}}(T_{\mathcal{P}}\varphi_z)$. This means that sampling from the continuous distribution f_z (which is impossible on an actual computer) is not required per se for our reduction to work: indeed, the efficiently computable finite surrogate distribution $\mathcal{D}_z$ will do, too, and causes only a tiny deviation of the end distribution.

Proposition 9.1. *Let $\alpha > 1$, $0 < \varepsilon < 1$, $B \gg 1$, and let $(\mathbf{B}, \mathbf{I})$ be a pseudo-basis for a module lattice z be that is α-balanced. Denote by $\mathcal{P}$ the set of all prime ideals of norm up to B. Then there exists a finite distribution $\mathcal{D}_z$ such that*

$$\|\mathrm{Round}_{\mathrm{Lat}}(T_{\mathcal{P}}\mathcal{D}_z) - \mathrm{Round}_{\mathrm{Lat}}(T_{\mathcal{P}}\varphi_z)\|_1 \leq \varepsilon + \varepsilon_0$$

that is sampleable in time $\exp(8r^2\log(r))\cdot\mathrm{poly}(n, \log(1/\varepsilon), \log(1/\varepsilon_0), \log B, \mathrm{size}(\mathbf{B}))$, where $\varepsilon_0 > 0$ is an input parameter to $\mathrm{Round}_{\mathrm{Lat}}$, Algorithm 2, and $\varphi_z, \mathcal{D}_z$ are defined through parameters $t \leq 1$ and $\sigma \leq 1$.

Proof. **Definition of $\mathcal{D}_z$.** We define $\mathcal{D}_z$ to be the distribution from Algorithm 4, where each continuous distribution is replaced by a finite substitute. So, the Gaussian distribution in line 1 is replaced by a discrete and windowed Gaussian distribution as in Definition 2.19; the uniform distributions over $\mathrm{SU}_r(K_\nu)$ in line 3 are replaced by a finite counterpart defined in Definition 9.22 (for each place ν); and the "diagonal distribution" in line 3 is replaced by a finite distribution as in Definition 9.11.

Efficiency of $\mathcal{D}_z$. The efficiency of $\mathcal{D}_z$ follows from the efficiency of all distributions involved, for which the efficiency is shown in the discussion in Section 9.5.1, Lemmas 9.17 and 9.28. Note that that the running time is polynomial time in $r, d, \log N$, except for the diagonal distribution, for which it is $O(d\exp(8r^2\log(r))\log N)$.

Closeness of distributions. By the description in Algorithm 4 we know that a sample from the distribution f_z can be described as $z\cdot k_1\cdot M_h\cdot a\cdot k_2$ where $k_1, k_2 \leftarrow \mathcal{U}(\mathrm{SU}_r(K_{\mathbb{R}}))$, where $M_h = \mathrm{diag}(e^{h/r}, \ldots, e^{h/r})$ with h sampled from a Gaussian over H with parameter σ, and where a is some diagonal matrix in $\mathrm{GL}_r(K_{\mathbb{R}})$ sampled from a specific diagonal distribution.

Similarly, a sample from the *discretized* distribution $\mathcal{D}_z$ can be described by $z\cdot\ddot{k}_1\cdot M_{\ddot{h}}\cdot\ddot{a}\cdot\ddot{k}_2$, where $\ddot{k}_1, \ddot{k}_2$ are from the distribution described in Definition 9.22, $\ddot{h}$ is sampled from a discrete Gaussian over H (Definition 2.19) and where $\ddot{a}$ is from a discrete analogue of the specific diagonal distribution.

The distributions $\mathrm{Round}_{\mathrm{Lat}}(T_{\mathcal{P}}(\mathcal{D}_z))$ and $\mathrm{Round}_{\mathrm{Lat}}(T_{\mathcal{P}}(f_z))$ can be alternatively described by respectively

$$\mathop{\mathbb{E}}_{\ddot{k}_1,\ddot{h},\ddot{a},\ddot{k}_2}[\mathrm{Round}_{\mathrm{Lat}}(T_{\mathcal{P}}(z\cdot\ddot{k}_1\cdot M_{\ddot{h}}\cdot\ddot{a}\cdot\ddot{k}_2))] \text{ and } \mathop{\mathbb{E}}_{k_1,h,a,k_2}[\mathrm{Round}_{\mathrm{Lat}}(T_{\mathcal{P}}(z\cdot k_1\cdot M_h\cdot a\cdot k_2))].$$

By Algorithm 1, and since $T_{\mathcal{P}}$ changes the ideal part of the pseudo-basis only by multiplying one ideal by a random $\mathfrak{p} \in \mathcal{P}$, (see also Remark 8.1) we may, by the law of total probability, instead replace the operation $T_{\mathcal{P}}$ by a multiplication from the left by a matrix T.

Writing $\bar{z} = T \cdot z$, we can measure the closeness of these distributions, we apply the triangle inequality and discretize one-by-one (starting from the right):

$$\|\mathrm{Round}_{\mathrm{Lat}}(T_{\mathcal{P}}(\mathcal{D}_z)) - \mathrm{Round}_{\mathrm{Lat}}(T_{\mathcal{P}}(f_z))\|_1 \tag{36}$$

$$\leq \left\| \mathop{\mathbb{E}}_{\ddot{k}_1,\ddot{h},\ddot{a},\ddot{k}_2} [\mathrm{Round}_{\mathrm{Lat}}(\bar{z} \cdot \ddot{k}_1 \cdot M_{\ddot{h}} \cdot \ddot{a} \cdot \ddot{k}_2)] - \mathop{\mathbb{E}}_{\ddot{k}_1,\ddot{h},\ddot{a},k_2} [\mathrm{Round}_{\mathrm{Lat}}(\bar{z} \cdot \ddot{k}_1 \cdot M_{\ddot{h}} \cdot \ddot{a} \cdot k_2)] \right\|_1 \tag{37}$$

$$+ \left\| \mathop{\mathbb{E}}_{\ddot{k}_1,\ddot{h},\ddot{a},k_2} [\mathrm{Round}_{\mathrm{Lat}}(\bar{z} \cdot \ddot{k}_1 \cdot M_{\ddot{h}} \cdot \ddot{a} \cdot k_2)] - \mathop{\mathbb{E}}_{\ddot{k}_1,\ddot{h},a,k_2} [\mathrm{Round}_{\mathrm{Lat}}(\bar{z} \cdot \ddot{k}_1 \cdot M_{\ddot{h}} \cdot a \cdot k_2)] \right\|_1 \tag{38}$$

$$+ \left\| \mathop{\mathbb{E}}_{\ddot{k}_1,\ddot{h},a,k_2} [\mathrm{Round}_{\mathrm{Lat}}(\bar{z} \cdot \ddot{k}_1 \cdot M_{\ddot{h}} \cdot a \cdot k_2)] - \mathop{\mathbb{E}}_{\ddot{k}_1,h,a,k_2} [\mathrm{Round}_{\mathrm{Lat}}(\bar{z} \cdot \ddot{k}_1 \cdot M_h \cdot a \cdot k_2)] \right\|_1 \tag{39}$$

$$+ \left\| \mathop{\mathbb{E}}_{\ddot{k}_1,h,a,k_2} [\mathrm{Round}_{\mathrm{Lat}}(\bar{z} \cdot \ddot{k}_1 \cdot M_h \cdot a \cdot k_2)] - \mathop{\mathbb{E}}_{k_1,h,a,k_2} [\mathrm{Round}_{\mathrm{Lat}}(\bar{z} \cdot k_1 \cdot M_h \cdot a \cdot k_2)] \right\|_1 \tag{40}$$

We now bound each of the components in above sum. By Lemma 9.29, we can bound Equation (37) by

$$O(N^{-1/4} \cdot \mathrm{cd}(\bar{z} \cdot \ddot{k}_1 \cdot M_{\ddot{h}} \cdot \ddot{a})^{1/2} \cdot n^5 \sqrt[4]{\log(1/\varepsilon_0)}). \tag{41}$$

By Lemma 9.18, we may deduce that Equation (38) is bounded by

$$N^{-1/2} O(d \exp(8r^2 \log(r)) + n^5 \,\mathrm{cd}(\bar{z} \cdot \ddot{k}_1 \cdot M_{\ddot{h}})^{1/2} \cdot \sqrt[4]{\log(1/\varepsilon_0)}) \tag{42}$$

By Lemma 9.7 and the fact that M_h and a are both diagonal matrices (and thus commute), we deduce that Equation (39) is bounded by

$$N^{-1/2} O(n^4 \,\mathrm{cd}(\bar{z} \cdot \ddot{k}_1)^{1/2} \cdot \sqrt[4]{\log(1/\varepsilon_0)} + n\sigma). \tag{43}$$

By Lemma 9.29, we can bound Equation (40) by

$$O(N^{-1/4} \cdot \mathrm{cd}(\bar{z})^{1/2} \cdot n^5 \sqrt[4]{\log(1/\varepsilon_0)}). \tag{44}$$

Combining the bounds of Equations (41) to (44), and simplifying, we obtain

$$\begin{aligned} &\|\mathrm{Round}_{\mathrm{Lat}}(T_{\mathcal{P}}(\mathcal{D}_z)) - \mathrm{Round}_{\mathrm{Lat}}(T_{\mathcal{P}}(f_z))\|_1 \\ &\leq \mathrm{cd}(\bar{z} \cdot \ddot{k}_1 \cdot M_{\ddot{h}} \cdot \ddot{a})^{1/2} \cdot N^{-1/4} \cdot \sqrt[4]{\log(1/\varepsilon_0)} \cdot n^5 \cdot (d \exp(8r^2 \log(r)) + n\sigma) \end{aligned} \tag{45}$$

We will now bound the conditioning number. We have, by submultiplicativity of the conditioning number, and the fact that conditioning numbers of unitary matrices equal one,

$$\mathrm{cd}(\bar{z} \cdot \ddot{k}_1 \cdot M_{\ddot{h}} \cdot \ddot{a}) \leq \mathrm{cd}(\bar{z}) \cdot \mathrm{cd}(\ddot{k}_1) \cdot \mathrm{cd}(M_{\ddot{h}}) \cdot \mathrm{cd}(\ddot{a}) = \mathrm{cd}(\bar{z}) \cdot \mathrm{cd}(M_{\ddot{h}}) \cdot \mathrm{cd}(\ddot{a}) \tag{46}$$

$$\leq \mathrm{cd}(\bar{z}) \cdot e^{2n^2\sigma} \cdot e^{2t} \tag{47}$$

$$\leq 2^{8(rd)^2} \cdot |\Delta_K|^{r+2} \cdot 2^{(2rd+3) \cdot \mathrm{size}(\mathbf{B}) + \mathrm{size}(\mathfrak{p})} \cdot e^{2n^2\sigma} \cdot e^{2t} \tag{48}$$

$$\leq \exp(O(n^2 + n^2\sigma + n \cdot \mathrm{size}(\mathbf{B}) + \mathrm{size}(\mathfrak{p}) + n \log |\Delta_K|)). \tag{49}$$

Indeed, since $\ddot{a}$ is diagonal, where the entries at each ν-component are bounded by $[e^{-t}, e^t]$, so the total conditioning number must be bounded above by e^{2t}. For the bound on the (discrete and windowed) Gaussian distributed $M_{\ddot{h}}$, note that $M_{\ddot{h}} = \mathrm{diag}(e^{\ddot{h}/r}, \ldots, e^{\ddot{h}/r})$ and $\ddot{h}$ is bounded by $n^2\sigma$ in absolute value, and hence $\mathrm{cd}(M_{\ddot{h}}) \leq e^{2n^2\sigma}$.

For the bound on the conditioning number of $\bar{z} = T \cdot z$, we use Lemma 9.2 and Lemma 9.3 to see that (using $t \leq 1$)

$$\mathrm{cd}(\bar{z}) \leq (rd)^4 \cdot 2^{2d} \cdot |\Delta_K|^{1/d} \cdot 2^{\mathrm{size}(\mathbf{B}) + \mathrm{size}(\mathfrak{p})} \cdot \mathrm{cd}(z) \tag{50}$$

$$\leq (rd)^4 \cdot 2^{2d} \cdot |\Delta_K|^{1/d} \cdot 2^{\mathrm{size}(\mathbf{B}) + \mathrm{size}(\mathfrak{p})} \cdot 2^{4(rd)^2} \cdot |\Delta_K|^{r+1} \cdot 2^{(2rd+2)S} \tag{51}$$

$$\leq 2^{8(rd)^2} \cdot |\Delta_K|^{r+2} \cdot 2^{(2rd+3)\,\mathrm{size}(\mathbf{B}) + \mathrm{size}(\mathfrak{p})}. \tag{52}$$

Combining the bounds Equations (45) and (46), using $\sigma \leq 1$, $t \leq 1$, $d \leq n = rd$, we obtain

$$\begin{aligned}&\|\mathrm{Round}_{\mathrm{Lat}}(T_{\mathcal{P}}(\mathcal{D}_z)) - \mathrm{Round}_{\mathrm{Lat}}(T_{\mathcal{P}}(f_z))\|_1 \\ &\leq N^{-1/4} \cdot \exp(O(n^2 \log n + n \cdot \mathrm{size}(\mathbf{B}) + \max_{\mathfrak{p}\in\mathcal{P}} \mathrm{size}(\mathfrak{p}) + n \log |\Delta_K|)) \cdot \sqrt[4]{\log(1/\varepsilon_0)}. \end{aligned} \tag{53}$$

Hence by choosing

$$\log(N) = O(n^2 \log n + n \cdot \mathrm{size}(\mathbf{B}) + n^2 \cdot \log(B) + n \log |\Delta_K| + \log(1/\varepsilon_0) + 4\log(1/\varepsilon)) \tag{54}$$

(where we use that $\max_{\mathfrak{p}\in\mathcal{P}} \mathrm{size}(\mathfrak{p}) \leq n^2 \log B$, by Lemma 2.3) we obtain an error

$$\|\mathrm{Round}_{\mathrm{Lat}}(T_{\mathcal{P}}(\mathcal{D}_z)) - \mathrm{Round}_{\mathrm{Lat}}(T_{\mathcal{P}}(f_z))\|_1 \leq \varepsilon.$$

By the property (ii) in Proposition 3.1, we have that $\mathrm{Round}^{\mathrm{Perf}}_{\mathrm{Lat}}(T_{\mathcal{P}}(f_z)) = \mathrm{Round}^{\mathrm{Perf}}_{\mathrm{Lat}}(T_{\mathcal{P}}(\varphi_z))$. The same proposition shows that

$$\left\|\mathrm{Round}^{\mathrm{Perf}}_{\mathrm{Lat}}(T_{\mathcal{P}}(f_z)) - \mathrm{Round}_{\mathrm{Lat}}(T_{\mathcal{P}}(f_z))\right\|_1 \leq \varepsilon_0$$

and we are done by the triangle inequality. □

9.3 Preliminaries on sizes and conditioning numbers

Lemma 9.2. *Let $(\mathbf{B}, \mathbf{I})$ be a pseudo-basis of a module lattice M and put $S = \mathrm{size}(\mathbf{B}, \mathbf{I})$ (as in Section 2.3.3). Then $\mathrm{cd}(\mathbf{B}) \leq 2^{4(rd)^2} \cdot |\Delta_K|^{r+1} \cdot 2^{(2rd+2)S}$.*

Proof. By definition, $\mathrm{cd}(\mathbf{B}) = \|\mathbf{B}\|\|\mathbf{B}^{-1}\|$, where we interpret the induced norm $\|\cdot\|$ from the Euclidean norm on $K^r_{\mathbb{R}}$. It suffices to bound both $\|\mathbf{B}\|$ and $\|\mathbf{B}^{-1}\|$ in terms of the bound on the size S.

We have $\|\mathbf{B}\| \leq (rd)^2 \cdot \max_{ij} \|\mathbf{B}_{ij}\| \leq (rd)^2 \cdot 2^d \cdot |\Delta_K|^{1/d} \cdot 2^S$, since the coefficient $\mathbf{B}_{ij} = \sum_i a_i \beta_i$, with $(\beta_1, \ldots, \beta_d)$ an LLL-reduced integral basis of $\mathcal{O}_K$, satisfies

$$\|\mathbf{B}_{ij}\| \leq \max_i |a_i| \cdot \max_j \|\beta_j\| \leq 2^d \cdot |\Delta_K|^{1/d} \cdot 2^S.$$

Using Lemma A.1, seeing $\mathbf{B}$ as a basis of a free $\mathcal{O}_K$-module, using that $\lambda_1(\mathbf{B} \cdot \mathcal{O}^r_K) \geq 2^{-S}$ (since the least common multiple of the denominators occurring in $\mathbf{B}$ can be at most 2^S), and using the previous result on the bound on (columns of) $\mathbf{B}$, we obtain

$$\begin{aligned}\|\mathbf{B}^{-1}\| &\leq (rd)^{rd/2+1} \cdot 2^S \cdot \left(\frac{(rd)^2 \cdot 2^d \cdot |\Delta_K|^{1/d} \cdot 2^S}{2^{-S}}\right)^{rd} \\ &\leq (rd)^{rd/2+1} \cdot 2^{(2rd+1)S} \cdot (rd)^{2rd} \cdot 2^{rd^2} \cdot |\Delta_K|^r\end{aligned}$$

Combining the two results, we obtain

$$\begin{aligned}\mathrm{cd}(\mathbf{B}) &\leq (rd)^{rd/2+1} \cdot 2^{(2rd+1)S} \cdot (rd)^{2rd} \cdot 2^{rd^2} \cdot |\Delta_K|^r \cdot (rd)^2 \cdot 2^d \cdot |\Delta_K|^{1/d} \cdot 2^S \\ &\leq 2^{4(rd)^2} \cdot |\Delta_K|^{r+1} \cdot 2^{(2rd+2)S}.\end{aligned}$$

Here, the last simplification in terms of rd can be obtained graphically. □

Lemma 9.3. *Let $(\mathbf{B}, \mathbf{I})$ with $\mathbf{B} \in K^{r\times r}_{\mathbb{R}}$ and $\mathbf{I} = (\mathfrak{a}_1, \ldots, \mathfrak{a}_r)$ be a pseudo-basis of a module lattice M with $S = \mathrm{size}(\mathbf{B}, \mathbf{I})$. Let $M' \subseteq M$ be a sub-module lattice satisfying $M/M' \simeq \mathcal{O}_K/\mathfrak{p}$ for some prime ideal $\mathfrak{p}$, constructed by multiplying one of the ideals $\mathfrak{a}_i$ by $\mathfrak{p}$ and by multiplying $\mathbf{B}$ from the right by $id + \sum_{j>i} \alpha_j \cdot e_{ij}$ with $\alpha_j \in \mathfrak{a}_i/(\mathfrak{p}\mathfrak{a}_i)$ (here e_{ij} is the matrix that has 1 on the*

ij-th position and zero elsewhere), see also Algorithm 1, resulting in the pseudo-basis $(\mathbf{B}', \mathbf{I}')$ *of* M'.

Then

$$\mathrm{cd}(\mathbf{B}') \leq (rd)^4 \cdot 2^{2d} \cdot |\Delta_K|^{1/d} \cdot 2^{S+\mathrm{size}(\mathfrak{p})} \cdot \mathrm{cd}(B)$$

and

$$\mathrm{size}(\mathbf{B}', \mathbf{I}') \leq 3S + 4\,\mathrm{size}(\mathfrak{p}) \cdot d \cdot \log|\Delta_K|.$$

Proof. Writing $\mathbf{A} = \mathrm{id} + \sum_{j>i} \alpha_j \cdot e_{ij}$ we have that, by submultiplicativity of the conditioning number,

$$\mathrm{cd}(\mathbf{B}') = \mathrm{cd}(\mathbf{BA}) \leq \mathrm{cd}(\mathbf{B}) \cdot \mathrm{cd}(\mathbf{A}).$$

Since $\mathbf{A}$ has a very simple and similar inverse, namely $\mathbf{A}^{-1} = \mathrm{id} - \sum_{j>i} \alpha_j \cdot e_{ij}$, we can bound

$$\mathrm{cd}(\mathbf{A}) = \|\mathbf{A}\|\|\mathbf{A}^{-1}\| \leq (rd)^4 \max_j \|\alpha_j\| \leq (rd)^4 \cdot 2^d \cdot |\Delta_K|^{1/d} \cdot 2^{\max_j \mathrm{size}(\alpha_j)},$$

by similar arguments as in Lemma 9.2. Since $\alpha_j \in \mathfrak{a}_i/(\mathfrak{p}\mathfrak{a}_i)$, we can deduce that (by clearing denominators of $\mathfrak{a}_i$ by k and observing that the Hermite normal form of the ideal $k\mathfrak{p}\mathfrak{a}_i$ has coefficients at most $N(k\mathfrak{p}\mathfrak{a}_i)$) we must have $\mathrm{size}(\alpha_j) \leq \mathrm{size}(\mathfrak{p}) + \mathrm{size}(\mathfrak{a}_i) + d$, and hence

$$\mathrm{cd}(\mathbf{A}) \leq (rd)^4 \cdot 2^{2d} \cdot |\Delta_K|^{1/d} \cdot 2^{S+\mathrm{size}(\mathfrak{p})},$$

which finishes the bound on $\mathrm{cd}(\mathbf{B}')$. For the bound on $\mathrm{size}(\mathbf{B}', \mathbf{I}')$ note that $\mathrm{size}(\mathbf{I}') = \sum_{j=1, j\neq i}^{r} \mathrm{size}(\mathfrak{a}_j) + \mathrm{size}(\mathfrak{p}\mathfrak{a}_i) \leq \mathrm{size}(\mathbf{I}) + \mathrm{size}(\mathfrak{p}) + d \leq S + \mathrm{size}(\mathfrak{p}) + d$. For the size of $\mathbf{B}'$, note that $\mathbf{B}' = \mathbf{BA}$, with $\mathbf{A} = \mathrm{id} + \sum_{j>i} \alpha_j \cdot e_{ij}$, which means that for each $j > i$, the j-th column of $\mathbf{B}$ is increased by α_j times the i-th column. Hence, the size of B' can be maximally

$$S + \mathrm{size}(\mathfrak{p}) \cdot 2d \cdot \log|\Delta_K| + \mathrm{size}(\mathbf{B}) \leq 2S + \mathrm{size}(\mathfrak{p}) \cdot 2d \cdot \log|\Delta_K|.$$

Combining the results then yields a bound of $\mathrm{size}(\mathbf{B}', \mathbf{I}') \leq 3S + 4\,\mathrm{size}(\mathfrak{p}) \cdot d \cdot \log|\Delta_K|$. □

9.4 Discretization in general

Lemma 9.4. *Let* X *be a probability space and let* Y *be any set. Let* $h \in L^1(X)$ *be a distribution and let* $\ddot{h} \in L^1(X)$ *a distribution with finite support* $\ddot{X}$*. Let* $\{C_{\ddot{x}}\}$ *be a collection of finite measure subsets of* X *with* $\ddot{x} \in C_{\ddot{x}}$ *and let* $T \subset X$*, so that* $T \cup \bigcup_{\ddot{x}\in\ddot{X}} C_{\ddot{x}} = X$ *is a disjoint union. Let* $\mathcal{A}_x : X \to L^1(Y)$ *be a map sending* $x \in X$ *to a distribution on* Y*.*

Then

$$\|\mathop{\mathbb{E}}_{x\leftarrow h}[\mathcal{A}_x] - \mathop{\mathbb{E}}_{\ddot{x}\leftarrow \ddot{h}}[\mathcal{A}_{\ddot{x}}]\| = \left\| \int_{x\in X} \mathcal{A}_x \cdot h(x)dx - \sum_{\ddot{x}\in\ddot{X}} \mathcal{A}_{\ddot{x}} \cdot \ddot{h}(\ddot{x}) \right\| \tag{55}$$

$$\leq \Delta(h, \ddot{h}) + \mathcal{C}(h, \ddot{h}, \mathcal{A}) + \mathcal{T}(h), \tag{56}$$

with discretization error

$$\Delta(h, \ddot{h}) := \sum_{\ddot{x}\in\ddot{X}} \int_{x\in C_{\ddot{x}}} |h(x) - \frac{\ddot{h}(\ddot{x})}{|C_{\ddot{x}}|}|dx$$

continuity error

$$\mathcal{C}(\ddot{h}, \mathcal{A}) := \sum_{\ddot{x}\in\ddot{X}} \ddot{h}(\ddot{x}) \frac{1}{|C_{\ddot{x}}|} \int_{x\in C_{\ddot{x}}} \|\mathcal{A}_x - \mathcal{A}_{\ddot{x}}\|_1 dx,$$

and tail error $\mathcal{T}(h) = \int_{x\in T} h(x)dx$.

Additionally, the continuity error satisfies the bounds

$$\mathcal{C}(\ddot{h}, \mathcal{A}) \leq \max_{\ddot{x}\in\ddot{X}} \frac{1}{|C_{\ddot{x}}|} \int_{x\in C_{\ddot{x}}} \|\mathcal{A}_x - \mathcal{A}_{\ddot{x}}\|_1 dx \leq \max_{\ddot{x}\in\ddot{X}} \max_{x\in C_{\ddot{x}}} \|\mathcal{A}_x - \mathcal{A}_{\ddot{x}}\|_1$$

Proof. Use

$$\mathcal{A}_x \cdot h(x) - \mathcal{A}_{\ddot{x}} \cdot \ddot{h}(\ddot{x}) = \mathcal{A}_x \cdot h(x) - \mathcal{A}_x \cdot \ddot{h}(\ddot{x}) + \mathcal{A}_x \cdot \ddot{h}(\ddot{x}) - \mathcal{A}_{\ddot{x}} \cdot \ddot{h}(\ddot{x})$$

and the disjoint union $X = T \cup \bigcup_{\ddot{x} \in \ddot{X}} C_{\ddot{x}}$ to obtain

$$\begin{aligned}
&\int_{x \in X} \mathcal{A}_x h(x) dx - \sum_{\ddot{x} \in \ddot{X}} \mathcal{A}_{\ddot{x}} \ddot{h}(\ddot{x}) \\
&= \int_{x \in T} \mathcal{A}_x h(x) dx + \sum_{\ddot{x} \in \ddot{X}} \int_{x \in C_{\ddot{x}}} \mathcal{A}_x [h(x) - \frac{\ddot{h}(\ddot{x})}{|C_{\ddot{x}}|^{-1}}] dx && (57) \\
&+ \sum_{\ddot{x} \in \ddot{X}} \ddot{h}(\ddot{x}) \frac{1}{|C_{\ddot{x}}|} \int_{x \in C_{\ddot{x}}} [\mathcal{A}_x - \mathcal{A}_{\ddot{x}}] dx. && (58)
\end{aligned}$$

Note that the expression in Equation (58) is a distribution in $L^1(Y)$. So, by taking the 1-norm on $L^1(Y)$ and putting the norm within the integrals (a form of triangle inequality), one obtains the following inequality, using that $\|\mathcal{A}_x\| = 1$,

$$\begin{aligned}
&\left\| \int_{x \in X} \mathcal{A}_x \cdot h(x) dx - \sum_{\ddot{x} \in \ddot{X}} \mathcal{A}_{\ddot{x}} \cdot \ddot{h}(\ddot{x}) \right\| && (59) \\
&\leq \int_{x \in T} h(x) dx + \sum_{\ddot{x} \in \ddot{X}} \int_{x \in C_{\ddot{x}}} |h(x) - \frac{\ddot{h}(\ddot{x})}{|C_{\ddot{x}}|^{-1}}| dx + \sum_{\ddot{x} \in \ddot{X}} \ddot{h}(\ddot{x}) \frac{1}{|C_{\ddot{x}}|} \int_{x \in C_{\ddot{x}}} \|\mathcal{A}_x - \mathcal{A}_{\ddot{x}}\|_1 dx && (60) \\
&= \mathcal{T}(h) + \Delta(h, \ddot{h}) + \mathcal{C}(h, \ddot{h}, \mathcal{A}). && (61)
\end{aligned}$$

Here, the last equality holds by definition. Additionally, by Hölder's inequality, and the fact that the $\ddot{h}(\ddot{x})$ sum to one (it is a distribution), one obtains the bound

$$\mathcal{C}(\ddot{h}, \mathcal{A}) \leq \max_{\ddot{x} \in \ddot{X}} \frac{1}{|C_{\ddot{x}}|} \int_{x \in C_{\ddot{x}}} \|\mathcal{A}_x - \mathcal{A}_{\ddot{x}}\|_1 dx \leq \max_{\ddot{x} \in \ddot{X}} \max_{x \in C_{\ddot{x}}} \|\mathcal{A}_x - \mathcal{A}_{\ddot{x}}\|_1.$$

□

9.5 Discretization of the Gaussian distribution over H

9.5.1 The continuous and the finite distribution

The continuous distribution We denote $H = \{(h_\nu)_\nu \in \prod_\nu \mathbb{R} \mid \sum_\nu h_\nu = 0\}$ for the logarithmic unit hyper plane, with standard Euclidean metric[8]. The continuous distribution over H is the *Gaussian distribution* $\mathcal{G}_{H,\sigma}$ defined as in Definition 2.18.

The finite distribution Choosing an ordering $\{\nu_1, \dots, \nu_{\ell+1}\}$ (with $\ell = \dim(H)$) of the places, we define a basis B_H of H consisting of the basis elements $\mathbf{b}_j = \mathbf{e}_{\nu_{j+1}} - \mathbf{e}_{\nu_j}$ for $j = 1, \dots, \ell$. Here, $\mathbf{e}_{\nu_j}$ is the element of H that is one at the place ν_j and zero elsewhere. Given a discretization parameter $N \in \mathbb{Z}_{>0}$, this allows us to define the discrete Gaussian distribution, written $\mathcal{G}_{\ddot{H},\sigma}$ (see Definition 2.19) with

$$\ddot{H} := \frac{1}{N} B_H \mathbb{Z}^\ell = \{\sum_{j=1}^{\ell} z_j \mathbf{b}_{\nu_j} \mid z_j \in \frac{1}{N}\mathbb{Z} \text{ for all } j\}.$$

[8]The Euclidean length on H is not consistent with that in [BDP+20, Section 2.1], in which the Euclidean length is defined over the embeddings and accounts to $(\sum_\nu [K_\nu : \mathbb{R}] h_\nu^2)^{1/2}$. This does not pose a real problem, since it merely increases the hidden constant of the main result [BDP+20, Theorem 3.3] of that work by a small constant.

The finite distribution over $\ddot{H}$ that we will use in this work is a finite *approximation* of this discrete Gaussian distribution [Kle00; GPV08], which we denote $\ddot{\mathcal{G}}_\sigma$, that can be efficiently sampled and that deviates only slightly from $\mathcal{G}_{\ddot{H},\sigma}$. More precisely [FPS+23b, Lemma A.7] states that, for any $\varepsilon_{\mathcal{G}} > 0$, by paying time polynomial in the size of the input and in $\log(1/\varepsilon_{\mathcal{G}})$, we can manage to have the approximation as good as $\|\ddot{\mathcal{G}}_\sigma - \mathcal{G}_{\ddot{H},\sigma}\|_1 \leq \varepsilon_{\mathcal{G}}$; and, additionally, any sample v from $\ddot{\mathcal{G}}_\sigma$ satisfies $\|v\| \leq \sigma \cdot \sqrt{\log(1/\varepsilon) + 4n}$. That is, $\ddot{\mathcal{G}}_\sigma$ is supported on vectors in $v \in \ddot{H}$ satisfying $\|v\| \leq \sigma \cdot \sqrt{\log(1/\varepsilon) + 4n}$ (which is a finite set).

9.5.2 The tail error and the discretization error

The tail error We fix $N \in \mathbb{Z}_{>0}$ and $\varepsilon_{\mathcal{G}} = \frac{1}{N}$ and we write

$$\ddot{H}_{\text{fin}} = \{\ddot{h} \in \ddot{H} \mid \|\ddot{h}\| \leq \sqrt{2} \cdot \sigma \cdot \sqrt{n} \cdot \sqrt{\log(n/\varepsilon_{\mathcal{G}}) + 4}\}.$$

We write $F_H := \{x \in H \mid x_i \in [-\frac{1}{2N}, \frac{1}{2N}) \text{ for all } i\}$ and for each $\ddot{h} \in \ddot{H}_{\text{fin}}$ we put $C_{\ddot{h}} := \ddot{h} + F_H$. We put $T = H \backslash (\bigcup_{\ddot{h} \in \ddot{H}} C_{\ddot{h}})$, so that $T \cup \bigcup_{\ddot{h} \in \ddot{H}} C_{\ddot{h}}$ is a disjoint union.

We can then reasonably bound

$$\mathcal{T}(\mathcal{G}_{\sigma,H}) = \int_{h \in T} \mathcal{G}_{\sigma,H}(h)dh \leq \int_{\|h\| \geq \sigma \cdot \sqrt{n(\log(1/\varepsilon_{\mathcal{G}})+4)}} \mathcal{G}_{\sigma,H}(h)dh \leq \varepsilon_{\mathcal{G}} = N^{-1}. \tag{62}$$

This holds because writing $h = \sum_{i=1}^{\dim(H)} c_i h_i$ in an orthonormal basis yields that $\max_i c_i \geq \|h\|_2/\sqrt{\dim(H)} \geq \|h\|_2/\sqrt{n} \geq \sqrt{2}\sigma\sqrt{\log(n/\varepsilon_{\mathcal{G}}) + 4}$. Since the coefficients c_i are all independently Gaussian distributed with the same parameter σ (but with a single variable), we have that the probability that $\max_i c_i \geq t := \sqrt{2}\sigma \cdot \sqrt{\log(n/\varepsilon_{\mathcal{G}}) + 4}$ is at most $n \cdot \exp(-t^2/(2\sigma^2)) \leq n \cdot \exp(-(\log(n/\varepsilon_{\mathcal{G}}) + 4)) \leq \varepsilon_{\mathcal{G}}$.

The discretization error To estimate the discretization error, we use that $\ddot{\mathcal{G}}_\sigma$ is an $\varepsilon_{\mathcal{G}}$-close approximation of $\mathcal{G}_{\sigma,\ddot{H}}$, and hence we can conclude that

$$\Delta(\mathcal{G}_{\sigma,H}, \ddot{\mathcal{G}}_\sigma) \leq \Delta(\mathcal{G}_{\sigma,H}, \mathcal{G}_{\sigma,\ddot{H}}) + \varepsilon_{\mathcal{G}}. \tag{63}$$

So it remains to bound $\Delta(\mathcal{G}_{\sigma,H}, \mathcal{G}_{\sigma,\ddot{H}})$. Before doing that, we need to apply a result on Gaussian smoothing.

We can apply Lemma 2.17 to the Gaussian sum $\mathcal{G}_{\sigma,H}$ over the *shifted* ℓ-dimensional lattice $\ddot{H} + h$, where $\ddot{H} = \frac{1}{N} B_H \mathbb{Z}^\ell$ and $h \in H$. Since $\lambda_\ell(\ddot{H}) \leq \frac{2}{N}$, we can deduce that for

$$\sigma \geq \sqrt{\frac{\log(2n(1+1/\varepsilon))}{\pi}} \cdot \frac{2}{N} \tag{64}$$

(for some $\varepsilon > 0$) holds that, for any $h \in H$, (see Definition 2.18)

$$\mathcal{G}_{\sigma,H}(\ddot{H} + h) \in [1-\varepsilon, 1+\varepsilon] \frac{1}{\det(\ddot{H})}$$

Lemma 9.5. *Let $N \in \mathbb{Z}_{>0}$ and let $\ddot{H} = \frac{1}{N} B_H \mathbb{Z}^\ell$, and let $F_H = \frac{1}{N} B_H [-1/2, 1/2)^\ell$ be a fundamental domain of $\ddot{H}$ in H. Let $\sigma \geq \sqrt{\frac{\log(2n(1+N))}{\pi}} \cdot \frac{4}{N}$ (which is twice as large as Equation (64) with $\varepsilon = 1/N$).*

Then

$$\Delta(\mathcal{G}_{\sigma,H}, \mathcal{G}_{\sigma,\ddot{H}}) \leq (1 + 8\ell\sigma)N^{-1/2}.$$

Proof. Writing out the definition of $\Delta(\mathcal{G}_{\sigma,H}, \mathcal{G}_{\sigma,\ddot{H}})$ and $\mathcal{G}_{\sigma,\ddot{H}}(\ddot{h}) = \mathcal{G}_{\sigma,H}(\ddot{h})/\mathcal{G}_{\sigma,H}(\ddot{H})$, we have

$$\begin{aligned}\Delta(\mathcal{G}_{\sigma,H}, \mathcal{G}_{\sigma,\ddot{H}}) &= \int_{h\in F} \sum_{\ddot{h}\in\ddot{H}} |\mathcal{G}_{\sigma,H}(\ddot{h}+h) - |F|^{-1}\ddot{\mathcal{G}}_{\sigma,\ddot{H}}(\ddot{h})|dh \\ &= |F|^{-1} \int_{h\in F} \sum_{\ddot{h}\in\ddot{H}} |\frac{|F|\cdot\mathcal{G}_{\sigma,H}(\ddot{H}+h)\mathcal{G}_{\sigma,H}(\ddot{h}+h)}{\mathcal{G}_{\sigma,H}(\ddot{H}+h)} - \frac{\mathcal{G}_{\sigma,H}(\ddot{h})}{\mathcal{G}_{\sigma,H}(\ddot{H})}|dh \end{aligned} \tag{65}$$

By Lemma 2.17 and the text immediately after that lemma (which applies it to $\ddot{H}$), we see that, by Definition 2.19, by the fact that $|F| = \det(\ddot{H})$,

$$|F|\cdot\mathcal{G}_\sigma(\ddot{H}+h) \in [1-\frac{1}{N}, 1+\frac{1}{N}]$$

Hence, we obtain that Equation (65) is at most

$$\frac{1}{N} + |F|^{-1} \int_{h\in F} \sum_{\ddot{h}\in\ddot{H}} \Big|\frac{\mathcal{G}_\sigma(\ddot{h}+h)}{\mathcal{G}_\sigma(\ddot{H}+h)} - \frac{\mathcal{G}_\sigma(\ddot{h})}{\mathcal{G}_\sigma(\ddot{H})}\Big|dh \tag{66}$$

$$\leq \frac{1}{N} + \max_{h\in F} \sum_{\ddot{h}\in\ddot{H}} \Big|\frac{\mathcal{G}_\sigma(\ddot{h}+h)}{\mathcal{G}_\sigma(\ddot{H}+h)} - \frac{\mathcal{G}_\sigma(\ddot{h})}{\mathcal{G}_\sigma(\ddot{H})}\Big| \tag{67}$$

where we used Hölder's inequality. Now we use a result from Pellet-Mary and Stehlé [PS21, Lemma 2.3], by seeing $\frac{\mathcal{G}_\sigma(\ddot{h}+h)}{\mathcal{G}_\sigma(\ddot{H}+h)}$ and $\frac{\mathcal{G}_\sigma(\ddot{h})}{\mathcal{G}_\sigma(\ddot{H})}$ as distributions and the sum as the total variation distance. We will postpone the check of the premise of [PS21, Lemma 2.3] ($\eta_{1/2}(\sigma^{-1}\ddot{H}) \leq 1/2$) to the end of this proof. We obtain that Equation (67) is bounded by

$$\frac{1}{N} + 4\sqrt{\ell}\cdot\sigma\cdot\max_{h\in F}\sqrt{\|h\|} \leq \frac{1}{N} + 8\ell\cdot\sigma\cdot N^{-1/2} \leq (1+8\ell\sigma)N^{-1/2},$$

where the last inequality follows from the definition of F.

It remains to show that $\eta_{1/2}(\sigma^{-1}\ddot{H}) \leq 1/2$, i.e., $\eta_{1/2}(\ddot{H}) \leq \sigma/2$. By [MR07, Lemma 3.3] we have that $\eta_{1/2}(\ddot{H}) \leq \eta_{1/N}(\ddot{H}) \leq \sqrt{\frac{\log(2n(1+N))}{\pi}}\cdot\lambda_\ell(\ddot{H}) \leq \sqrt{\frac{\log(2n(1+N))}{\pi}}\cdot\frac{2}{N} \leq \sigma/2$. This finishes the proof. □

We can conclude that the discretization error in case of the Gaussian (since $\varepsilon_{\mathcal{G}} := N^{-1}$) is bounded as follows.

$$\Delta(\mathcal{G}_{\sigma,H}, \ddot{\mathcal{G}}_\sigma) \leq N^{-1} + (1+8\ell\sigma)N^{-1/2} \tag{68}$$

whenever $\sigma \geq \sqrt{\frac{\log(2n(1+N))}{\pi}}\cdot\frac{4}{N}$.

9.5.3 The continuity error

Lemma 9.6. *Let $\mathcal{A}_h$ (for $h \in H$) be the output distribution of Algorithm 2 on input $g\cdot M_h\cdot g'$ for fixed $g, g' \in \mathrm{GL}_r(K_\mathbb{R})$. Let $N \in \mathbb{Z}_{>0}$ be the discretization parameter.*

Then

$$\mathcal{C}(\ddot{\mathcal{G}}_\sigma, \mathcal{A}) \leq 92n^{7/2}\sqrt[4]{\log(12r/\varepsilon_0)}\,\mathrm{cd}(g)^{1/2}\cdot N^{-1/2},$$

where ε_0 is part of the input of Algorithm 2.

Proof. Using the bound on the continuity error of Lemma 9.4, we have

$$\mathcal{C}(\ddot{\mathcal{G}}_\sigma, \mathcal{A}) \leq \max_{\ddot{h}\in\ddot{H}_{\mathrm{fin}}} \max_{h\in F_H} \|\mathcal{A}_{\ddot{h}+h} - \mathcal{A}_{\ddot{h}}\|_1.$$

The distribution $\mathcal{A}$ is the output distribution of Algorithm 2 on input $g \cdot M_h \cdot g'$, where $g, g' \in \mathrm{GL}_r(K_{\mathbb{R}})$. Writing $\mathcal{R}$ for the output distribution of Algorithm 2, we can show that, by Lemma 3.7, writing $L = 92n^3 \sqrt[4]{\log(12r/\varepsilon_0)}$,

$$\begin{aligned}
\|\mathcal{A}_{\ddot{h}+h} - \mathcal{A}_{\ddot{h}}\|_1 &= \|\mathcal{R}(g \cdot M_{\ddot{h}+h} \cdot g') - \mathcal{R}(g \cdot M_{\ddot{h}} \cdot g')\|_1 \\
&\leq L\|gM_{\ddot{h}+h}g'(gM_{\ddot{h}}g')^{-1} - I\|^{1/2} \leq L\|gM_{\ddot{h}+h}M_{\ddot{h}}^{-1}g^{-1} - I\|^{1/2} \\
&\leq L\|gM_hg^{-1} - I\|^{1/2} \leq L\,\mathrm{cd}(g)^{1/2}\|M_h - I\|^{1/2} \\
&\leq L\,\mathrm{cd}(g)^{1/2}\sqrt{n} \cdot N^{-1/2} \leq 92n^{7/2}\sqrt[4]{\log(12r/\varepsilon_0)}\,\mathrm{cd}(g)^{1/2} \cdot N^{-1/2},
\end{aligned}$$

where the last inequality follows from, instantiating $L = 92n^3 \sqrt[4]{\log(12r/\varepsilon_0)}$ and the fact that $M_h - I = \mathrm{diag}(e^{h/r} - 1)$ and hence $\|M_h - I\| \leq |e^{h/r} - 1|_{K_{\mathbb{R}}} \leq \sqrt{n}/N$. □

9.5.4 Concluding all errors

Lemma 9.7. *Let $\mathcal{A}_h$ (for $h \in H$) be the output distribution of Algorithm 2 on input $g \cdot M_h \cdot g'$ for fixed $g, g' \in \mathrm{GL}_r(K_{\mathbb{R}})$ and input $\varepsilon_0 > 0$.*

Let $N \in \mathbb{Z}_{>0}$ be a discretization parameter, and let $\sigma \geq \Omega(N^{-1/2}) \geq \sqrt{\frac{\log(2n(1+N))}{\pi}} \cdot \frac{4}{N}$. Let $\mathcal{G}_{\sigma,H}$ respectively $\ddot{\mathcal{G}}_\sigma$ be the continuous respectively finite distribution described in Section 9.5.1, where the finite distribution is instantiated with discretization parameter $N \in \mathbb{Z}_{>0}$ (and $\varepsilon_{\mathcal{G}} = N^{-1}$).

Then,

$$\|\mathop{\mathbb{E}}_{x \leftarrow \mathcal{G}_{\sigma,H}}[\mathcal{A}_x] - \mathop{\mathbb{E}}_{\ddot{x} \leftarrow \ddot{\mathcal{G}}_\sigma}[\mathcal{A}_{\ddot{x}}]\| \leq N^{-1/2} \cdot O(n^4\,\mathrm{cd}(g)^{1/2}\log(1/\varepsilon_0)^{1/4} + n\sigma).$$

Proof. This is just an application of Lemmas 9.5 and 9.6 and Equation (62), where we simplified

$$N^{-1/2}(92n^{7/2}\sqrt[4]{\log(12r/\varepsilon_0)}\,\mathrm{cd}(g)^{1/2} + 2 + 8d\sigma)$$

into the big-O expression

$$N^{-1/2}O(n^4\,\mathrm{cd}(g)^{1/2}\log(1/\varepsilon_0)^{1/4} + n\sigma).$$

□

9.6 Discretization of the distribution over Δ_t^*

9.6.1 The continuous and the finite distribution

Continuous distribution

Definition 9.8 (Component-wise diagonal distribution)**.** For a fixed place ν, the diagonal distribution $\mathcal{D}_{\mathrm{diag}}^{(\nu)}$ on the polytope Δ_t^* for $t \in \mathbb{R}_{>0}$ (and rank r) is defined by the following procedure.

1. (Sample a uniform element from Δ_t^*, see also Section 8.4.3)
2. Sample $r-1$ independent uniform variables on $[0,1]$ and sort them, yielding
$$(x_1, \ldots, x_{r-1}) \in \Delta^0$$
3. If $(x_1, \ldots, x_{r-1}) \notin S$ as in Equation (34), goto line 1.

4. If $(x_1, \ldots, x_{r-1}) \in S$, put $a_i = t - 2tx_i$ for all i.

5. (Rejection sampling with respect to the diagonal density g (see Equation (33)))

6. With probability $1 - \frac{\bar{g}(a_1,\ldots,a_{r-1})}{\bar{M}}$ reject and goto line 1, where

$$\bar{g} = \prod_{1 \le i < j \le r} \sinh(a_i - a_j)^{[K_\nu:\mathbb{R}]} \text{ and } \bar{M} := (4t)^{r(r-1)} \ge \|\bar{g}\|_\infty$$

7. Output $(a_1, \ldots, a_{r-1})$.

Definition 9.9 (Diagonal distribution)**.** We denote by $\mathcal{D}_{\text{diag}}$ the compound distribution over rank r diagonal matrices over $K_{\mathbb{R}}$ where each ν-component is independently distributed with $\mathcal{D}^{(\nu)}_{\text{diag}}$.

Finite distribution

Definition 9.10 (Component-wise discretized diagonal distribution)**.** For a fixed place ν, the discretized diagonal distribution $\ddot{\mathcal{D}}^{(\nu)}_{\text{diag}}$ on the polytope Δ^*_t for $t \in \mathbb{R}_{>0}$ (and rank r) and discretization parameter $N \in \mathbb{Z}_{>0}$ is defined by the following procedure.

1. (Sample a uniform element from Δ^*_t, see also Section 8.4.3)

2. Sample $r-1$ independent uniform variables in $[0,1) \cap \frac{1}{N}\mathbb{Z}$; sort them, yielding

$$(x_1, \ldots, x_{r-1}) \in \Delta^0$$

3. If $(x_1, \ldots, x_{r-1}) \notin S$ as in Equation (34), goto line 1.

4. If $(x_1, \ldots, x_{r-1}) \in S$, put $a_i = t - 2ty_i$ for all i.

5. (Rejection sampling with respect to the diagonal density g (see Equation (33)))

6. Compute $\tilde{\tau} \in \frac{1}{N^2}\mathbb{Z}$ with $|\tilde{\tau} - \frac{\bar{g}(a_1,\ldots,a_{r-1})}{\bar{M}}| < \frac{1}{2N^2}$, where

$$\bar{g} = \prod_{1 \le i < j \le r} \sinh(a_i - a_j)^{[K_\nu:\mathbb{R}]} \text{ and } \bar{M} := (4t)^{r(r-1)} \ge \|\bar{g}\|_\infty.$$

7. With probability $1 - \tilde{\tau}$ reject and goto line 1.

8. Output $(a_1, \ldots, a_{r-1})$.

Definition 9.11 (Discretized diagonal distribution)**.** We denote by $\ddot{\mathcal{D}}_{\text{diag}}$ the compound distribution over rank r diagonal matrices over $K_{\mathbb{R}}$ where each ν-component is independently distributed with $\ddot{\mathcal{D}}^{(\nu)}_{\text{diag}}$.

Help lemmas

Lemma 9.12. *We have, for $N > 64r^2$,*

$$|S \cap \frac{1}{N}\mathbb{Z}^{r-1}| \in [e^{\frac{-8(r-1)^2 r}{N}}, e^{\frac{8(r-1)^2 r}{N}}] \cdot N^{r-1} \cdot \text{vol}(S),$$

$$|\Delta^0 \cap \frac{1}{N}\mathbb{Z}^{r-1}| \in [e^{\frac{-8(r-1)^2 r}{N}}, e^{\frac{8(r-1)^2 r}{N}}] \cdot N^{r-1} \cdot \text{vol}(\Delta^0).$$

Furthermore,

$$\left|\{x \in S \cap \frac{1}{N}\mathbb{Z}^{r-1} \mid x + (\frac{1}{2N}, \frac{1}{2N}]^{r-1} \not\subseteq S\}\right| \le \frac{64(r-1)^2 r}{N} \cdot N^{r-1} \cdot \text{vol}(S)$$

Proof. We use Lemma A.7 with $\Lambda = \frac{1}{N}\mathbb{Z}^{r-1}$, $X = S - \mathbf{t}'$, $q = 1$, $\mathbf{t} = 0$ and $c = \frac{4r(r-1)}{N}$ to obtain

$$|S \cap \frac{1}{N}\mathbb{Z}^{r-1}| \in [e^{\frac{-8(r-1)^2 r}{N}}, e^{\frac{8(r-1)^2 r}{N}}] \cdot N^{r-1} \cdot \mathrm{vol}(S). \tag{69}$$

Since $\mathcal{V}_0 = (-\frac{1}{2N}, \frac{1}{2N}]^{r-1} \subseteq c(S - \mathbf{t}')$ and $c = \frac{4r(r-1)}{N}$ (and similarly for $X \supset S$). Note that in order to have $1 = q > 2c$, we require $N > 8r^2$.

For the last statement, put $c' = \frac{4r(r-1)}{N}$ note that for $x \in (1-c')[X - \mathbf{t}'] + \mathbf{t}'$, we have

$$x + \mathcal{V}_0 \subseteq (1-c')[X - \mathbf{t}'] + \mathbf{t}' + c'[X - \mathbf{t}'] = X$$

Now, using Lemma A.7 with $\Lambda = \frac{1}{N}\mathbb{Z}^{r-1}$, $X = (1-c')[S - \mathbf{t}']$, $q = 1$, $\mathbf{t} = 0$ and $c = \frac{8r(r-1)}{N}$ we obtain

$$\left|\frac{1}{N}\mathbb{Z}^{r-1} \cap [(1-c)(X - \mathbf{t}') + \mathbf{t}']\right| \in [e^{\frac{-16(r-1)^2 r}{N}}, e^{\frac{16(r-1)^2 r}{N}}] \cdot N^{r-1} \cdot (1-c)^{r-1} \,\mathrm{vol}(S)$$

So, by $(1-c)^{r-1} \geq e^{-c(r-1)} = e^{-16(r-1)^2 r/N}$, we deduce that

$$\left|\frac{1}{N}\mathbb{Z}^{r-1} \cap [(1-c)(X - \mathbf{t}') + \mathbf{t}']\right| \geq e^{-32(r-1)^2 r/N} \cdot N^{r-1} \,\mathrm{vol}(S).$$

Using Equation (69), we obtain

$$\begin{aligned}
&\left|\{x \in S \cap \frac{1}{N}\mathbb{Z}^{r-1} \mid x + (\frac{1}{2N}, \frac{1}{2N}]^{r-1} \subsetneq S\}\right| \\
&\leq |S \cap \frac{1}{N}\mathbb{Z}^{r-1}| - \left|\frac{1}{N}\mathbb{Z}^{r-1} \cap [(1-c)(X - \mathbf{t}') + \mathbf{t}']\right| \\
&\leq [e^{\frac{8(r-1)^2 r}{N}} - e^{\frac{-32(r-1)^2 r}{N}}] \cdot N^{r-1} \,\mathrm{vol}(S) \\
&\leq \frac{64(r-1)^2 r}{N} \cdot N^{r-1} \,\mathrm{vol}(S)
\end{aligned}$$

whenever $\frac{32(r-1)^2 r}{N} < 1/2$, since $e^{8x} - e^{-32x} < 64x$ for $x < 0.4$, which can be verified graphically. □

Lemma 9.13. *We have* $\mathrm{vol}(\Delta_t^*) \leq \frac{(2t)^{r-1}}{(r-1)!}$. *Similarly,* $\mathrm{vol}(S) \leq \frac{1}{(r-1)!}$.

Proof. Write

$$W = \{(x_i)_i \in \mathbb{R}^r \mid 1 \geq x_1 \geq x_2 \geq \ldots \geq x_{r-1} \geq -1 \text{ and } x_r = -\sum_{i=1}^{r-1} x_i\}$$

. Then $\Delta_t^* \subseteq t \cdot W$. But one can prove that, by permuting the first $r-1$ indices of S, that

$$\bigcup_\sigma \sigma(W) = \{(x_i)_i \in \mathbb{R}^r \mid x_i \in [-1,1] \text{ for } i \in \{1, \ldots, r-1\} \text{ and } x_r = -\sum_{i=1}^{r-1} x_i\} =: U,$$

where the σ are all permutations of the first $r-1$ indices. This is (up to sets of measure zero) a disjoint union. The volume of the latter set equals 2^{r-1}... One can see this by applying the linear transformation ϕ that keeps the first $r-1$ indices intact and maps x_r to $x_r \mapsto x_r - \sum_{i=1}^{r-1} x_i$ to the set U; we have that $\phi(U) = \{(x_i)_i \in \mathbb{R}^r \mid x_i \in [-1,1], x_r = 0\}$ has volume 2^r. Hence, U itself has volume 2^r, too, since $\det(\phi) = 1$ (by the substitution rule). Hence, $\mathrm{vol}(W) = \frac{2^{r-1}}{(r-1)!}$. As a consequence, $\mathrm{vol}(\Delta_t^*) \leq \frac{(2t)^{r-1}}{(r-1)!}$. For the bound on the volume on S, note that the map $y_i = \frac{t - a_i}{2t}$ for very $i \in \{1, \ldots, r-1\}$ linearly transforms Δ_t^* into the set S. □

9.6.2 The tail error and the discretization error

The tail error Since the space Δ_t^* is a compact space, we choose $T = 0$, which leads to a tail error of zero.

The discretization error

Lemma 9.14. *Let $N \in \mathbb{Z}_{>0}$ satisfy $N \geq O(de^{8r^2\log(r)})$ and let $t \geq 1$. Then*

$$\Delta(\mathcal{D}_{diag}, \ddot{\mathcal{D}}_{diag}) \leq N^{-1} \cdot O(de^{8r^2\log(r)})$$

Proof. This follows from the fact that each of the components of the distributions of $\mathcal{D}_{\text{diag}}$ and $\ddot{\mathcal{D}}_{\text{diag}}$ are independent of each other. Applying Lemma 9.15, together with the fact that there are at most d places ν, we obtain the claim. □

Lemma 9.15. *Let $r \geq 2$, let $N \geq O(e^{8r^2\log(r)})$, let $t \leq 1$ and let ν some fixed place of K. Let $w = \mathcal{D}_{diag}^{(\nu)} : \Delta_t^* \to \mathbb{R}$ denote the density function of the distribution as in Definition 9.9 and denote $\ddot{w} = \ddot{\mathcal{D}}_{diag}^{(\nu)} : X \to \mathbb{R}$ for the probability function defined by the sampling process in Definition 9.11, where $X = [t \cdot \mathbf{1} - \frac{2t}{N} \cdot \mathbb{Z}^{r-1}] \cap \Delta_t^*$ (where $\mathbf{1}$ is the all-one vector). Write, for every $\ddot{a} \in X$, $F_{\ddot{a}} = (\ddot{a} + [-\frac{t}{N}, \frac{t}{N})^{r-1}) \cap \Delta_t^*$.*

Then

$$\Delta(\mathcal{D}_{diag}^{(\nu)}, \ddot{\mathcal{D}}_{diag}^{(\nu)}) = \sum_{\ddot{a}\in X} \int_{a\in F_{\ddot{a}}} |w(a) - \frac{\ddot{w}(\ddot{a})}{|F_{\ddot{a}}|}| da \leq N^{-1} \cdot O(e^{8r^2\log(r)}).$$

Proof. Note that $|X| = [t\cdot\mathbf{1} - \frac{2t}{N}\cdot\mathbb{Z}^{r-1}]\cap\Delta_t^* = \psi(\frac{1}{N}\mathbb{Z}^{r-1}\cap S)$ with the linear bijection ψ sending $y_i \mapsto t - 2ty_i$ for each component. Hence, by Lemma 9.12,

$$|X| = |\frac{1}{N}\mathbb{Z}^{r-1} \cap S| \in [e^{\frac{-8(r-1)^2 r}{N}}, e^{\frac{8(r-1)^2 r}{N}}] \cdot N^{r-1} \cdot \mathrm{vol}(S)$$

which implies, together with $N \geq 8r^{10r^2} \geq 8r^3$ and Lemma 9.13, that $|X| \leq N^{r-1} \cdot \frac{e}{(r-1)!}$.

We have $w(a) = g(a) = c\bar{g}(a)$ (for all $a \in \Delta_t^*$), as in Equation (33). We also would like to write $\ddot{w}(\ddot{a})$ in terms of $g(\ddot{a})$. By the procedure described in Definition 9.11 we can deduce that

$$\ddot{w}(\ddot{a}) \in c_1 \cdot c_0 \cdot [\frac{\bar{g}(\ddot{a})}{\bar{M}} - \frac{1}{N^2}, \frac{\bar{g}(\ddot{a})}{\bar{M}} + \frac{1}{N^2}], \tag{70}$$

for some constants $c_1, c_0 \in \mathbb{R}_{>0}$. By the fact that $\ddot{w}$ is a probability function, we also have $\sum_{\ddot{a}\in X} \ddot{w}(\ddot{a}) = 1$, which gives means of estimating $c_1 \cdot c_0$. As an Ansatz, we put $c_0 = \frac{\bar{M}\cdot c}{N_0^{r-1}}$, where $N_0 = N/(2t)$ and where $c \in \mathbb{R}_{>0}$ is the same c as in the identity $g = c\bar{g}$; this choice is made in order to make c_1 close to one. This then yields (using $g = c\bar{g}$), and writing $\delta_0 := c_0/N^2$,

$$\ddot{w}(\ddot{a}) \in c_1 [\frac{g(\ddot{a})}{N_0^{r-1}} - \delta_0, \frac{g(\ddot{a})}{N_0^{r-1}} + \delta_0], \tag{71}$$

Our proof will now consist of a few technical parts.

Claim (a):

$$\sum_{\ddot{a}\in X} \int_{a\in F_{\ddot{a}}} |g(a) - g(\ddot{a})| da \leq \delta_1 := \frac{r \cdot \mathrm{Lip}(g) \cdot \mathrm{vol}(\Delta_t^*)}{N_0} \tag{72}$$

Proof of claim (a): We show that

$$\sum_{\ddot{a}\in X} |F_{\ddot{a}}| g(\ddot{a}) \underbrace{\approx}_{\text{error } \delta_1} \int_{a\in\Delta_t^*} g(a) da = 1$$

by the Lipschitz-continuity of g. By splitting up the space Δ_t^* into pieces $F_{\ddot{a}}$, we obtain, by the fact that $|a - \ddot{a}| \leq r/N_0$,

$$\sum_{\ddot{a}\in X} |F_{\ddot{a}}|g(\ddot{a}) - \int_{a\in\Delta_t^*} g(a)da \leq \sum_{\ddot{a}\in X} \int_{a\in F_{\ddot{a}}} |g(\ddot{a}) - g(a)|da \leq \sum_{\ddot{a}\in X} \int_{a\in F_{\ddot{a}}} \mathrm{Lip}(g) \cdot \frac{r}{N_0} da$$
$$\leq \frac{r \cdot \mathrm{Lip}(g) \cdot \mathrm{vol}(\Delta_t^*)}{N_0} = \delta_1$$

Claim (b):

$$\sum_{\ddot{a}\in X} \left| |F_{\ddot{a}}|g(\ddot{a}) - \frac{g(\ddot{a})}{N_0^{r-1}} \right| \leq \delta_2 := \frac{64(r-1)^2 r}{N} \cdot \|g\|_\infty \cdot (2t)^{r-1} \,\mathrm{vol}(S). \tag{73}$$

Proof of claim (b): We will show that

$$\left| \sum_{\ddot{a}\in X} \frac{g(\ddot{a})}{N_0^{r-1}} - \sum_{\ddot{a}\in X} |F_{\ddot{a}}|g(\ddot{a}) \right| \leq \sum_{\ddot{a}\in X} \left| \frac{g(\ddot{a})}{N_0^{r-1}} - |F_{\ddot{a}}|g(\ddot{a}) \right| \leq \delta_2.$$

This inequality stems from the fact that, for most $\ddot{a} \in X$ holds that $|F_{\ddot{a}}| = N_0^{-(r-1)}$ (all of them, except those at the edge of Δ_t^*).

Our goal is to count those $\ddot{a}$ for which $|F_{\ddot{a}}| < N_0^{-(r-1)}$. By the last statement of Lemma 9.12 (considering the linear map between S and Δ_t^*), there are at most $\frac{64(r-1)^2 r}{N} \cdot N^{r-1} \cdot \mathrm{vol}(S)$ of these.

Hence,

$$\left| N_0^{-(r-1)} \sum_{\ddot{a}\in X} g(\ddot{a}) - \sum_{\ddot{a}\in X} |F_{\ddot{a}}|g(\ddot{a}) \right| \leq \|g\|_\infty \cdot N_0^{-(r-1)} \cdot \frac{64(r-1)^2 r}{N} \cdot \mathrm{vol}(S) \cdot N^{r-1}$$
$$\leq \frac{64(r-1)^2 r}{N} \cdot \|g\|_\infty \cdot (2t)^{r-1} \,\mathrm{vol}(S) = \delta_2,$$

where we use that $N_0 = N/(2t)$.

Claim (c):

$$\sum_{\ddot{a}\in X} \frac{g(\ddot{a})}{N_0^{r-1}} \in [1 - \delta_1 - \delta_2, 1 + \delta_1 + \delta_2]. \tag{74}$$

in particular $\sum_{\ddot{a}\in X} \frac{g(\ddot{a})}{N_0^{r-1}} \leq 2$ if $\delta_1 + \delta_2 \leq 1$.

Proof of claim (c): By using part (a) and (b) we can deduce that

$$N_0^{-(r-1)} \sum_{\ddot{a}\in X} g(\ddot{a}) \underbrace{\approx}_{\text{error } \delta_2} \sum_{\ddot{a}\in X} |F_{\ddot{a}}|g(\ddot{a}) \underbrace{\approx}_{\text{error } \delta_1} \int_{a\in\Delta_t^*} g(a)da = 1$$

Claim (d):

$$|c_1 - 1| \leq \delta_3 := 2\delta_1 + 2\delta_2 + 2 \cdot |X| \cdot \delta_0. \tag{75}$$

if $\delta_1 + \delta_2 + |X| \cdot \delta_0 \leq 1/4$. In particular, $|c_1| \leq 2$ in that case. This requires the assumption of N being sufficiently large in the lemma.

Proof of claim (d): Combining Equation (71) with the law of total probability, we deduce

$$1 = \sum_{\ddot{a}\in X} \ddot{w}(\ddot{a}) \in c_1 \cdot [\frac{\sum_{\ddot{a}\in X} g(\ddot{a})}{N_0^{r-1}} - |X| \cdot \delta_0, \frac{\sum_{\ddot{a}\in X} g(\ddot{a})}{N_0^{r-1}} + |X| \cdot \delta_0]$$

Hence we can deduce that $|c_1^{-1} - N_0^{-(r-1)} \sum_{\ddot{a}\in X} g(\ddot{a})| \leq |X| \cdot \delta_0$. So, using part (c),

$$|c_1^{-1} - 1| \leq \delta_1 + \delta_2 + |X| \cdot \delta_0$$

and, inverting, assuming the right-hand size being smaller than $1/4$, we obtain

$$|c_1 - 1| \leq 2\delta_1 + 2\delta_2 + 2 \cdot |X| \cdot \delta_0.$$

Conclusion: Combining these results, we obtain the following sequence of inequalities, assuming that $\delta_1 + \delta_2 \leq 1$ and $\delta_1 + \delta_2 + c_1 \cdot |X| \cdot \delta_0 \leq 1/4$.

$$\begin{aligned}
&\sum_{\ddot{a}\in X} \int_{a\in F_{\ddot{a}}} |w(a) - \frac{\ddot{w}(\ddot{a})}{|F_{\ddot{a}}|}| da = \sum_{\ddot{a}\in X} \int_{a\in F_{\ddot{a}}} |g(a) - \frac{\ddot{w}(\ddot{a})}{|F_{\ddot{a}}|}| da \quad \text{(since } w(a) = g(a)\text{)} \\
\leq &\sum_{\ddot{a}\in X} \int_{a\in F_{\ddot{a}}} |g(a) - \frac{c_1 g(\ddot{a})}{|F_{\ddot{a}}| N_0^{r-1}}| da + \sum_{\ddot{a}\in X} c_1\delta_0 \quad \text{(by Equation (71))} \\
\leq &\sum_{\ddot{a}\in X} \int_{a\in F_{\ddot{a}}} |g(a) - \frac{g(\ddot{a})}{|F_{\ddot{a}}| N_0^{r-1}}| da + \delta_3 \sum_{\ddot{a}\in X} \frac{g(\ddot{a})}{N_0^{r-1}} + 2\delta_0|X| \quad \text{(by Equation (75))} \\
\leq &\sum_{\ddot{a}\in X} \int_{a\in F_{\ddot{a}}} |g(a) - \frac{g(\ddot{a})}{|F_{\ddot{a}}| N_0^{r-1}}| da + 2\delta_3 + 2\delta_0|X| \quad \text{(by Equation (74))} \\
\leq &\sum_{\ddot{a}\in X} \int_{a\in F_{\ddot{a}}} |g(a) - g(\ddot{a})| da + \delta_2 + 2\delta_3 + 2\delta_0|X| \quad \text{(by Equation (73))} \\
\leq &\delta_1 + \delta_2 + 2\delta_3 + 2\delta_0|X| \quad \text{(by Equation (72))} \\
\leq &6|X|\delta_0 + 5\delta_1 + 5\delta_2
\end{aligned} \tag{76}$$

where the last inequality follows from writing out the definition $\delta_3 = 2\delta_1 + 2\delta_2 + 2 \cdot |X| \cdot \delta_0$ and using that $|c_1| \leq 2$.

We have $\delta_0 = \frac{\bar{M}c}{N_0^{r-1}N^2} = \frac{\bar{M}c(2t)^{r-1}}{N^{r-1}N^2}$ and $|X| \leq N^{r-1} \cdot \frac{e}{(r-1)!}$. Hence, using that $\bar{M}c \leq (16r^2)^{r(r-1)} \cdot \left(\frac{4r^2}{t}\right)^{r-1}$ by Lemma 8.7,

$$6|X|\delta_0 \leq \frac{6e\bar{M}c(2t)^{r-1}}{(r-1)!N^2} \leq \frac{6e(16r^2)^{r(r-1)}\left(8r^2\right)^{r-1}}{(r-1)!N^2} \leq N^{-2} \cdot O(e^{8r^2\log(r)}). \tag{77}$$

By the fact that $\mathrm{vol}(\Delta_t^*) = (2t)^{(r-1)}\,\mathrm{vol}(S)$, and $N_0 = N/(2t)$ and subsequently the bound $\mathrm{Lip}(g) \leq \frac{r^2}{t} \cdot (16r^2)^{r(r-1)} \cdot \left(\frac{4r^2}{t}\right)^{r-1}$ by Lemma 8.7, we obtain

$$5\delta_1 = \frac{5r \cdot \mathrm{Lip}(g)(2t)^r\,\mathrm{vol}(S)}{N} \leq \frac{5r \cdot (16r^2)^{r(r-1)}(8r^2)^r}{(r-1)!N} \leq N^{-1} \cdot O(e^{8r^2\log(r)}). \tag{78}$$

For the last error, δ_2, note that, $\|g\|_\infty \leq \bar{M}c \leq (16r^2)^{r(r-1)} \cdot \left(\frac{4r^2}{t}\right)^{r-1}$ by Lemma 8.7, we see that

$$5\delta_2 \leq \frac{64(r-1)^2 r}{(r-1)! \cdot N}(16r^2)^{r(r-1)} \cdot \left(8r^2\right)^{r-1} \leq N^{-1} \cdot O(e^{8r^2\log(r)}).$$

This finishes the proof. □

9.6.3 The continuity error

Lemma 9.16. *Let $\mathcal{A}_x$ (for $x \in \mathrm{GL}_r(K_\mathbb{R})$) be the output distribution of Algorithm 2 on input*[9] *$g \cdot e^x \cdot g'$ for fixed $g, g' \in \mathrm{GL}_r(K_\mathbb{R})$. Let $N \in \mathbb{Z}_{>0}$ be the discretization parameter.*

Then

$$\mathcal{C}(\ddot{\mathcal{D}}_{diag}, \mathcal{A}) \leq N^{-1/2} \cdot O(n^5 \cdot \mathrm{cd}(g)^{1/2} \cdot \sqrt[4]{\log(1/\varepsilon_0)})$$

[9] We denote by e^x with a diagonal matrix $x \in \mathrm{GL}_r(K_\mathbb{R})$ the element of $\mathrm{GL}_r(K_\mathbb{R})$ with diagonal $\mathrm{diag}(e^{x_i})_i$, where e^{x_i} is also component-wise over all places of K.

Proof. By using again that the ν-components of $\ddot{\mathcal{D}}_{\mathrm{diag}}$ are independent and commute, we can deduce that

$$\mathcal{C}(\ddot{\mathcal{D}}_{\mathrm{diag}}, \mathcal{A}) \leq d \cdot \max_{\nu} \mathcal{C}(\ddot{\mathcal{D}}^{(\nu)}_{\mathrm{diag}}, \mathcal{A}).$$

Hence, writing out the continuity error, using the bound of Lemma 9.4, with $X = \frac{2t}{N}\mathbb{Z}^{r-1} \cap \Delta^*_t$ and $F_{\ddot{x}} = (\ddot{x} + [-\frac{t}{N}, \frac{t}{N}]) \cap \Delta^*_t$,

$$\mathcal{C}(\ddot{\mathcal{D}}^{(\nu)}_{\mathrm{diag}}, \mathcal{A}) \leq \max_{\ddot{x} \in X} \max_{x \in F_{\ddot{x}}} \|\mathcal{A}_x - \mathcal{A}_{\ddot{x}}\|_1$$

Writing $\mathcal{R}$ for the output distribution of Algorithm 2, we see that (writing $e^{x'}$ for the diagonal on the not-ν-component), using Lemma 3.7,

$$\begin{aligned}
\|\mathcal{A}_x - \mathcal{A}_{\ddot{x}}\|_1 &= \|\mathcal{R}_{ge^x e^{x'} g'} - \mathcal{R}_{ge^{\ddot{x}} e^{x'} g'}\|_1 \leq L \cdot \|ge^x e^{x'} g' (ge^{\ddot{x}} e^{x'} g')^{-1} - I\|^{1/2} \\
&\leq L \cdot \|ge^{x-\ddot{x}} g^{-1} - I\|^{1/2} \leq \mathrm{cd}(g)^{1/2} \cdot L \cdot \|e^{x-\ddot{x}} - I\|^{1/2} \\
&\leq \frac{2 \cdot \mathrm{cd}(g)^{1/2} \cdot L \cdot \sqrt{r}}{N^{1/2}}.
\end{aligned}$$

The last inequality follows from the fact that $\|x - \ddot{x}\|_\infty \leq 2/N$ whenever $x \in F_{\ddot{x}}$ (since $\ddot{x} \in \frac{2t}{N}\mathbb{Z}^{r-1}$ and $t \leq 1$); and the fact that $e^a - 1 \leq 2a$ for $a < 1$. Instantiating $L = 92n^3 \sqrt[4]{\log(1/\varepsilon_0)}$ from Lemma 3.7 yields the claim. □

9.6.4 Run time

Lemma 9.17. *Let $N \geq O(e^{8r^2 \log(r)})$ Then the discretized diagonal distribution $\ddot{\mathcal{D}}_{diag}$ (Definition 9.11) can be sampled from using bit complexity $O(d \cdot e^{8r^2 \log(r)} \log N)$.*

Proof. We show that the procedure described in Definition 9.10 can be run with bit complexity $O(e^{8r^2 \log(r)} \log N)$. Then repeating this for each place ν (which there are at most d) yields the claim.

We now focus on the algorithm in Definition 9.10. The first (inner) loop is about sampling a uniform element from Δ^*_t and consists of lines 2 and 3; the acceptance probability is $\frac{|S \cap \frac{1}{N}\mathbb{Z}^{r-1}|}{|\Delta^0 \cap \frac{1}{N}\mathbb{Z}^{r-1}|}$.

By Lemma 9.12, we can estimate this acceptance probability by

$$\frac{|S \cap \frac{1}{N}\mathbb{Z}^{r-1}|}{|\Delta^0 \cap \frac{1}{N}\mathbb{Z}^{r-1}|} \in [e^{\frac{-16(r-1)^2 r}{N}}, e^{\frac{16(r-1)^2 r}{N}}] \frac{\mathrm{vol}(S)}{\mathrm{vol}(\Delta^0)}$$

Hence, using the lower bound on $\frac{\mathrm{vol}(S)}{e\,\mathrm{vol}(\Delta^0)}$ from Equation (35) in Section 8.4.3, and assuming $N \geq 16r^3$, we deduce

$$\frac{|S \cap \frac{1}{N}\mathbb{Z}^{r-1}|}{|\Delta^0 \cap \frac{1}{N}\mathbb{Z}^{r-1}|} \geq \frac{\mathrm{vol}(S)}{e\,\mathrm{vol}(\Delta^0)} \geq e^{-1} \cdot (2(r-1))^{-(r-1)}.$$

Hence, using that sampling a uniform element in $[0,1) \cap \frac{1}{N}\mathbb{Z}$ costs time $O(\log N)$, we obtain that this first loop takes about $O((2(r-1))^{-(r-1)} \log(N))$ bit operations.

For the second (outer) loop, the acceptance probability is at least (using the notation $\ddot{a}$ and X from Lemma 9.15)

$$\begin{aligned}
-\frac{1}{N^2} + \frac{1}{|S \cap \frac{1}{N}\mathbb{Z}^r|} \sum_{\ddot{a} \in X} \frac{\bar{g}(\ddot{a})}{\bar{M}} &\geq -\frac{1}{N^2} + \frac{1}{|S \cap \frac{1}{N}\mathbb{Z}^r|} \frac{1}{c\bar{M}} \sum_{\ddot{a} \in X} g(\ddot{a}) \\
&\geq -\frac{1}{N^2} + \frac{N_0^{r-1}}{c\bar{M}|S \cap \frac{1}{N}\mathbb{Z}^r|}. \qquad (79)
\end{aligned}$$

where the last lower bound comes from Equation (74) (where we need to assume $N \geq O(e^{8r^2\log(r)})$). We note that from $N \geq 8r^3$ and Lemma 9.13, we see that $|S \cap \frac{1}{N}\mathbb{Z}^{r-1}| \leq N^{r-1} \cdot \frac{e}{(r-1)!}$. And, using the bound $c\bar{M} \leq (16r^2)^{r(r-1)} \cdot \left(\frac{4r^2}{t}\right)^{r-1}$ by Lemma 8.7, we can continue lower bounding Equation (79) by (using $N_0 = N/(2t)$)

$$\geq -\frac{1}{N^2} + \frac{(r-1)!/e \cdot (2t)^{-(r-1)}}{c\bar{M}} \geq -\frac{1}{N^2} + \frac{(r-1)!}{e \cdot (16r^2)^{r(r-1)} \cdot (8r^2)^{r-1}}$$
$$\geq -\frac{1}{N^2} + O(e^{-8r^2\log(r)}) \geq O(e^{-8r^2\log(r)}),$$

by the assumption on N. Hence, the outer loop running time is $O(e^{8r^2\log(r)})$, yielding a total running time of $O(e^{8r^2\log(r)}\log N)$. □

9.6.5 Concluding all errors

Lemma 9.18. *Let $\mathcal{A}_x$ (for $x \in \mathrm{GL}_r(K_\mathbb{R})$) be the output distribution of Algorithm 2 on input*[10] *$g \cdot e^x \cdot g'$ for fixed $g, g' \in \mathrm{GL}_r(K_\mathbb{R})$. Let $N \in \mathbb{Z}_{>0}$ be the discretization parameter that satisfies $N \geq O(de^{8r^2\log(r)})$*

Then Then,

$$\| \mathop{\mathbb{E}}_{x \leftarrow \mathcal{D}_{diag}} [\mathcal{A}_x] - \mathop{\mathbb{E}}_{\ddot{x} \leftarrow \ddot{\mathcal{D}}_{diag}} [\mathcal{A}_{\ddot{x}}] \| \qquad \leq N^{-1/2} \cdot O(de^{8r^2\log(r)} + n^5 \operatorname{cd}(g)^{1/2} \cdot \sqrt[4]{\log(1/\varepsilon_0)}).$$

Proof. This follows from Lemmas 9.14 and 9.16. □

9.7 Discretization of the uniform distribution in $\mathrm{SU}_r(K_\mathbb{R})$

9.7.1 The continuous and the finite distribution

The continuous distribution

Definition 9.19 (Angle distribution)**.** We denote $\Theta^{(r)} = [0, 2\pi] \times [0, \pi]^{r-1}$ and we define on it a density function by the following rule: $\rho^{(r)}(\theta) := \prod_{j=1}^r \rho_j(\theta_j)$ for $\theta = (\theta_1, \ldots, \theta_r) \in \Theta^{(r)}$, where

$$\rho_j(\theta) := \begin{cases} \frac{1}{\sqrt{\pi}} \frac{\Gamma(\frac{j+1}{2})}{\Gamma(\frac{j}{2})} \sin^{j-1}(\theta) & \text{if } j > 1 \\ \frac{1}{2\pi} & \text{if } j = 1 \end{cases}.$$

Definition 9.20 (Uniform distribution on SU_r)**.** As in Definition 8.6, we define the *uniform distribution* on $\mathrm{SU}_r(\mathbb{R})$ by the distribution of $U_\theta \in \mathrm{SU}_r(\mathbb{R})$, the real unitary matrix associated with θ defined by the procedure in Lemma 8.5, where $\theta \in \prod_{j=2}^r S^{j-1}(\mathbb{R})$ is for each component S^{j-1} is sampled according to the (continuous) angle distribution as in Definition 9.19.

Analogously, we define the *uniform distribution* on $\mathrm{SU}_r(\mathbb{C})$ by the distribution of $U_\theta \in \mathrm{SU}_r(\mathbb{C})$, the complex unitary matrix associated with θ defined by the procedure in Lemma 8.5, where $\theta \in \prod_{j=1}^r S^{2j-1}(\mathbb{R})$ is for each component S^{2j-1} is sampled according to the discrete angle distribution as in Definition 9.19.

Both are just the uniform distribution over $\mathrm{SU}_r(\mathbb{R})$ and $\mathrm{SU}_r(\mathbb{C})$ respectively.

[10] We denote by e^x with a diagonal matrix $x \in \mathrm{GL}_r(K_\mathbb{R})$ the element of $\mathrm{GL}_r(K_\mathbb{R})$ with diagonal $\mathrm{diag}(e^{x_i})_i$, where e^{x_i} is also component-wise over all places of K.

The finite distribution

Definition 9.21 (Discretized angle distribution)**.** For $N \in \mathbb{Z}_{>0}$, we denote

$$\ddot{\Theta}^{(r)} = ([0, 2\pi] \cap \frac{2\pi}{N}\mathbb{Z}) \times ([0, \pi]^{r-1} \cap \frac{\pi}{N}\mathbb{Z}^{r-1})$$

and we define on it a density function $\ddot{\rho}^{(r)}$ by the following procedure:

1. For each $i \in \{1, \ldots, r\}$ do:
2. If $i = 1$, sample $z_1 = \frac{\theta_1}{2\pi}$ from $[0, 1) \cap \frac{1}{N}\mathbb{Z}$ uniformly.
3. If $i > 1$,
4. Sample $z_i = \frac{\theta_i}{\pi}$ from $[0, 1) \cap \frac{1}{N}\mathbb{Z}$ uniformly.
5. Compute $q_i \in \frac{1}{2N^2}\mathbb{Z}$ such that $\frac{1}{2N^2} > q_i - \frac{1}{\sqrt{\pi}}\frac{\Gamma(\frac{i+1}{2})}{\Gamma(\frac{i}{2})} \geq 0$.
6. Sample $u \leftarrow \frac{1}{N^2}\mathbb{Z} \cap [0, q_i]$ uniformly.
7. Compute $\tilde{\rho}_i \in \frac{1}{2N^2}\mathbb{Z}$ such that $-\frac{1}{2N^2} < \tilde{\rho}_i - \rho_i(\pi z_i) \leq 0$
8. If $u < \tilde{\rho}_i$ proceed (accept θ_i), otherwise go to line 4.

Definition 9.22 (Discretized uniform distribution on SU_r)**.** We define the *discretized uniform distribution* on $\mathrm{SU}_r(\mathbb{R})$ by the distribution of $U_\theta \in \mathrm{SU}_r(\mathbb{R})$, the real unitary matrix associated with θ defined by the procedure in Lemma 8.5, where $\theta \in \prod_{j=2}^{r} S^{j-1}(\mathbb{R})$ is for each component S^{j-1} is sampled according to the discrete angle distribution as in Definition 9.21.

Analogously, we define the *discretized uniform distribution* on $\mathrm{SU}_r(\mathbb{C})$ by the distribution of $U_\theta \in \mathrm{SU}_r(\mathbb{C})$, the complex unitary matrix associated with θ defined by the procedure in Lemma 8.5, where $\theta \in \prod_{j=1}^{r} S^{2j-1}(\mathbb{R})$ is for each component S^{2j-1} is sampled according to the discrete angle distribution as in Definition 9.21 (see also Definition 8.6).

Lemma 9.23 (Efficiency of the finite angle distribution)**.** *For $N \geq \pi^3 r^2 + 2$, there exists an algorithm that computes a sample from the discrete angle distribution (Definition 9.21), assuming we can sample perfect bits. This algorithm runs in time* $\mathrm{poly}(\log N, r)$.

Proof. Going over the lines of Definition 9.21, we show that this is an efficient algorithm (without regarding the rejection probability). We finish the proof by showing that the algorithm has only a polynomially small (in r) acceptance probability.

Since sampling uniformly in $[0, 1) \cap \frac{1}{N}\mathbb{Z}$ can be efficiently done in time $\mathrm{poly}(\log N)$, we deduce that lines 1 – 4 can be handled efficiently. In line 5 we approximate $\frac{1}{\sqrt{\pi}}\frac{\Gamma(\frac{i+1}{2})}{\Gamma(\frac{i}{2})}$ within an error of $1/N^2$ which can be done in time $\mathrm{poly}(\log N)$. In line 6, again a uniform sample is drawn, which can be done in time $\mathrm{poly}(\log N)$. In line 7, $\rho_i(\pi z_i)$ is being approximated within an error range of $1/N^2$, which can be done in time $\mathrm{poly}(\log N)$. In line 8 two rationals $u, \tilde{\rho}_i \in \frac{1}{2N^2}\mathbb{Z}$ are compared, which can be done in time $\mathrm{poly}(\log N)$.

For the acceptance probability, we assume that $r > 1$, otherwise the proof is trivial. We compute the acceptance probability in a single loop over i (starting at line 3), we can deduce that it is at least

$$q_i^{-1} \sum_{z_i \in [0,1) \cap \frac{1}{N}\mathbb{Z}} \left(\rho_i(\pi z_i) - \frac{1}{N^2}\right) \geq \frac{1}{\sqrt{r}} \left(\sum_{z_i \in [0,1) \cap \frac{1}{N}\mathbb{Z}} \rho_i(\pi z_i) - \frac{1}{N}\right) \tag{80}$$

since we have $q_i \leq \frac{1}{\sqrt{\pi}}\frac{\Gamma(\frac{i+1}{2})}{\Gamma(\frac{i}{2})} + \frac{1}{2N^2} \leq \sqrt{r}$.

As ρ_j is πr^2-Lipschitz, we can deduce that

$$\begin{aligned}
&\left| \sum_{z_i \in [0,1) \cap \frac{1}{N}\mathbb{Z}} \rho_i(\pi z_i) - \int_{t_i \in [0,\pi]} \rho_i(t_i) dt_i \right| \\
&\leq \int_{t_i \in [0,\frac{\pi}{N}]} \sum_{z_i \in [0,\pi) \cap \frac{\pi}{N}\mathbb{Z}} |\rho_i(z_i + t_i) - \rho_i(z_i)| dt_i \\
&\leq \int_{t_i \in [0,\frac{\pi}{N}]} \sum_{z_i \in [0,\pi) \cap \frac{\pi}{N}\mathbb{Z}} \pi r^2 t_i dt_i = N \pi r^2 \cdot \frac{\pi^2}{2N^2} = \frac{\pi^3 r^2}{2N}.
\end{aligned}$$

Hence, using that $\int_{t_i \in [0,\pi]} \rho_i(t_i) dt_i = 1$ and Equation (80), we obtain a lower bound on the acceptance probability of

$$\frac{1}{\sqrt{r}} \left(1 - \frac{(1 + \pi^3 r^2/2)}{N} \right) \geq \frac{1}{2\sqrt{r}},$$

which is inversely polynomial in r.

Hence, the entire algorithm runs in time $\mathrm{poly}(\log N, r)$. □

9.7.2 The tail error and the discretization error

For this distribution, it is nicer to write $\mathcal{B}_\theta = \mathcal{A}_{U_\theta}$ where U_θ is defined by the procedure in Lemma 8.5.

Recall that $\mathrm{SU}_r(K_\mathbb{R}) \simeq \prod_\nu \mathrm{SU}_r(K_\nu)$ and that an element in $\mathrm{SU}_r(K_\nu)$ can be encoded by a sequence of angles as in

$$\mathrm{Ang}^\nu := \{(\theta_1^{(1)}, (\theta_1^{(2)}, \theta_2^{(2)}), \ldots, (\theta_1^{(k)}, \theta_2^{(k)} \ldots, \theta_k^{(k)}), \ldots, (\theta_1^{(r)}, \ldots, \theta_r^{(r)}))\},$$

where each tuple is distributed as $\rho^{(j)}$ as in Definition 9.19, which yields a distribution $\mathcal{D}_{\mathrm{Ang}^\nu}$ over Ang^ν. The precise sizes of the tuples depend on whether ν is real or complex.

We put $\mathrm{Ang} = \prod_\nu \mathrm{Ang}^\nu$ and $\mathcal{D}_{\mathrm{Ang}}$ as the compound distribution. The discrete distribution $\ddot{\mathcal{D}}_{\mathrm{Ang}}$ is defined as the distribution in which each of the angles in Ang^ν are distributed via the *discrete* angle distribution.

The tail error We choose the tail to be

$$T = \{\theta \in \mathrm{Ang} \mid \text{ there exists } i \text{ such that } \theta_i \leq 2N^{-1/2}\}.$$

By the law of total probability, the fact that Ang has at most $2dr^2$ "angular components" and subsequently by the $2\pi r^2$-Lipschitz constant of the probability distributions $\rho^{(i)}(\theta^{(i)})$, we obtain

$$\begin{aligned}
\mathcal{T}(\mathrm{Ang}) = \int_{\theta \in T} \mathcal{D}_{\mathrm{Ang}}(\theta) d\theta &\leq 2dr^2 \max_{i \in \{1,\ldots,r\}} \int_{\theta^{(i)} \in T^{(i)}} \rho^{(i)}(\theta^{(i)}) d\theta^{(i)} \\
&\leq 2dr^2 (2\pi r^2) \cdot 2N^{-1/2} \leq N^{-1/4} \cdot O(n^5),
\end{aligned} \tag{81}$$

where $T^{(j)} = \{\theta^{(j)} \mid \text{ there exists } i \text{ such that } \theta_i^{(j)} \leq 2N^{-1/2}\}$.

The discretization error

Lemma 9.24. *Writing $\mathcal{D}_{\mathrm{Ang}}$ for the uniform distribution over $\mathrm{SU}_r(K_\mathbb{R})$ and $\ddot{\mathcal{D}}_{\mathrm{Ang}}$ for the discretized version of it (via the angle distributions), we have*

$$\Delta(\mathcal{D}_{\mathrm{Ang}}, \ddot{\mathcal{D}}_{\mathrm{Ang}}) \leq \frac{16\pi^2 dr^4}{N},$$

for $N > 8\pi^2 r^2$.

Proof. Note that, by the triangle inequality, by discretizing the ν-components of $\mathcal{D}_{\mathrm{Ang}}$ (which are $\mathcal{D}_{\mathrm{Ang}^\nu}$) component by component, and subsequently discretizing the components of the distribution over Ang^ν (which are $\rho^{(i)}$ for $i \in \{1, \dots, r\}$) component by component (which is possible by independence), we have

$$\Delta(\mathcal{D}_{\mathrm{Ang}}, \ddot{\mathcal{D}}_{\mathrm{Ang}}) \leq d \cdot \max_\nu \Delta(\mathcal{D}_{\mathrm{Ang}^\nu}, \ddot{\mathcal{D}}_{\mathrm{Ang}^\nu}) \leq d \sum_{i=1}^{r} \Delta(\rho^{(i)}, \ddot{\rho}^{(i)}).$$

The claim follows by Lemma 9.25. Note that in this upper bound we included the tail space T, but since that can only increase the estimate, that does not matter. □

Lemma 9.25. *For any $r_0 \in \mathbb{Z}_{>0}$ and $N > 8\pi^2 r_0^2$, the discretized angle distribution (Definition 9.21) and the angle distribution (Definition 9.19) satisfy the following property:*

$$\Delta(\rho^{(r_0)}, \ddot{\rho}^{(r_0)}) \sum_{\ddot{\theta}^{(r_0)} \in \ddot{\Theta}^{(r_0)}} \int_{\theta^{(r_0)} \in F^{(r_0)}} \left| \rho^{(r_0)}(\theta^{(r_0)}) - \frac{\ddot{\rho}^{(r_0)}(\ddot{\theta}^{(r_0)})}{\mathrm{vol}(F^{(r_0)})} \right| d\theta \leq \frac{16\pi^2 r_0^3}{N}, \tag{82}$$

where $F^{(r_0)} = [0, \frac{2\pi}{N}) \times [0, \frac{\pi}{N})^{r_0 - 1}$.

Proof. From the sample procedure in Definition 9.21 follows that the sampling probabilities of the components $\ddot{\theta}_i^{(r_0)}$ of $\ddot{\theta}^{(r_0)}$ are independent, as well as those of $\theta^{(r_0)}$. We just write the corresponding probability functions with $\ddot{\rho}_i^{(r_0)}$ and $\rho_i^{(r_0)}$. By the trick $ab - a'b' = (a - a')b + (b - b')a'$ (and applying this inductively to $\rho^{(r_0)} = \prod_i \rho_i^{(r_0)}$ and $\ddot{\rho}^{(r_0)} = \prod_i \ddot{\rho}_i^{(r_0)}$) we obtain

$$\sum_{\ddot{\theta}^{(r_0)} \in \ddot{\Theta}^{(r_0)}} \int_{\theta^{(r_0)} \in F^{(r_0)}} \left| \rho^{(r_0)}(\theta^{(r_0)}) - \frac{\ddot{\rho}^{(r_0)}(\ddot{\theta}^{(r_0)})}{\mathrm{vol}(F^{(r_0)})} \right| d\theta \tag{83}$$

$$\leq \sum_{i=1}^{r} \sum_{\ddot{\theta}_i^{(r_0)} \in a_i\pi \cdot ([0,1) \cap \frac{1}{N}\mathbb{Z})} \int_{\theta_i^{(r_0)} \in [0, a_i\pi/N)} \left| \rho_i^{(r_0)}(\theta_i^{(r_0)} + \ddot{\theta}_i^{(r_0)}) - \frac{\ddot{\rho}_i^{(r_0)}(\ddot{\theta}_i^{(r_0)})}{\mathrm{vol}([0, a_i\pi/N))} \right| \tag{84}$$

where $a_i = 2$ if $i = 1$ and $a_i = 1$ otherwise.

Now it is true, by the rejection sampling mechanism of Definition 9.21, that $\ddot{\rho}_i^{(r_0)}(\ddot{\theta}_i^{(r_0)}) \in c_i[\rho_i^{(r_0)}(\ddot{\theta}_i^{(r_0)}) - 2N^{-2}, \rho_i^{(r_0)}(\ddot{\theta}_i^{(r_0)})]$ where $c_i \in \mathbb{R}_{>0}$ is a constant only depending on i, satisfying

$$c_i^{-1} \in [\sum_{\ddot{\theta}_i^{(r_0)}} (\rho_i^{(r_0)}(\ddot{\theta}_i^{(r_0)}) - 2N^{-2}), \sum_{\ddot{\theta}_i^{(r_0)}} \rho_i^{(r_0)}(\ddot{\theta}_i^{(r_0)})] \subseteq [-2N^{-1} + \sum_{\ddot{\theta}_i^{(r_0)}} \rho_i^{(r_0)}(\ddot{\theta}_i^{(r_0)}), \sum_{\ddot{\theta}_i^{(r_0)}} \rho_i^{(r_0)}(\ddot{\theta}_i^{(r_0)})],$$

where $\ddot{\theta}_i^{(r_0)}$ ranges over $a_i\pi \cdot ([0, 1) \cap \frac{1}{N}\mathbb{Z})$ (with $a_i = 2$ if $i = 1$ and $a_i = 1$ otherwise).

Since $\rho_i^{(r_0)}$ is $\pi \cdot r_0^2$-Lipschitz, we can deduce that

$$\left| \int_{\theta_i^{(r_0)}} \rho_i^{(r_0)}(\theta) d\theta - \frac{a_i\pi}{N} \sum_{\ddot{\theta}_i^{(r_0)}} \rho_i^{(r_0)}(\ddot{\theta}_i^{(r_0)}) \right| \leq \sum_{\ddot{\theta}_i^{(r_0)}} \int_{\theta_i^{(r_0)} \in [0, a_i\pi/N)} |\rho_i^{(r_0)}(\ddot{\theta}_i^{(r_0)} + \theta_i^{(r_0)}) - \rho_i^{(r_0)}(\ddot{\theta}_i^{(r_0)})| d\theta_i^{(r_0)}$$

$$\leq \frac{2\pi^2 r_0^2}{N}$$

Hence, since $\int_{\theta_i^{(r_0)}} \rho_i^{(r_0)}(\theta) d\theta = 1$, we thus have

$$c_i^{-1} \in [-2N^{-1} + \sum_{\ddot{\theta}_i^{(r_0)}} \rho_i^{(r_0)}(\ddot{\theta}_i^{(r_0)}), \sum_{\ddot{\theta}_i^{(r_0)}} \rho_i^{(r_0)}(\ddot{\theta}_i^{(r_0)})] = [-2N^{-1} + \frac{N}{a_i\pi} - 2\pi^2 r_0^2, \frac{N}{a_i\pi} + 2\pi^2 r_0^2].$$

Which means that $a_i\pi/(c_iN) \in [-2a_i\pi N^{-2} - 2\pi^2 r_0^2 N^{-1} + 1, 2\pi^2 r_0^2 N^{-1} + 1]$. Choosing $N > 8\pi^2 r_0^2$ we surely have $\frac{c_i N}{a_i \pi} \in [1 - \frac{4\pi^2 r_0^2}{N}, 1 + \frac{4\pi^2 r^2}{N}]$ and therefore,

$$\frac{\ddot{\rho}_i^{(r_0)}(\ddot{\theta}_i^{(r_0)})}{\mathrm{vol}([0, a_i\pi/N))} \in \frac{c_i N}{a_i \pi} \cdot [\rho_i^{(r_0)}(\ddot{\theta}_i^{(r_0)}) - 2N^{-2}, \rho_i^{(r_0)}(\ddot{\theta}_i^{(r_0)})].$$

Thus,

$$\left| \frac{\ddot{\rho}_i^{(r_0)}(\ddot{\theta}_i^{(r_0)})}{\mathrm{vol}([0, a_i\pi/N))} - \rho_i^{(r_0)}(\ddot{\theta}_i^{(r_0)}) \right| \leq \frac{8\pi^2 r_0^2}{N}$$

Using again the Lipschitz constant, we therefore deduce

$$\left| \frac{\ddot{\rho}_i^{(r_0)}(\ddot{\theta}_i^{(r_0)})}{\mathrm{vol}([0, a_i\pi/N))} - \rho_i^{(r_0)}(\theta_i^{(r_0)} + \ddot{\theta}_i^{(r_0)}) \right| \leq \frac{16\pi^2 r_0^2}{N}.$$

Plugging this into Equation (84), we obtain a bound of

$$\sum_{\ddot{\theta}^{(r_0)} \in \ddot{\Theta}^{(r_0)}} \int_{\theta^{(r_0)} \in F^{(r_0)}} \left| \rho^{(r_0)}(\theta^{(r_0)}) - \frac{\ddot{\rho}^{(r_0)}(\ddot{\theta}^{(r_0)})}{\mathrm{vol}(F^{(r_0)})} \right| d\theta \leq \frac{16\pi^2 r_0^3}{N}.$$

□

9.7.3 The continuity error

Lemma 9.26. *Let $\mathcal{A}_\theta$ (for $\theta \in \mathrm{Ang}$) be the output distribution of Algorithm 2 on input $g \cdot U_\theta \cdot g'$ for fixed $g, g' \in \mathrm{GL}_r(K_\mathbb{R})$. Let $N \in \mathbb{Z}_{>0}$ be the discretization parameter.*

Then the continuity error satisfies

$$\mathcal{C}(\ddot{\mathcal{D}}_{\mathrm{Ang}}, \mathcal{A}) \leq N^{-1/4} \cdot O(n^5 \,\mathrm{cd}(g)^{1/2} \cdot \sqrt[4]{\log(1/\varepsilon_0)}).$$

Proof. We have, by Lemma 9.4, writing $\ddot{\mathrm{Ang}}$ for the support of $\ddot{\mathcal{D}}_{\mathrm{Ang}}$,

$$\mathcal{C}(\ddot{\mathcal{D}}_{\mathrm{Ang}}, \mathcal{A}) \leq \max_{\ddot{\theta} \in \ddot{\mathrm{Ang}}} \max_{\theta \in C_{\ddot{\theta}}} \|\mathcal{A}_\theta - \mathcal{A}_{\ddot{\theta}}\|_1.$$

Since we may omit the tail space T, we can assume, by Lemma 9.27, that $\|U_\theta - U_\vartheta\|_2 \leq 2\pi^2 r^3 d \cdot N^{1/2} \|\theta - \vartheta\|$. Since $\|\ddot{\theta} - \theta\| \leq \frac{4\pi}{N}$, we can deduce, by Lemma 3.7, that, writing $L = 92n^3 \sqrt[4]{\log(1/\varepsilon_0)}$,

$$\begin{aligned}
\|\mathcal{A}_\theta - \mathcal{A}_{\ddot{\theta}}\|_1 &\leq L \|g U_\theta g' (g U_{\ddot{\theta}} g')^{-1} - I\|^{1/2} \leq L \cdot \mathrm{cd}(g)^{1/2} \cdot \|U_\theta - U_{\ddot{\theta}}\|^{1/2} \\
&\leq L \cdot \mathrm{cd}(g)^{1/2} \cdot \left(2\pi^2 r^3 d \cdot N^{1/2} \|\theta - \vartheta\|\right)^{1/2} \\
&\leq L \cdot \mathrm{cd}(g)^{1/2} \cdot 2\pi r^{3/2} d^{1/2} N^{1/4} \|\theta - \vartheta\|^{1/2} \\
&\leq N^{-1/4} \cdot O(n^5 \,\mathrm{cd}(g)^{1/2} \cdot \sqrt[4]{\log(1/\varepsilon_0)}).
\end{aligned}$$

□

Lemma 9.27. *Let $\theta = (\theta_1, \ldots, \theta_m) \in \mathrm{Ang}$ satisfy $\theta_i \geq 2 \cdot N^{-1/2}$ for all $i \in \{1, \ldots, m\}$. Then, for any $\vartheta \in \mathrm{Ang}$,*

$$\|U_\theta U_\vartheta^{-1} - I\|_2 = \|U_\theta - U_\vartheta\|_2 \leq 2\pi^2 r^3 d \cdot N^{1/2} \|\theta - \vartheta\|,$$

where U is defined as in Lemma 8.5.

Proof. We prove this first for the space Ang^ν, after which it, by the triangle inequality, can be shown for the whole space Ang as well. We write $\tau = 2N^{-1/2}$.

Write $\mathrm{Ang}^\nu = \Theta^{(r)} \times \cdots \times \Theta^{(1)}$. We have the maps

$$\Theta^{(r)} \times \cdots \times \Theta^{(1)} \xrightarrow{f} S^r \times \cdots \times S^1 \xrightarrow{g} \mathrm{SU}_r(\mathbb{R}),$$

and we write $U_\theta = gf(\theta) \in \mathrm{SU}_r(\mathbb{R})$ for $\theta \in \Theta := \Theta^{(r)} \times \cdots \times \Theta^{(1)}$.

Clearly, $U_\theta = U_{\theta^{(r)}} \cdots U_{\theta^{(1)}}$, where $\theta^{(j)} \in \Theta^{(j)}$, and where $U_{\theta^{(j)}}$ is described by the Householder transformation that sends $y_j := f_j(\theta^{(j)}) \in S^j$ to e_j. This Householder transformation is defined, writing $w = \frac{y_j - e_j}{\|y_j - e_j\|}$ by the rule $U_{\theta^{(j)}} := I - 2ww^\top$.

We have, since $U_\theta, U_\vartheta \in \mathrm{SU}_r(\mathbb{R})$ are unitary, that $\|U_\theta U_\vartheta^{-1} - I\|_2 = \|U_\theta - U_\vartheta\|_2$; indeed,

$$\begin{aligned}\|U_\theta - U_\vartheta\|_2 &= \|(U_\theta U_\vartheta^{-1} - I)U_\vartheta\|_2 \leq \|U_\theta U_\vartheta^{-1} - I\|_2 \|U_\vartheta\|_2 \leq \|U_\theta U_\vartheta^{-1} - I\|_2 \\ &= \|(U_\theta - U_\vartheta)U_\vartheta^{-1}\|_2 \leq \|U_\theta - U_\vartheta\|_2 \|U_\vartheta^{-1}\|_2 = \|U_\theta - U_\vartheta\|_2.\end{aligned}$$

Hence, by repeated application of the trick $ab - a'b' = (a - a')b + (b - b')a'$, and the fact that the two-norm of a unitary matrix equals one, we find,

$$\|U_\theta U_\vartheta^{-1} - I\|_2 = \|U_\theta - U_\vartheta\|_2 = \|U_{\theta^{(r)}} \cdots U_{\theta^{(1)}} - U_{\vartheta^{(r)}} \cdots U_{\vartheta^{(1)}}\|_2 \leq \sum_{j=1}^r \|U_{\theta^{(j)}} - U_{\vartheta^{(j)}}\|_2$$

Now, writing $U_{\theta^{(j)}} = I - 2vv^\top$ and $U_{\vartheta^{(j)}} = I - 2ww^\top$ (with unit vectors $v = \frac{y_j - e_j}{\|y_j - e_j\|}, w = \frac{y'_j - e_j}{\|y'_j - e_j\|}$, with $y_j = f_j(\theta^{(j)})$ and $y'_j = f_j(\vartheta^{(j)})$) we have, using that $\|A^\top\|_2 = \|A\|_2$,

$$\begin{aligned}\|U_{\theta^{(j)}} - U_{\vartheta^{(j)}}\|_2 &= 2\|ww^\top - vv^\top\|_2 = 2\|w(w - v)^\top + [v(w - v)^\top]^\top\|_2 \\ &\leq 2\|w(w - v)^\top\|_2 + 2\|v(w - v)^\top\| \leq 4\|w - v\|.\end{aligned}$$

Assuming that $\|y_j - e_j\| > \tau$ or $\|y'_j - e_j\| > \tau$ and writing $d = y'_j - y_j$, and using the reverse triangle inequality $|\|a\| - \|b\|| \leq \|a - b\|$, we have that

$$\begin{aligned}4\|w - v\| &= 4\left\|\frac{(y_j - e_j)\|y_j - e_j + d\| - (y_j - e_j + d)\|y_j - e_j\|}{\|y_j - e_j\|\|y'_j - e_j\|}\right\| \\ &= 4\frac{\|(y_j - e_j)(\|y_j - e_j + d\| - \|y_j - e_j\|) - d\|y_j - e_j\|\|}{\|y_j - e_j\|\|y'_j - e_j\|} \\ &\leq 4\frac{\|y_j - e_j\|\|d\| + \|d\|\|y_j - e_j\|}{\|y_j - e_j\|\|y'_j - e_j\|} \leq 4\frac{\|y_j - y'_j\|}{\|y'_j - e_j\|} \leq 4\tau^{-1}\|y_j - y'_j\|.\end{aligned}$$

Since this inequality is symmetric in y_j and y'_j, we can just assume $\|y_j - e_j\| > \tau$. Since the function $y_j = f_j(\theta^{(j)})$ is $\pi^2 r^2$-Lipschitz, we immediately deduce,

$$\|U_{\theta^{(j)}} - U_{\vartheta^{(j)}}\|_2 \leq 4\tau^{-1}\|y_j - y'_j\| \leq \frac{4\pi^2 r^2}{\tau}\|\theta^{(j)} - \vartheta^{(j)}\|,$$

provided that $y_j = f_j(\theta^{(j)})$ satisfies $\|y_j - e_j\| > \tau$. Note that, for the map $f_j : \Theta^{(j)} \to S^j$, we have $x_j = f_j(\theta_j^{(j)}) = \cos(\theta_j^{(j)})$; hence, for sure, if $\theta_j^{(j)} > 2\sqrt{\tau}$, we have $\|y_j - e_j\| > 1 - \cos(2\sqrt{\tau}) > \tau$ for $\tau < 1$.

So,

$$\|U_\theta U_\vartheta^{-1} - I\|_2 = \|U_\theta - U_\vartheta\|_2 \leq \frac{4\pi^2 r^3}{\tau}\|\theta - \vartheta\|,$$

for $\theta = (\theta^{(r)}, \ldots, \theta^{(1)})$ with $\theta_j^{(j)} > 2\sqrt{\tau}$ for all $j \in \{1, \ldots, r\}$.

For general $\theta \in \mathrm{Ang}$ (instead of just Ang^ν) we arrive at the similar claim, but with an additional factor d, which finishes the proof. □

9.7.4 Run time

Lemma 9.28. *There exists an algorithm sampling from* $\ddot{\text{Ang}}$ *within time* $\text{poly}(\log N, dr)$.

Proof. By Lemma 9.23 one can sample a single angle component (note that the components are independent) from $\ddot{\text{Ang}}$ within polynomial time in $\log N$ and r. Hence, since Ang has at most $2dr^2$ angular components, we obtain at the claim of this lemma. □

9.7.5 Concluding all errors

Lemma 9.29. *Let* $\mathcal{A}_\theta$ *(for* $\theta \in \text{Ang}$*) be the output distribution of Algorithm 2 on input* $g \cdot U_\theta \cdot g'$ *for fixed* $g, g' \in \text{GL}_r(K_\mathbb{R})$*. Let* $N \in \mathbb{Z}_{>0}$ *be the discretization parameter satisfying* $N \geq 8\pi^2 r^2 + 2$ *Then,*

$$\| \mathop{\mathbb{E}}_{x \leftarrow \mathcal{D}_{\text{Ang}}} [\mathcal{A}_x] - \mathop{\mathbb{E}}_{\ddot{x} \leftarrow \ddot{\mathcal{D}}_{\text{Ang}}} [\mathcal{A}_{\ddot{x}}] \| \leq N^{-1/4} n^5 O(\text{cd}(g)^{1/2} \cdot \sqrt[4]{\log(1/\varepsilon_0)}).$$

Proof. This follows from Equation (81) and lemmas 9.24 and 9.26 and simplifying the expression. □

10 Conclusion

We finally piece together all ingredients and prove Theorem 1, our main theorem on the worst-case to average-case reduction of SIVP.

Recall from Section 2.3.2 the invariant measure μ on the space $X_r = X_r(K)$ of module lattices of rank r over the number field K. Recalling the definition of $\text{Round}_{\text{Lat}}$ from Section 3, define the average-case distribution as

$$\mathcal{D} = \text{Round}_{\text{Lat}}(\mu_{\text{cut}})$$

where μ_{cut} is the Haar-measure induced distribution on X_r, restricted (hence the name "cut") to module lattices that are α-balanced, with $\alpha = O(B \cdot d \cdot c_K) = \exp(O(d \log d + \log|\Delta_K|))$, where B is as in line 1 in Algorithm 5 and where $c_K = 1 + \frac{\Gamma_K \sqrt{r \cdot d}}{2}$ with $\Gamma_K \leq |\Delta_K|^{1/d}$.

Note that, by Theorem 4, the distributions μ and μ_{cut} are close in statistical distance, and that (by Proposition 3.1) $\text{Round}_{\text{Lat}}$ rounds its input lattice to a very close lattice. This gives a justification as to why $\text{Round}_{\text{Lat}}(\mu_{\text{cut}})$ can be seen as a sound discrete average-case distribution.

Proof of Theorem 1. By Theorem 7, it is sufficient to reduce γ-SIVP for $(4d \cdot c_K)$-balanced lattices to γ'-SIVP for lattices sampled from $\mathcal{D}$. We use here that $c_K^{r-1} \cdot (1 + d/2^{(rd+1)/2})^{r-1}$ from Theorem 7 is $\text{poly}_r(|\Delta_K|^{1/d}, d)$, since $\Gamma_K \leq |\Delta_K|^{1/d}$ (see Lemma 2.12).

Given a $(4d \cdot c_K)$-balanced module lattice L_0, we randomize it using the framework from Section 4, but with discretized underlying distributions, as in Section 9. After that, we apply $\text{Round}_{\text{Lat}}$ (from Proposition 3.1) and feed the randomized and rounded module lattice to the oracle solving γ'-SIVP for $\text{Round}_{\text{Lat}}(\mu_{\text{cut}})$. This yields an output for SIVP for this rounded and randomized module lattice. By undoing the "rounding" and the "randomization", we get an SIVP solution for the original lattice L_0. This process is described in a precise manner in Algorithm 5.

For this reduction in Algorithm 5 to be sound, we need to prove three things. One, we need to show that the distribution of L_3 in line 6 is statistically $o(p)$-close to $\text{Round}_{\text{Lat}}(\mu_{\text{cut}})$ in order for the oracle in line 7 to succeed with probability $\Omega(p)$. Two, we need to upper bound the loss in quality of the output SIVP solution caused by the randomization (and de-randomization). Three, we need to bound the expected number of queries to the oracle, and show that every step can be performed in polynomial time in the size of the input (where we assume $r = O(1)$).

Algorithm 5 Reducing a fixed $(4d \cdot c_K)$-balanced instance of SIVP over module lattices to a random instance of SIVP over module lattices.

Require:
- A pseudo-basis $(\mathbf{B}, \mathbf{I})$ of a rank r module lattice L_0,
- An oracle $\mathcal{O}$ solving γ'-SIVP for $\mathrm{Round}_{\mathrm{Lat}}(\mu_{\mathrm{cut}})$ with probability $p = 2^{-o(n)}$.

Ensure: With probability $1-2^{-\Omega(n)}$, a solution to γ-SIVP for L_0, with $\gamma = \mathrm{poly}_r(|\Delta_K|^{1/d}, d)\cdot\gamma'$

1: Put $B = \exp\left(C_r(d\log d + \log|\Delta_K|)\right)$ for a large enough constant $C_r > 0$ depending on r, $t = 1$ and $\sigma = 1/d^2$.
2: Instantiate the discretization parameter N as in Equation (54):

$$\log(N) = O(n^2\log n + n\cdot \mathrm{size}(\mathbf{B}) + n^2\cdot\log(B) + n\log|\Delta_K| + \log(1/\varepsilon_0) + \log(1/\varepsilon)).$$

3: **repeat**
4: Compute a module lattice $L_1 = g\cdot L_0$ using Algorithm 4 on input L_0 with parameters t and σ as above, and where every distribution occurring is discretized as in Section 9 with discretization parameter N, with $\varepsilon_0 := 2^{-\Theta(n)}$ and $\varepsilon = 2^{-\Theta(n)}$ as in Proposition 9.1.
5: Sample uniformly random $\mathfrak{p}$ from the set $\mathcal{P}$ of all prime ideals with norm at most B (using [BDP+20, Lemma 2.2]) and take a random sublattice L_2 of L_1 satisfying $L_2/L_1 \cong \mathcal{O}_K/\mathfrak{p}$ using Algorithm 1.
6: Sample $L_3 \leftarrow \mathrm{Round}_{\mathrm{Lat}}(L_2)$, where $\mathrm{Round}_{\mathrm{Lat}}$ is the algorithm given in Proposition 3.1, with error parameter ε_0 as above and balancedness parameter $\alpha = O(Bdc_K)$.
7: Apply the oracle $\mathcal{O}$ on L_3.
8: **until** the output of $\mathcal{O}$ is of the form $\{v_1^{(3)},\dots,v_n^{(3)}\}$ and satisfies $\|v_j^{(3)}\| \le \gamma'\cdot O(n\cdot|\Delta_K|^{\frac{1}{2d}})\cdot \det(L_3)^{\frac{1}{n}}$ for all j.
9: Use the transformation Y of Proposition 3.1(iii) to compute $v_j^{(2)} := Y\cdot v_j^{(3)}$ for all j.
10: Put $v_j^{(1)} := v_j^{(2)} \in L_2 \subseteq L_1$ for all j.
11: Put $v_j^{(0)} := g^{-1}v_j^{(1)}$ for all j, to get $\{v_1^{(0)},\dots,v_n^{(0)}\} \subset L_0$ with g as in Line 4.
12: **return** $(v_1^{(0)},\dots,v_r^{(0)})$.

(1) Statistical closeness. Because the final oracle solving the random instance has success probability at least $2^{-o(n)}$, it suffices to allow a statistical error of $2^{-\Omega(n)}$. In this proof, we will instantiate with parameters aiming for a statistical error of $2^{-\Theta(n)} = 2^{-\Theta(d)}$ as $r = O(1)$. Note that most of the ingredients of the proof can handle arbitrary errors $\varepsilon > 0$, consuming additional time $\log(1/\varepsilon)$.

Let $z = (\mathbf{B}, \mathbf{I})$ be the input pseudo-basis for L_0, and we use the notation f_z, φ_z and $\mathcal{D}_z$ as in Section 9 (see the discussion before Proposition 9.1).

Note that, by construction, L_3 in line 6 is distributed according to $\mathrm{Round}_{\mathrm{Lat}}(T_{\mathcal{P}}(\mathcal{D}_z))$. Our strategy is to bound the distance $\|\mathrm{Round}_{\mathrm{Lat}}(T_{\mathcal{P}}(\mathcal{D}_z)) - \mathrm{Round}_{\mathrm{Lat}}(T_{\mathcal{P}}(\varphi_z))\|_1$, as well as $\|T_{\mathcal{P}}\varphi_z - \mu\|_1$ and $\|\mu - \mu_{\mathrm{cut}}\|_1$ by $2^{-\Omega(n)}$. Assuming this, by the data processing inequality (Proposition 2.22) applied to $\mathrm{Round}_{\mathrm{Lat}}$ and the triangle inequality, this reasonably yields

$$\|\mathrm{Round}_{\mathrm{Lat}}(T_{\mathcal{P}}(\mathcal{D}_z)) - \mathrm{Round}_{\mathrm{Lat}}(\mu_{\mathrm{cut}})\|_1 \le 2^{-\Omega(n)}.$$

First, $\|\mathrm{Round}_{\mathrm{Lat}}(T_{\mathcal{P}}(\mathcal{D}_z)) - \mathrm{Round}_{\mathrm{Lat}}(T_{\mathcal{P}}(\varphi_z))\|_1$ is bounded by $\varepsilon_0 + \varepsilon = 2^{-\Omega(n)}$, by Proposition 9.1 and our choices of ε_0 and ε in the algorithm. Next, $\|\mu - \mu_{\mathrm{cut}}\|_1$ satisfies the same bound by Theorem 4. Indeed, a μ-random module lattice L satisfies

$$\lambda_r^K(L)/\lambda_1^K(L) \le \lambda_n(L)/\lambda_1(L) \ll n|\Delta_K|^{1/d}$$

with probability at least $1 - 2^{\Omega(n\log r)}$, and on the other hand $\alpha = \Omega(n\cdot|\Delta_K|^{1/d})$.

Next, we bound the statistical distance between $T_{\mathcal{P}}\varphi_z\mu_{\mathrm{Riem}}$ and μ, which is

$$\frac{1}{2}\int_{X_r}|T_{\mathcal{P}}\varphi_z\cdot\mu_{\mathrm{Riem}}(X_r)-1|\,d\mu=\frac{1}{2}\left\|T_{\mathcal{P}}\varphi_z-\mu_{\mathrm{Riem}}(X_r)^{-1}\mathbf{1}_{X_r}\right\|_1,$$

where the L^1-norm is now with respect to μ_{Riem}. Applying Cauchy–Schwarz, we have

$$\begin{aligned}\left\|T_{\mathcal{P}}\varphi_z-\mu_{\mathrm{Riem}}(X_r)^{-1}\mathbf{1}_{X_r}\right\|_1&\le\sqrt{\mu_{\mathrm{Riem}}(X_r)}\cdot\left\|T_{\mathcal{P}}\varphi_z-\mu_{\mathrm{Riem}}(X_r)^{-1}\mathbf{1}_{X_r}\right\|_2\\&\le\exp(C(d+\log|\Delta_K|))\left\|T_{\mathcal{P}}\varphi_z-\mu_{\mathrm{Riem}}(X_r)^{-1}\mathbf{1}_{X_r}\right\|_2,\end{aligned}\tag{85}$$

for some constant $C>0$ depending on r, using Lemma 2.37.

To finally apply Theorem 3, we rework its statement using the assumption that $r=O(1)$ and using that $\log x=O(x^\delta)$ for any $\delta>0$. Let $\kappa_d=\kappa\sigma=\kappa/d^2$ to simplify notation and note that $\kappa\ge\sqrt{d}/\sigma=d^{5/2}$ in the theorem (we make a valid choice of κ below), so that $\kappa_d\ge\sqrt{d}\gg1$. For the first term, we trivially bound $r_u\le d$ and $r_u(\log r_u)^3=o(d^2)$, so we may assume that $\max(r_u(\log r_u)^3,1/\sigma)=1/\sigma=d^2$. We also bound

$$C_1\ll B^{-1/4}(d\log\kappa_d+\log|\Delta_K|).$$

For the second, denote by $\alpha(z)$ the balancedness of L_0. Thus, $\alpha(z)\ll dc_K\ll d^{3/2}|\Delta_K|^{1/d}$ (using Lemma 2.12 again), so that

$$C_2\le\exp(O(d\log d+\log|\Delta_K|)).$$

Let

$$\kappa_d^2=\kappa^2/d=\max\left(d^{5/2},C(d+\log|\Delta_K|)+d\log d+d\right).$$

Since κ_d is polynomial in d and $\log|\Delta_K|$, we have that $d\log\kappa_d+\log|\Delta_K|=O(d\log d+\log|\Delta_K|)$. All in all, applying again some trivial bounds to simplify expressions, we have

$$\left\|T_{\mathcal{P}}\varphi_z-\mu_{\mathrm{Riem}}(X_r)^{-1}\mathbf{1}_{X_r}\right\|_2^2\ll\exp(2d\log d-2\kappa_d^2)+B^{-1/2}\exp(C'\cdot(d\log d+\log|\Delta_K|))$$

for some constant $C'>0$ depending on r.

We plug this last bound into (85) and use simplifying bounds as above, such as $\log x\le x$, and that $\sqrt{x+y}\le\sqrt{x}+\sqrt{y}$ for $x,y>0$ to arrive at

$$\left\|T_{\mathcal{P}}\varphi_z-\mu_{\mathrm{Riem}}(X_r)^{-1}\mathbf{1}_{X_r}\right\|_1\ll e^{-d}=2^{-\Omega(n)}.$$

We use here that our choice of κ_d implies that

$$\exp(C(d+\log|\Delta_K|))\cdot\exp(d\log d-\kappa_d^2)\le e^{-d}$$

and that

$$B^{1/4}\ge\exp\left(C'(d\log d+\log|\Delta_K|)/2+C(d+\log|\Delta_K|)+d\right).$$

This is possible with a minimal

$$B=\exp\left(O_r(d\log d+\log|\Delta_K|)\right),$$

where the implied constant depends on r.

(2) Bound on the loss in SIVP-quality. The processing of the SIVP-vectors happens in lines 8, 9, 10 and 11.

We prove in part (1) of this proof that L_3 follows a distribution that is $2^{-\Omega(n)}$-close to $\mathrm{Round}_{\mathrm{Lat}}(\mu_{\mathrm{cut}})$. Since module lattices L sampled from μ satisfy $\lambda_n(L) \le O(n|\Delta_K|^{\frac{1}{2d}}) \cdot \det(L)^{\frac{1}{n}}$ by Theorem 4 with probability at least $1 - 2^{-\Omega(n \log r)}$, surely module lattices L sampled from μ_{cut} satisfy the same inequality (even with a higher probability).

So, with probability $1 - 2^{-\Omega(n \log r)}$, we have that $\det(L_3)^{\frac{1}{n}} \le \lambda_n(L_3) \le O(n \cdot |\Delta_K|^{\frac{1}{2n}}) \cdot \det(L_3)^{\frac{1}{n}}$, and hence line 8 suffices to check whether the oracle is successful, though it might allow for an extra slack of $O(n \cdot |\Delta_K|^{\frac{1}{2n}}) = \mathrm{poly}_r(d, |\Delta_K|^{1/d})$, which is acceptable for our use-case. Therefore, since $p = 2^{-o(n)}$, we may assume with probability $1 - 2^{-\Omega(n)}$ that after line 8, the solution $\{v_1^{(3)}, \dots, v_n^{(3)}\}$ satisfies $\|v_j^{(3)}\| \le \gamma' \cdot \mathrm{poly}(d, |\Delta_K|^{1/d}) \cdot \lambda_n(L_3)$. Additionally, we can assume that $\lambda_n(L_3) \le O(n|\Delta_K|^{\frac{1}{2d}}) \cdot \det(L_3)^{\frac{1}{n}}$.

By Proposition 3.1(iii), we see that $\det(L_3)^{\frac{1}{n}} \le 2 \det(L_2)^{\frac{1}{n}}$ and that applying Y only changes vector lengths by a factor $O(1)$. Therefore, $\{v_1^{(1)}, \dots, v_n^{(1)}\}$ satisfy, for all $j \in \{1, \dots, n\}$,

$$\begin{aligned}\|v_j^{(1)}\| &\le O(n|\Delta_K|^{\frac{1}{2d}}) \cdot \gamma' \cdot \det(L_3)^{\frac{1}{n}} \le O(n|\Delta_K|^{\frac{1}{2d}}) \cdot \gamma' \cdot \det(L_2)^{\frac{1}{n}} \\ &\le O(n|\Delta_K|^{\frac{1}{2d}}) \cdot B^{1/n} \cdot \gamma' \cdot \det(L_1)^{\frac{1}{n}} \\ &\le \mathrm{poly}_r(d, |\Delta_K|^{\frac{1}{d}}) \cdot \gamma' \cdot \det(L_1)^{\frac{1}{n}}\end{aligned}$$

where the last inequality holds by our choice of B in line 1 of Algorithm 5. Since g has conditioning number $e^{2n^2\sigma+2t}$ (see the proof of Proposition 9.1), by the very same arguments as those of Proposition 3.1(iii), multiplying by g^{-1} changes the determinant and the lengths of vectors by at most $O(1)$. Hence, we have, for all $j \in \{1, \dots, n\}$,

$$\|v_j^{(0)}\| \le \mathrm{poly}_r(d, |\Delta_K|^{\frac{1}{d}}) \cdot \gamma' \cdot \det(L_0)^{\frac{1}{n}} \le \mathrm{poly}_r(d, |\Delta_K|^{\frac{1}{d}}) \cdot \gamma' \cdot \lambda_n(L_0),$$

where the last inequality holds by the fact that $\det(L_0)^{1/n} \le (\prod_{j=1}^n \lambda_j(L_0))^{1/n} \le \lambda_n(L_0)$. So, indeed, the algorithm solves γ-SIVP for L_0 with $\gamma = \mathrm{poly}_r(d, |\Delta_K|^{\frac{1}{d}}) \cdot \gamma'$.

(3) Number of queries and efficiency. Line 4 uses Algorithm 4 with discretization, which can be computed efficiently according to Proposition 3.1. Line 5 uses the algorithm described in [BDP+20, Lemma 2.2] as well as Algorithm 1, which run both within polynomial time in the size of their input (Lemma 2.5). Line 6 uses Algorithm 2, which runs within polynomial in the size of the input. But for this algorithm to be applicable on L_2, we need to show that L_2 is α-balanced for $\alpha = O(B \cdot d \cdot c_K)$. By similar arguments as earlier in the proof, g does not change lengths of vectors much, and hence, since L_0 is $(4d \cdot c_K)$-balanced, we can conclude that L_1 is $O(d \cdot c_K)$-balanced. As L_2 is a sub-lattice of L_1 of index at most $2B$, we deduce, by Lemma 2.15, that L_2 is $O(B \cdot d \cdot c_K)$-balanced, which is what was required to show. Since lines 9, 10 and 11 are mere linear operations applied to vectors, these lines all run in polynomial time in the size of the input.

For the expected number of queries, note that the distribution of L_3 is $o(p)$-statistically close to $\mathrm{Round}_{\mathrm{Lat}}(\mu_{\mathrm{cut}})$, hence we may assume that the oracle $\mathcal{O}$ gives a sound output with probability $O(p)$. So the expected number of queries is $O(p^{-1})$. For the total reduction (which includes the cusp and the flare part) the number of queries is multiplicatively increased by $\mathrm{poly}_r(\log |\Delta_K|)$, which yields the total expected number of queries. □

A Appendix

The lemmas in Appendices A.1 to A.3 are almost literally from [BPW25], and are stated here for sake of self-containedness.

A.1 On the matrix norm of an inverse basis

Lemma A.1. *Suppose* $\mathbf{B} = (\mathbf{a}_1, \ldots, \mathbf{a}_n) \in \mathbb{R}^{n \times n}$ *is a square real matrix and a basis of a lattice* $L \subset \mathbb{R}^n$*. Then*

$$\|\mathbf{B}^{-1}\|_2 \leq n^{n/2+1} \cdot \lambda_1(L)^{-1} \cdot \left(\prod_{j=1}^{n} \frac{\|\mathbf{b}_j\|}{\lambda_j(L)} \right),$$

where $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$*.*

Proof. For $j \in \{1, \ldots, n\}$, put $C_j = \frac{\|\mathbf{b}_j\|}{\lambda_j(\Lambda)} \geq 1$. We have that $\mathbf{B}^{-1} = \frac{1}{\det \mathbf{B}} \mathrm{adj}(\mathbf{B})$. Also, $\mathrm{adj}(\mathbf{B})_{ij}$ is defined by the determinant of the minor of $\mathbf{B}$ where the i-th row and j-th column are deleted. By the Hadamard bound and subsequently by Minkowski's second theorem (see, e.g., [MG02, Theorem 1.5]),

$$\begin{aligned} |\mathrm{adj}(\mathbf{B})_{ij}| &\leq \prod_{k \neq i} \|\mathbf{b}_k\| = \prod_{k \neq i} C_k \cdot \lambda_k(L) \\ &\leq n^{n/2} \cdot (\prod_{k \neq i} C_k) \cdot \det(L)/\lambda_i(L) \leq n^{n/2} (\prod_{k=1}^{n} C_k) \cdot \det(L)/\lambda_1(L). \end{aligned}$$

Observing that $\det(\mathbf{B}) = \det(\Lambda)$, we obtain

$$\|\mathbf{B}^{-1}\|_2 \leq \|\mathbf{B}^{-1}\|_F \leq \frac{1}{\det(\mathbf{B})} \cdot n \cdot \max_{ij} |\mathrm{adj}(\mathbf{B})_{ij}| \leq n^{n/2+1} \cdot (\prod_{k=1}^{n} C_k)/\lambda_1(L).$$

□

A.2 On the weight of discrete Gaussians on strict sublattices

We show in the following two lemmas that the discrete Gaussian distribution over a lattice with an arbitrary center point has no heavy weight on any strict sublattice. This fact is used that we can compute a sample from a discrete Gaussian conditioned on the event that it is linearly independent to earlier samples.

Lemma A.2. *Writing* $\rho_\sigma(x) := e^{-\pi \|x\|^2/\sigma^2}$*, we have that for any lattice* $\Lambda \subseteq V$ *(where* V *is a Euclidean space), any* $\sigma > 0$ *and any* $t, w \in V$*, we have*

$$\rho_\sigma(\Lambda + t + w) + \rho_\sigma(\Lambda + t - w) \geq 2\rho_\sigma(w)\rho_\sigma(\Lambda + t),$$

where $\rho_\sigma(\Lambda + t) = \sum_{\ell \in \Lambda} \rho_\sigma(\ell + t)$*.*

Proof. This lemma is a simple generalization of [HR14, Claim 2.10], and we follow the same strategy:

$$\begin{aligned} \rho_\sigma(\Lambda + t + w) + \rho_\sigma(\Lambda + t - w) &= \sum_{x \in \Lambda + t} \left(e^{-\pi \|x+w\|^2/\sigma^2} + e^{-\pi \|x-w\|^2/\sigma^2} \right) \\ &= 2e^{-\pi \|w\|^2/\sigma^2} \sum_{x \in \Lambda + t} \left(e^{-\pi \|x\|^2/\sigma^2} \cosh(2\pi \langle x, w \rangle/\sigma^2) \right) \\ &\geq 2\rho_\sigma(w)\rho_\sigma(\Lambda + t), \end{aligned}$$

where the last inequality follows from $\cosh(\alpha) \geq 1$ for any real α. □

Lemma A.3. *Let* $\Lambda \subseteq V$ *be a lattice and* V *an Euclidean space,* $t \in V$ *and* $\sigma > c \cdot \sqrt{n} \cdot \lambda_n(\Lambda)$ *for some* $c > 0$*. Then, for any strict sublattice* $\Lambda' \subsetneq \Lambda$

$$\Pr_{x \leftarrow \mathcal{G}_{\Lambda+t,\sigma}} [x \in \Lambda' + t] = \frac{\rho_\sigma(\Lambda' + t)}{\rho_\sigma(\Lambda + t)} \leq \frac{1}{1 + e^{-\pi c^{-2}}}.$$

Proof. Let $\Lambda' \subsetneq \Lambda$ be a sub-lattice of Λ and let $w \in \Lambda \setminus \Lambda'$. Then, by Lemma A.2,

$$\begin{aligned}\rho_\sigma(\Lambda + t) &\geq \rho_\sigma(\Lambda' + t) + \frac{\rho_\sigma(\Lambda' + t + w) + \rho_\sigma(\Lambda' + t - w)}{2} \\ &\geq (1 + \rho_\sigma(w))\rho_\sigma(\Lambda' + t).\end{aligned}$$

Writing $\mathcal{G}_{\Lambda+t,\sigma}$ for the Gaussian distribution on $\Lambda + t$ with parameter σ, we have,

$$\Pr_{x \leftarrow \mathcal{G}_{\Lambda+t,\sigma}}[x \in \Lambda' + t] = \frac{\rho_\sigma(\Lambda' + t)}{\rho_\sigma(\Lambda + t)} \leq \frac{1}{1 + \rho_\sigma(w)}.$$

Note that the set $\{\ell \in \Lambda \mid \|\ell\| \leq \sqrt{n}\lambda_n(\Lambda)\}$ contains a HKZ-basis of Λ [LLS90]. Hence, for any $\Lambda' \subsetneq \Lambda$ there must exist $w \in \Lambda \setminus \Lambda'$ with $\|w\| \leq \sqrt{n}\lambda_n(\Lambda)$.

So there exists $w \in \Lambda \setminus \Lambda'$ such that $\|w\| \leq \sqrt{n} \cdot \lambda_n(\Lambda) < \sigma/c$, hence $\rho_\sigma(w) \geq \exp\left(-\pi c^{-2}\right)$, proving the lemma. □

A.3 On the number of lattice points in a convex measurable volume

Lemma A.7, which shares some similarities with [PP21, §4.2], provides means to estimate the number of lattice elements in a convex measurable volume. This estimate is essential in Section 9 about discretization. To prepare for the proof of this lemma, we will need some facts on Minkowski sums of sets.

Definition A.4. Let V be a Euclidean vector space. For two sets $X, Y \subseteq V$, we define the Minkowski sum $X \boxplus Y$ as follows.

$$X \boxplus Y = \{\mathbf{x} + \mathbf{y} \mid \mathbf{x} \in X, \mathbf{y} \in Y\}.$$

For $c \in \mathbb{R}_{>0}$ we denote by cX the set

$$cX = \{c \cdot \mathbf{x} \mid \mathbf{x} \in X\}.$$

Lemma A.5. *Let V be a Euclidean vector space and let $r, s > 0$ and let $X \subseteq V$ be a convex volume. Then*

$$(rX) \boxplus (sX) = (r + s)X.$$

Proof. We start with inclusion to the right. Suppose $\mathbf{y} \in (rX) \boxplus (sX)$, i.e., $\mathbf{y} = r\mathbf{x} + s\mathbf{x}'$ where $\mathbf{x}, \mathbf{x}' \in X$. Then $\frac{\mathbf{y}}{r+s} = \frac{r\mathbf{x}+s\mathbf{x}'}{r+s} \in X$, since it is a weighted average of two points in X and X is convex. So $\mathbf{y} \in (r + s)X$. Inclusion to the left holds because $\mathbf{y} \in (r + s)X$ means that $\mathbf{y} = (r + s)\mathbf{x} = r\mathbf{x} + s\mathbf{x} \in (rX) \boxplus (sX)$. □

Lemma A.6. *Let V be a Euclidean vector space, let $r > 0$, let $X, Y \subseteq V$ be sets and let $S \subseteq V$ be a symmetric set, i.e., $\mathbf{x} \in S \Leftrightarrow -\mathbf{x} \in S$. Then*

$$(X \boxplus S) \cap Y \subseteq [X \cap (Y \boxplus S)] \boxplus S.$$

Proof. Suppose $\mathbf{x} + \mathbf{s} = \mathbf{y} \in (X \boxplus S) \cap Y$. Then $\mathbf{x} = \mathbf{y} - \mathbf{s} \in X \cap (Y \boxplus S)$, so $\mathbf{y} = \mathbf{x} + \mathbf{s} \in [X \cap (Y \boxplus S)] \boxplus S$. □

Lemma A.7. *Let V be a n-dimensional Euclidean vector space, let $\Lambda \subseteq V$ be a full-rank lattice, let $X \subseteq V$ be a convex measurable volume for which $\mathcal{V}_0 \subseteq cX$ for some $c \in \mathbb{R}_{>0}$, where $\mathcal{V}_0$ is the (origin-centered) Voronoi cell of Λ. Then, for all $\mathbf{t}, \mathbf{t}' \in V$ and all $q > 2c$,*

$$|(\Lambda + \mathbf{t}) \cap q(X + \mathbf{t}')| \in [e^{-2nc/q}, e^{2nc/q}] \cdot \frac{q^n \cdot \mathrm{vol}(X)}{\det(\Lambda)},$$

where $q(X + \mathbf{t}') = \{q \cdot (x + \mathbf{t}') \mid x \in X\}$ is the scaling of the (translated) set $X + \mathbf{t}'$ by $q \in \mathbb{R}_{>0}$.

Proof. As $|(\Lambda+\mathbf{t})\cap(qX+q\mathbf{t}')| = |(\Lambda+\mathbf{t}-q\mathbf{t}')\cap qX|$, we just assume, without loss of generality, that $\mathbf{t}' = 0$. Note that $\mathcal{V}_0 \subseteq cX$, and that X is convex. So, by Lemma A.5, we have $(qX)\boxplus\mathcal{V}_0 \subseteq (qX)\boxplus(cX) = (q+c)X$. Similarly, $(q-c)X\boxplus\mathcal{V}_0 \subseteq qX$. Therefore

$$[(\Lambda+\mathbf{t})\cap qX]\boxplus\mathcal{V}_0 \subseteq (q+c)X. \tag{86}$$

Note that $\mathcal{V}_0$ is symmetric and $(\Lambda+\mathbf{t})\boxplus\mathcal{V}_0 = V$, the whole vector space. So, by Lemma A.6 and $(q-c)X\boxplus\mathcal{V}_0 \subseteq qX$,

$$(q-c)X = [(\Lambda+\mathbf{t})\boxplus\mathcal{V}_0]\cap(q-c)X \tag{87}$$
$$\subseteq [(\Lambda+\mathbf{t})\cap((q-c)X\boxplus\mathcal{V}_0)]\boxplus\mathcal{V}_0 \subseteq [(\Lambda+\mathbf{t})\cap qX]\boxplus\mathcal{V}_0 \tag{88}$$

By Equations (86) and (88) and the fact that $\mathcal{V}_0$ is a fundamental domain of Λ with volume $\det(\Lambda)$, we obtain

$$(q-c)^n\operatorname{vol}(X) \le |(\Lambda+\mathbf{t})\cap qX|\cdot\det(\Lambda) \le (q+c)^n\operatorname{vol}(X).$$

Dividing by $\det(\Lambda)$ and using the estimate $e^{-2nc/q} \le (1-c/q)^n \le (1+c/q)^n \le e^{2nc/q}$ (note that $q > 2c$) we arrive at the final claim. □

A.4 Gaussian tails

Lemma A.8. *Let V be a real vector space of dimension n and $s > 0$. For any $\varepsilon \in (0,1]$, it holds that $\Pr_{x\leftarrow\mathcal{G}_{V,s}}(\|x\| \ge s\cdot\sqrt{2n\cdot\log(2n/\varepsilon)}) \le \varepsilon$.*

Proof. Let B be an orthonormal basis of V and write $x = (x_1,\cdots,x_n)$ the coordinates of x in this basis. Then the random variables x_i are linearly independent Gaussian distributions over $\mathbb{R}$ with standard deviation s. Moreover, for any $t > 0$, if $\|x\| \ge t$, there should exist some i such that $|x_i| \ge t/\sqrt{n}$. Hence, we obtain

$$\Pr_{x\leftarrow\mathcal{G}_{V,s}}(\|x\| \ge t) \le n\cdot\Pr_{x\leftarrow\mathcal{G}_{\mathbb{R},s}}(|x| \ge t/\sqrt{n}) \le 2n\cdot\exp\Big(-\frac{t^2}{2n\cdot s^2}\Big),$$

where the first inequality comes from the union bound and the last one comes from Chernoff's bound. Taking $t = s\cdot\sqrt{2n\cdot\log(2n/\varepsilon)}$ leads to the desired result. □

A.5 Sizes of elements

Lemma A.9 (Rules on sizes of elements)**.**

1. *For $m_j \in \mathbb{Z}$, $\operatorname{size}(\prod_{j=1}^k m_j) \le \sum_{j=1}^k \operatorname{size}(m_j)$ and $\operatorname{size}(\sum_{j=1}^k m_j) \le \log_2(k)+\max_j(\operatorname{size}(m_j))$.*
2. *For $q_i \in \mathbb{Q}$, $\operatorname{size}(\prod_{i=1}^k q_i) \le \sum_{i=1}^k \operatorname{size}(q_i)$ and $\operatorname{size}(\sum_{i=1}^k q_i) \le 3\sum_{j=1}^k \operatorname{size}(q_j)$.*
3. *For $\gamma_j \in K$, we have $\operatorname{size}(\sum_j \gamma_j) \le 3\sum_j \operatorname{size}(\gamma_j)$. Additionally,*

$$\operatorname{size}(\prod_{j=1}^k \gamma_j) \le k\cdot 3d^2\cdot(\lceil\log|\Delta_K|\rceil + \sum_{j=1}^k \operatorname{size}(\gamma_j)).$$

4. *For fractional $\mathcal{O}_K$ ideals $\mathfrak{a},\mathfrak{a}_i$ of K, we have $\operatorname{size}(\mathfrak{a}) \le d^2\operatorname{size}(N(\mathfrak{a}))$ and $\operatorname{size}(\prod_{i=1}^k \mathfrak{a}_i) \le d^2\sum_{i=1}^k \operatorname{size}(\mathfrak{a}_i)$.*

Proof. 1. We have $\operatorname{size}(mn) = 1+\lceil\log_2(|m|)+\log_2(|n|)\rceil \le \operatorname{size}(m)+\operatorname{size}(n)$. This generalizes to larger products. Assume without loss of generality that m_1 is the largest (in absolute value) among the m_j. Then we have

$$\operatorname{size}(\sum_{j=1}^k m_j) = 1+\lceil\log_2|\sum_{j=1}^k m_j|\rceil \le 1+\lceil\log_2(k\cdot|m_1|)\rceil \le \operatorname{size}(k)+\operatorname{size}(m_1).$$

2. We have $\text{size}(\frac{a}{b} \cdot \frac{c}{d}) = \text{size}(ac) + \text{size}(bd) \leq \text{size}(a) + \text{size}(c) + \text{size}(b) + \text{size}(d) \leq \text{size}(\frac{a}{b}) + \text{size}(\frac{c}{d})$, (by part (i)) which generalizes to larger products.

   Write $q_j = \frac{a_j}{b_j}$, and write

$$q = \sum_{j=1}^{k} q_i = \sum_{j=1}^{k} \frac{a_j}{b_j} = \frac{\sum_{j=1}^{k} \left(a_j \prod_{t \neq j} b_t \right)}{\prod_{j=1}^{k} b_j}$$

   Then, by definition and by part (i),

$$\text{size}(q) \leq \text{size}(\prod_{j=1}^{k} b_j) + \text{size}(\sum_{j=1}^{k} (a_j \prod_{t \neq j} b_t)) \leq \sum_{j=1}^{k} \text{size}(b_j) + \max_j \text{size}(a_j \prod_{t \neq j} b_t) + \text{size}(k).$$

$$\leq 2 \sum_{j=1}^{k} \text{size}(q_j) + \text{size}(k) \leq 3 \sum_{j=1}^{k} \text{size}(q_j).$$

3. Note that the size of $\gamma = \sum_{j=1}^{k} \gamma_j$ is dictated by its rational coefficients in the $\mathcal{O}_K$-basis $(\beta_1, \ldots, \beta_d)$, which are just the rational coefficients of γ_j added together. Hence, $\text{size}(\gamma) \leq 3 \sum_{j=1}^{k} \text{size}(\gamma_j)$ by part (ii).

   Writing $\gamma = \sum_{i=1}^{d} g_i \beta_i$ and $\delta = \sum_{i=1}^{d} d_i \beta_i$, we obtain

$$\gamma \cdot \delta = (\sum_i g_i \beta_i)(\sum_i d_i \beta_i) = \sum_{ij} g_i d_j \beta_i \beta_j = \sum_{k=1}^{d} \left(\sum_{ij} g_i d_j [\beta_i \beta_j]_k \right) \beta_k,$$

   where $[\beta_i \beta_j]_k \in \mathbb{Z}$ denotes the coefficient in $\mathbb{Q}$ of $\beta_i \beta_j$ in terms of the basis element β_k, i.e., $\beta_i \beta_j = \sum_{k=1}^{d} [\beta_i \beta_j]_k \beta_k$. By the fact that $\beta_i \beta_j$ can be written in the $(\beta_1, \ldots, \beta_d)$-basis with integer coefficients bounded by $\sqrt{d}|\Delta_K|^{d+2}$, i.e., $|[\beta_i \beta_j]_k| \leq \sqrt{d}|\Delta_K|^{d+2} \leq |\Delta_K|^{3d}$ (this follows from the assumptions in the beginning of Section 2.3.3) for all i, j, k, we see that, by part (ii),

$$\text{size}(\gamma\delta) = \sum_{k=1}^{d} \text{size} \left(\sum_{ij} g_i d_j [\beta_i \beta_j]_k \right) \leq 3d \cdot \sum_{i,j} (\text{size}(g_i d_j) + 3d \lceil \log |\Delta_K| \rceil)$$

$$\leq 3d^3 \lceil \log |\Delta_K| \rceil + 3d \sum_{i,j} (\text{size}(g_i) + \text{size}(d_j)) \leq 3d^3 (\lceil \log |\Delta_K| \rceil + \text{size}(\gamma) + \text{size}(\delta))$$

   For larger products, by dividing the products in two in a binary fashion, we obtain, by induction,

$$\text{size}(\prod_{j=1}^{k} \gamma_j) \leq k \cdot 3d^2 \cdot (\lceil \log |\Delta_K| \rceil + \sum_{j=1}^{k} \text{size}(\gamma_j)).$$

4. For any integral ideal $\mathfrak{a} \subseteq \mathcal{O}_K$, we have that $\text{size}(\mathfrak{a}) \leq d^2 \, \text{size}(N(\mathfrak{a}))$, since $\mathfrak{a}$ is represented by its HNF generating matrix (with entries in $\mathbb{Z}$), of which the product of the diagonal entries must equal $N(\mathfrak{a})$. Hence, by the HNF properties, each of the coefficients must be bounded in absolute value by $N(\mathfrak{a})$. For fractional ideals, the scaling of the generating matrix of $\mathfrak{a}$ can be chosen to be the denominator of $N(\mathfrak{a})$. Hence, also for fractional ideals $\mathfrak{a}$ holds that $\text{size}(\mathfrak{a}) \leq d^2 \, \text{size}(N(\mathfrak{a}))$. By the fact that the product of the diagonals equals the norm, we also have $\text{size}(N(\mathfrak{a})) \leq \text{size}(\mathfrak{a})$.

   It follows then that $\text{size}(\prod_{i=1}^{k} \mathfrak{a}_i) \leq d^2 \sum_{i=1}^{k} \text{size}(\mathfrak{a}_i)$.

□

References

[Ajt02] M. Ajtai. "Random Lattices and a Conjectured 0 - 1 Law about Their Polynomial Time Computable Properties". *43rd FOCS*. IEEE Computer Society Press, Nov. 2002, pp. 733–742. DOI: 10.1109/SFCS.2002.1181998 (cit. on p. 3).

[Ajt96] M. Ajtai. "Generating Hard Instances of Lattice Problems (Extended Abstract)". *28th ACM STOC*. ACM Press, May 1996, pp. 99–108. DOI: 10.1145/237814.237838 (cit. on pp. 1, 3).

[Ajt99] M. Ajtai. "Generating Hard Instances of the Short Basis Problem". *Automata, Languages and Programming, 26th International Colloquium, ICALP'99, Prague, Czech Republic, July 11-15, 1999, Proceedings*. Ed. by J. Wiedermann, P. van Emde Boas, and M. Nielsen. Vol. 1644. Lecture Notes in Computer Science. Springer, 1999, pp. 1–9. DOI: 10.1007/3-540-48523-6_1 (cit. on p. 3).

[Alz97] H. Alzer. "On some inequalities for the gamma and psi functions". English. *Math. Comput.* 66.217 (1997), pp. 373–389. DOI: 10.1090/S0025-5718-97-00807-7 (cit. on p. 52).

[Ban93] W. Banaszczyk. "New bounds in some transference theorems in the geometry of numbers." *Mathematische Annalen* 296.4 (1993), pp. 625–636 (cit. on p. 54).

[BB11] V. Blomer and F. Brumley. "On the Ramanujan conjecture over number fields". *Ann. of Math. (2)* 174.1 (2011), pp. 581–605. DOI: 10.4007/annals.2011.174.1.18 (cit. on p. 28).

[BB13] V. Blomer and F. Brumley. "The role of the Ramanujan conjecture in analytic number theory". *Bull. Amer. Math. Soc. (N.S.)* 50.2 (2013), pp. 267–320. DOI: 10.1090/S0273-0979-2013-01404-6 (cit. on pp. 9, 28).

[BDK+18] J. W. Bos et al. "CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM". *2018 IEEE European Symposium on Security and Privacy*. IEEE Computer Society Press, Apr. 2018, pp. 353–367. DOI: 10.1109/EuroSP.2018.00032 (cit. on p. 2).

[BDP+20] K. de Boer, L. Ducas, A. Pellet-Mary, and B. Wesolowski. "Random Self-reducibility of Ideal-SVP via Arakelov Random Walks". *CRYPTO 2020, Part II*. Ed. by D. Micciancio and T. Ristenpart. Vol. 12171. LNCS. Springer, Cham, Aug. 2020, pp. 243–273. DOI: 10.1007/978-3-030-56880-1_9 (cit. on pp. 1, 4, 9, 29, 30, 37, 46, 47, 66, 79, 96, 98).

[BF12] J.-F. Biasse and C. Fieker. "A polynomial time algorithm for computing the HNF of a module over the integers of a number field". *Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation*. ISSAC '12. New York, NY, USA: Association for Computing Machinery, 2012, 75–82. DOI: 10.1145/2442829.2442844 (cit. on pp. 16, 34, 35).

[BK96] J. Buchmann and V. Kessler. "Computing a Reduced Lattice Basis From a Generating System". *Unpublished Manuscript* (Aug. 1996) (cit. on p. 35).

[Blu60] L. E. Blumenson. "A Derivation of n-Dimensional Spherical Coordinates". *The American Mathematical Monthly* 67.1 (1960), pp. 63–66 (cit. on pp. 68, 69).

[Boe22] K. de Boer. "Random walks on Arakelov class groups". Doctoral Thesis. Leiden University, 2022 (cit. on p. 4).

[Bos20] J.-B. Bost. “Euclidean lattices, theta series and slopes [after W. Banaszczyk, O. Regev, D. Dadush, N. Stephens-Davidowitz, ...]” English. *Séminaire Bourbaki. Volume 2018/2019, Exposés 1151–1165. Avec table par noms d'auteurs de 1948 à 2018/19*. Paris: Société Mathématique de France (SMF), 2020, 1–59, ex. DOI: 10.24033/ast.1130 (cit. on p. 47).

[BP89] J. Buchmann and M. Pohst. “Computing a Lattice Basis from a System of Generating Vectors”. *Proceedings of the European Conference on Computer Algebra*. EUROCAL '87. London, UK, UK: Springer-Verlag, 1989, pp. 54–63 (cit. on p. 35).

[BPW25] K. de Boer, A. Pellet-Mary, and B. Wesolowski. *Rigorous Methods for Computational Number Theory*. Cryptology ePrint Archive, Paper 2025/1514. 2025 (cit. on pp. 1, 4, 18, 98).

[Cas97] J. W. S. Cassels. *An introduction to the geometry of numbers*. Classics in Mathematics. Corrected reprint of the 1971 edition. Springer-Verlag, Berlin, 1997, pp. viii+344 (cit. on p. 18).

[Coh07] H. Cohen. *Number theory. Volume II: Analytic and modern tools*. English. Vol. 240. Grad. Texts Math. New York, NY: Springer, 2007. DOI: 10.1007/978-0-387-49894-2 (cit. on p. 50).

[Coh13] H. Cohen. *A course in computational algebraic number theory*. English. Vol. 138. Springer Berlin, Heidelberg, 2013. DOI: 10.1007/978-3-662-02945-9 (cit. on p. 2).

[Coh99] H. Cohen. *Advanced Topics in Computational Number Theory*. Graduate Texts in Mathematics. Springer New York, 1999 (cit. on pp. 15, 16).

[COU01] L. Clozel, H. Oh, and E. Ullmo. “Hecke operators and equidistribution of Hecke points”. *Invent. Math.* 144.2 (2001), pp. 327–351. DOI: 10.1007/s002220100126 (cit. on p. 5).

[CT06] T. M. Cover and J. A. Thomas. *Elements of Information Theory 2nd Edition (Wiley Series in Telecommunications and Signal Processing)*. Wiley-Interscience, July 2006 (cit. on p. 20).

[CU04] L. Clozel and E. Ullmo. “Équidistribution des points de Hecke”. *Contributions to automorphic forms, geometry, and number theory*. Johns Hopkins Univ. Press, Baltimore, MD, 2004, pp. 193–254 (cit. on pp. 3, 6, 9, 26, 28).

[Dev86] L. Devroye. *Non-Uniform Random Variate Generation(originally published with*. New York: Springer-Verlag, 1986 (cit. on pp. 71, 72).

[DK22] S. Düzlü and J. Krämer. “Application of automorphic forms to lattice problems”. *J. Math. Cryptol.* 16.1 (2022), pp. 156–197. DOI: 10.1515/jmc-2021-0045 (cit. on p. 4).

[DKL+18] L. Ducas et al. “CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme”. *IACR TCHES* 2018.1 (2018), pp. 238–268. DOI: 10.13154/tches.v2018.i1.238-268 (cit. on p. 2).

[EO06] A. Eskin and H. Oh. “Ergodic theoretic proof of equidistribution of Hecke points”. *Ergodic Theory Dynam. Systems* 26.1 (2006), pp. 163–167. DOI: 10.1017/S0143385705000428 (cit. on p. 5).

[FPS22] J. Felderhoff, A. Pellet-Mary, and D. Stehlé. “On Module Unique-SVP and NTRU”. *ASIACRYPT 2022, Part III*. Ed. by S. Agrawal and D. Lin. Vol. 13793. LNCS. Springer, Cham, Dec. 2022, pp. 709–740. DOI: 10.1007/978-3-031-22969-5_24 (cit. on pp. 16, 30).

[FPS+23a] J. Felderhoff, A. Pellet-Mary, D. Stehlé, and B. Wesolowski. "Ideal-SVP is Hard for Small-Norm Uniform Prime Ideals". *TCC 2023, Part IV*. Ed. by G. N. Rothblum and H. Wee. Vol. 14372. LNCS. Springer, Cham, 2023, pp. 63–92. DOI: 10.1007/978-3-031-48624-1_3 (cit. on pp. 4, 34).

[FPS+23b] J. Felderhoff, A. Pellet-Mary, D. Stehlé, and B. Wesolowski. *Ideal-SVP is Hard for Small-Norm Uniform Prime Ideals*. Cryptology ePrint Archive, Paper 2023/1370. 2023 (cit. on pp. 35, 80).

[Gen10] C. Gentry. "Toward Basing Fully Homomorphic Encryption on Worst-Case Hardness". *CRYPTO 2010*. Ed. by T. Rabin. Vol. 6223. LNCS. Springer, Berlin, Heidelberg, Aug. 2010, pp. 116–137. DOI: 10.1007/978-3-642-14623-7_7 (cit. on pp. 1, 3).

[GH24] J. R. Getz and H. Hahn. *An Introduction to Automorphic Representations: With a view toward trace formulae*. Vol. 300. Graduate Texts in Mathematics. Springer Cham, 2024. DOI: https://doi.org/10.1007/978-3-031-41153-3 (cit. on pp. 26, 27).

[GM03] D. Goldstein and A. Mayer. "On the equidistribution of Hecke points". *Forum Mathematicum* 15.2 (2003), pp. 165–189 (cit. on p. 3).

[GPV08] C. Gentry, C. Peikert, and V. Vaikuntanathan. "Trapdoors for hard lattices and new cryptographic constructions". *40th ACM STOC*. Ed. by R. E. Ladner and C. Dwork. ACM Press, May 2008, pp. 197–206. DOI: 10.1145/1374376.1374407 (cit. on pp. 34, 80).

[Gra84] D. R. Grayson. "Reduction theory using semistability". English. *Comment. Math. Helv.* 59 (1984), pp. 600–634. DOI: 10.1007/BF02566369 (cit. on pp. 6, 47, 54).

[GSV+25a] N. Gargava, V. Serban, M. Viazovska, and I. Viglino. *Module lattices and their shortest vectors*. Preprint, arXiv:2510.12893 [math.NT] (2025). 2025 (cit. on pp. 6, 47, 48).

[GSV+25b] N. P. Gargava, V. Serban, M. Viazovska, and I. Viglino. *Effective module lattices and their shortest vectors*. Preprint, arXiv:2402.10305 [math.NT] (2025). 2025 (cit. on pp. 6, 47, 48).

[Hen02] M. Henk. "Successive minima and lattice points". English. *IV international conference on "Stochastic geometry, convex bodies, empirical measures and applications to engineering science", Tropea, Italy, September 24–29, 2001. Vol. I*. Palermo: Circolo Matematico di Palermo, 2002, pp. 377–384 (cit. on p. 43).

[HR07] I. Haviv and O. Regev. "Tensor-based hardness of the shortest vector problem to within almost polynomial factors". *39th ACM STOC*. Ed. by D. S. Johnson and U. Feige. ACM Press, June 2007, pp. 469–477. DOI: 10.1145/1250790.1250859 (cit. on p. 1).

[HR14] I. Haviv and O. Regev. "On the Lattice Isomorphism Problem". *25th SODA*. Ed. by C. Chekuri. ACM-SIAM, Jan. 2014, pp. 391–404. DOI: 10.1137/1.9781611973402.29 (cit. on p. 99).

[IR08] I. C. F. Ipsen and R. Rehman. "Perturbation Bounds for Determinants and Characteristic Polynomials". *SIAM Journal on Matrix Analysis and Applications* 30.2 (2008), pp. 762–776. DOI: 10.1137/070704770. eprint: https://doi.org/10.1137/070704770 (cit. on p. 33).

[JMV09] D. Jao, S. D. Miller, and R. Venkatesan. "Expander graphs based on GRH with an application to elliptic curve cryptography". *J. Number Theory* 129.6 (2009), pp. 1491–1504. DOI: 10.1016/j.jnt.2008.11.006 (cit. on p. 4).

[Kle00] P. N. Klein. “Finding the closest lattice vector when it’s unusually close”. *11th SODA*. Ed. by D. B. Shmoys. ACM-SIAM, Jan. 2000, pp. 937–941 (cit. on p. 80).

[KV18] S. Kim and A. Venkatesh. “The behavior of random reduced bases”. *Int. Math. Res. Not. IMRN* 20 (2018), pp. 6442–6480. DOI: 10.1093/imrn/rnx074 (cit. on p. 1).

[LLL82] A. K. Lenstra, H. W. Lenstra Jr., and L. Lovász. “Factoring polynomials with rational coefficients”. *Mathematische Annalen* 261.4 (1982), pp. 515–534 (cit. on pp. 1, 3, 21, 56).

[LLS90] J. C. Lagarias, H. W. Lenstra Jr., and C.-P. Schnorr. “Korkin-Zolotarev bases and successive minima of a lattice and its reciprocal lattice.” *Combinatorica* 10.4 (1990), pp. 333–348 (cit. on p. 100).

[Lou00] S. Louboutin. “Explicit Bounds for Residues of Dedekind Zeta Functions, Values of L-Functions at s=1, and Relative Class Numbers”. *Journal of Number Theory* (2000). DOI: 10.1006/jnth.2000.2545 (cit. on p. 26).

[LPS+19] C. Lee, A. Pellet-Mary, D. Stehlé, and A. Wallet. “An LLL Algorithm for Module Lattices”. *ASIACRYPT 2019, Part II*. Ed. by S. D. Galbraith and S. Moriai. Vol. 11922. LNCS. Springer, Cham, Dec. 2019, pp. 59–90. DOI: 10.1007/978-3-030-34621-8_3 (cit. on p. 3).

[LS15] A. Langlois and D. Stehlé. “Worst-case to average-case reductions for module lattices”. *DCC* 75.3 (2015), pp. 565–599. DOI: 10.1007/s10623-014-9938-4 (cit. on pp. 2, 3).

[LS64] J. V. Linnik and B. F. Skubenko. “Asymptotic distribution of integral matrices of third order”. *Vestnik Leningrad. Univ. Ser. Mat. Meh. Astronom.* 19.3 (1964), pp. 25–36 (cit. on p. 5).

[MG02] D. Micciancio and S. Goldwasser. *Complexity of lattice problems: a cryptographic perspective*. Vol. 671. Springer Science & Business Media, 2002 (cit. on pp. 60, 99).

[Mic02] D. Micciancio. “Generalized Compact Knapsacks, Cyclic Lattices, and Efficient One-Way Functions from Worst-Case Complexity Assumptions”. *43rd FOCS*. IEEE Computer Society Press, Nov. 2002, pp. 356–365. DOI: 10.1109/SFCS.2002.1181960 (cit. on p. 2).

[Mic98] D. Micciancio. “The Shortest Vector in a Lattice is Hard to Approximate to Within Some Constant”. *39th FOCS*. IEEE Computer Society Press, Nov. 1998, pp. 92–98. DOI: 10.1109/SFCS.1998.743432 (cit. on p. 1).

[MP21] C. Maire and A. Page. “Codes from unit groups of division algebras over number fields”. English. *Math. Z.* 298.1-2 (2021), pp. 327–348. DOI: 10.1007/s00209-020-02614-5 (cit. on pp. 24–26, 65, 67, 71).

[MR07] D. Micciancio and O. Regev. “Worst-Case to Average-Case Reductions Based on Gaussian Measures”. *SIAM J. Comput.* 37.1 (Apr. 2007), pp. 267–302. DOI: 10.1137/S0097539705447360 (cit. on pp. 19, 20, 34, 37, 81).

[Nat24a] National Institute of Standards and Technology. *FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)*. Tech. rep. FIPS 203. U.S. Department of Commerce / NIST, 2024. DOI: 10.6028/NIST.FIPS.203 (cit. on pp. 1, 2).

[Nat24b] National Institute of Standards and Technology. *FIPS 204: Module-Lattice-Based Digital Signature Algorithm (ML-DSA)*. Tech. rep. FIPS 204. U.S. Department of Commerce / NIST, 2024. DOI: 10.6028/NIST.FIPS.204 (cit. on pp. 1, 2).

[Neu99] J. Neukirch. *Algebraic number theory*. Vol. 322. Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. Springer-Verlag, Berlin, 1999, pp. xviii+571. DOI: 10.1007/978-3-662-03983-0 (cit. on p. 13).

[Nic11] L. Nicolaescu. *The coarea formula*. 2011. URL: http://www.nd.edu/~lnicolae/Coarea.pdf (cit. on p. 22).

[NS06] P. Q. Nguyen and D. Stehlé. "LLL on the average". *Algorithmic number theory*. Vol. 4076. Lecture Notes in Comput. Sci. Springer, Berlin, 2006, pp. 238–256. DOI: 10.1007/11792086_18 (cit. on pp. 1, 3).

[Poi77] G. Poitou. *Sur les petits discriminants*. French. Semin. Delange-Pisot-Poitou, 18e Annee 1976/77, Theor. des Nombres, Fasc. 1, Expose 6, 18 p. (1977). 1977 (cit. on p. 55).

[PP21] M. Plançon and T. Prest. "Exact Lattice Sampling from Non-Gaussian Distributions". *PKC 2021, Part I*. Ed. by J. Garay. Vol. 12710. LNCS. Springer, Cham, May 2021, pp. 573–595. DOI: 10.1007/978-3-030-75245-3_21 (cit. on p. 100).

[PS21] A. Pellet-Mary and D. Stehlé. "On the Hardness of the NTRU Problem". *ASIACRYPT 2021, Part I*. Ed. by M. Tibouchi and H. Wang. Vol. 13090. LNCS. Springer, Cham, Dec. 2021, pp. 3–35. DOI: 10.1007/978-3-030-92062-3_1 (cit. on pp. 34, 37, 81).

[PW24] A. Page and B. Wesolowski. "The Supersingular Endomorphism Ring and One Endomorphism Problems are Equivalent". *EUROCRYPT 2024, Part VI*. Ed. by M. Joye and G. Leander. Vol. 14656. LNCS. Springer, Cham, May 2024, pp. 388–417. DOI: 10.1007/978-3-031-58751-1_14 (cit. on p. 4).

[Reg05] O. Regev. "On lattices, learning with errors, random linear codes, and cryptography". *37th ACM STOC*. Ed. by H. N. Gabow and R. Fagin. ACM Press, May 2005, pp. 84–93. DOI: 10.1145/1060590.1060603 (cit. on pp. 1, 4).

[Rog55] C. A. Rogers. "Mean values over the space of lattices". *Acta Math.* 94 (1955), pp. 249–287. DOI: 10.1007/BF02392493 (cit. on p. 3).

[Sar91] P. C. Sarnak. "Diophantine problems and linear groups". *Proceedings of the International Congress of Mathematicians, Vol. I, II (Kyoto, 1990)*. Math. Soc. Japan, Tokyo, 1991, pp. 459–471 (cit. on p. 5).

[Sie45] C. L. Siegel. "A mean value theorem in geometry of numbers". *Ann. of Math. (2)* 46 (1945), pp. 340–347. DOI: 10.2307/1969027 (cit. on p. 2).

[Ste99] N. Steenrod. *The Topology of Fibre Bundles*. Princeton Landmarks in Mathematics and Physics. Princeton University Press, 1999 (cit. on p. 70).

[SW14] U. Shapira and B. Weiss. "A volume estimate for the set of stable lattices". English. *C. R., Math., Acad. Sci. Paris* 352.11 (2014), pp. 875–879. DOI: 10.1016/j.crma.2014.08.019 (cit. on pp. 6, 47).

[Thu98] J. L. Thunder. "Higher-dimensional analogs of Hermite's constant". English. *Mich. Math. J.* 45.2 (1998), pp. 301–314. DOI: 10.1307/mmj/1030132184 (cit. on pp. 6, 47–49).

[Wei82] A. Weil. *Adèles and algebraic groups. (Appendix 1: The case of the group G_2, by M. Demazure. Appendix 2: A short survey of subsequent research on Tamagawa numbers, by T. Ono)*. English. Vol. 23. Prog. Math. Birkhäuser, Cham, 1982 (cit. on p. 49).

List of symbols

Symbol	Description
$\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \ldots$	Ideals of the ring of integers $\mathcal{O}_K$ of a number field K
$\mathbb{A}_K$	The adèles of the number field K
$B(t)$	The ball of radius t in $\mathrm{SL}_r(K_{\mathbb{R}})$, with respect to the the distance notation ρ (page 24)
B	Bound in the definition of the set of all prime ideals $\mathcal{P}(B)$ whose norm is bounded by B (page 29)
$\mathbf{B}$	Basis part in $(\mathbf{B}, \mathbf{I})$, with $\mathbf{B} \in K^{r \times r}$, a pseudo-bases of a module-lattice M, sometimes also just a basis in $\mathbb{Q}^{r \times r}$
d	Degree $d = [K : \mathbb{Q}]$ of the number field K
$\mathcal{G}_.$	Either discrete Gaussian or continuous Gaussian distribution, depending on the subscript (page 19)
H	The hyperplane where the logarithmic embedding of the units $\mathcal{O}_K^\times$ lives in (page 21)
$\mathbf{I}$	Ideal part in $(\mathbf{B}, \mathbf{I})$, with $\mathbf{I} = (\mathfrak{a}_1, \ldots, \mathfrak{a}_r)$, where $(\mathbf{B}, \mathbf{I})$ is a pseudo-basis of a rank r module-lattice M
K	Number field of degree $d = [K : \mathbb{Q}]$ and discriminant Δ_K
L	Generally, a lattice
$L^p(\cdot)$	The space of L^p-integrable functions over the specified space
M	A module (lattice) of rank r over the field K
n	The dimension $n = d \cdot r$ of the module lattices occurring in this work over $\mathbb{R}$
$N(\cdot)$	The absolute norm of elements of ideals of the field K
$O(\cdot), o(\cdot)$	Landau's big-O and small-o notation
$\mathcal{O}_K$	The ring of integers of K
$\mathcal{O}_K^\times$	The unit group of K
$\mathfrak{p}$	A prime ideal of K
$\mathcal{P}, \mathcal{P}(B)$	A set of prime ideals of K, generally $\mathcal{P} = \mathcal{P}(B)$, the set of all prime ideals with norm bounded by B
r	The rank as a module over K, of modules (module lattices) occurring in this work
r_1	The number of real embeddings of K
r_2	The number of complex embeddings of K
r_u	The rank of the unit group $\mathcal{O}_K^\times$
$\mathrm{Round}_{\mathrm{Lat}}, \mathrm{Round}_{\mathrm{Lat}}^{\mathrm{Perf}}$	The algorithm rounding a module lattice to a close rational module lattice (page 30)
$\mathrm{size}(\cdot)$	The number of bits required to represent the algebraic object at hand (page 15)
t	A parameter in the continuous randomization (or initial distribution) of the input module lattice of the random walk method of this paper (see also $B(t)$) (page 24)

Symbol	Description
$T_{\mathfrak{p}}$	The Hecke operator corresponding to uniform averaging over submodules $N \subset M$ such that at $M/N \cong \mathcal{O}_K/\mathfrak{p}$ (page 27)
$T_{\mathcal{P}}, T_{\mathcal{P}(B)}$	The Hecke operator corresponding to averaging over all $T_{\mathfrak{p}}$ with $\mathfrak{p} \in \mathcal{P}$ or $\mathcal{P}(B)$ (page 29)
$X_r, X_r(K)$	The space of similarity classes of modules lattices over K of rank r (page 14)
$X_{r,\mathfrak{a}}$	The component of the space of similarity classes of modules lattices over K of rank r, dictated by the ideal class of $\mathfrak{a}$ (page 14)
Y_r	The space of invertible $r \times r$ matrices over K up to rotation and scaling (page 21)
α	Balancedness parameter for a module lattice (page 17)
Γ_K	The maximum of the quotient between the outermost successive minima $\lambda_n(I)/\lambda_1(I)$ over all ideal lattices I of the number field K (page 17)
Δ_K	The discriminant of the number field K
ε	A small error parameter in $[0, 1]$, often indicating the failure probability of an algorithm
ε_0	The closeness of the $\mathrm{Round}_{\mathrm{Lat}}$-algorithm to the perfect distribution $\mathrm{Round}_{\mathrm{Lat}}^{\mathrm{Perf}}$ (page 31)
$\lambda_j(\Lambda)$	The j-th successive minimum of the lattice Λ with respect to the 2-norm (page 17)
$\lambda_j^{(\infty)}(\Lambda)$	The j-th successive minimum of the lattice Λ with respect to the ∞-norm (page 17)
$\lambda_j^K(M)$	The j-th successive K-minimum of the module lattice M with respect to the canonical norm (page 17)
μ	The Haar measure on X_r (page 14)
μ_{cut}	The 'cut' Haar measure on X_r (page 95)
μ_{Riem}	The Riemannian measure on X_r (page 21 and page 14)
ρ_σ	The Gaussian function $x \mapsto e^{-\pi\|x\|^2/\sigma^2}$ (page 19)
σ	The deviation for the Gaussian function or the (discrete) Gaussian distribution
φ_z	The initial distribution on X_r by 'folding' the distribution f_z (page 39)