Solving the Shortest Vector Problem in $2^{0.63269n+o(n)}$ time on Random Lattices

Amaury Pouly[1] and Yixin Shen[2]

[1] Centre National de la Recherche Scientifique (CNRS), France
[2] Univ Rennes, Inria, CNRS, IRISA, Rennes, France

Abstract. The Shortest Vector problem (SVP) is the most important problem in lattice-based cryptanalysis. There is currently a gap in the understanding of this problem with respect to its worst-case complexity and its average-case behaviour. For instance, SVP on an n-dimensional lattice has worst-case complexity $2^{n+o(n)}$ [ADRS15]. However, in practice, people rely on heuristic (unproven) sieving algorithms of time complexity $2^{0.292n+o(n)}$ [BDGL16] to assess the security of lattice-based cryptography schemes. Those heuristic algorithms are experimentally verified for lattices used in cryptography, which are usually random in some way *.
In this paper, we try to bridge the gap between worst-case and heuristic algorithms. Using the formalism of random real lattices developed by Siegel [Sie45], we show a tighter upper bound on an important lattice parameter called the smoothing parameter that applies to almost all random lattices. Using a known discrete Gaussian sampler at the smoothing parameter, we can then directly sample short vectors. This allows us to provably solve an approximation version of the SVP on almost all random lattices with a small constant approximation factor 1.123, in time $2^{n/2+o(n)}$. With further analysis, we can provably solve the exact SVP in time $2^{0.63269n+o(n)}$ on almost all random lattices as well. We also provide a smooth time approximation factor tradeoff between these two cases. All our algorithms work in space $2^{n/2+o(n)}$. Our paper is a first step towards better understanding the heuristic behaviour of lattice sieving on random lattices.

1 Introduction

Lattice problems are central to modern cryptography and computational complexity theory due to their inherent hardness, which provides a foundation for secure cryptographic protocols. These problems are believed to be difficult to solve efficiently, even for quantum computers. This makes lattice-based cryptography a promising candidate for post-quantum security, offering resilience against future quantum attacks [BDK+18, DKL+18, FHK+19]. Moreover, lattice problems have applications in algorithmic number theory [LLL82], convex optimization [Jr.83, Kan87, FT87], coding theory [dB89], and cryptanalysis tools [Sha84, Bri84, LO85], reinforcing their importance across both theoretical and practical domains in computer science.

There is currently a gap in the understanding of these problems with respect to their worst-case complexity and their average-case behaviour. For instance, the Shortest Vector problem (SVP) on an n-dimensional lattice has worst-case complexity $2^{n+o(n)}$ [ADRS15]. However, in practice, people rely on heuristic (unproven) sieving algorithms of time complexity $2^{0.292n+o(n)}$ [BDGL16] to assess the security of lattice-based cryptography schemes. Those heuristic algorithms are experimentally verified for lattices used in

E-mail: amaury.pouly@cnrs.fr (Amaury Pouly), yixin.shen@inria.fr (Yixin Shen)
*There exists several formal notions of random lattices.

Date of this document: 2025-02-14.

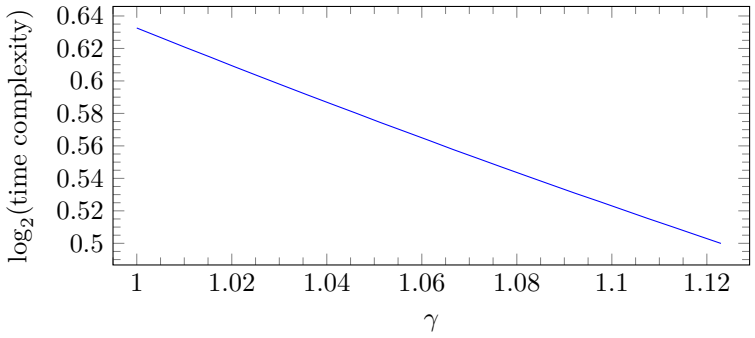

Figure 1: Time complexity to solve γ-SVP on random lattices (Theorem 1)

cryptography, which are usually random in some way, but only seem to provide very short and not shortest nonzero vectors.

For most cryptographic applications, finding a short, but not necessarily shortest, nonzero vector is in fact sufficient. The α-SVP consists in finding a nonzero vector of length at most α times the length of a shortest nonzero vector. Surprisingly, very little is known about the worst-case complexity about this problem. The best provable algorithm has worst-case complexity $2^{0.802n+o(n)}$ [WLW15] but only solve $O(1)$-SVP for an unspecified constant. More explicit constants are provided in [AUV19] but even for $\alpha = 100$, the time complexity is still $2^{0.824n+o(n)}$. In [BN24], the authors noted that there is no theoretical evidence to show that $\sqrt{2}$-SVP is easier than SVP. In fact, solving $\sqrt{2}$-SVP in time better than $2^{n+o(n)}$ would give a better algorithm for $\mathbb{Z}$LIP which is a recent hardness assumption in lattice-based cryptographic schemes [DvW22]. If we relax the approximation ratio, better complexities can be achieved. For example, [ALSD21] gives an algorithm that solves $\tilde{O}(\sqrt{n})$-SVP in time $2^{n/2+o(n)}$.

SVP. In this paper, we try to bridge the gap between worst-case and heuristic algorithms. Using the formalism of random real lattices developped by Siegel [Sie45], we obtain a $2^{n/2+o(n)}$ time algorithm for 1.123-SVP and a $2^{0.63269n+o(n)}$ time algorithm for exact SVP on random lattices. More generally, we obtain a smooth tradeoff between the time complexity and the approximation factor (see Figure 1). Our algorithm (Theorem 1) achieves a much better approximation ratio compared to all worst-case algorithms and is particularly simple compared to [ALSD21].

Theorem 1 (Informal, see Theorem 9, Remark 2 and Corollary 5)**.** *There is an algorithm that, for every $n \geqslant 1$ and $\gamma \in [1, 1.122973948]$ solves γ-SVP on most lattices in time $e^{o(n)}(\frac{\gamma^2}{2}e^{-\gamma^2/2e})^{-n/2}$ and space $2^{n/2+o(n)}$.*

Hermite SVP. Most lattice reduction algorithms rely on solving α-SVP in smaller dimension [Sch87] for α close to 1 [ABLR21]. In certain lattice reduction algorithms such as slide reduction [GN08, ALNSD20], it is more convenient for the analysis to compare the length of short vectors to the determinant of the lattice instead of the length of a shortest vector. The problem of finding a vector of length at most $\alpha \operatorname{vol}(\mathcal{L})^{1/n}$ for a lattice $\mathcal{L} \subset \mathbb{R}^n$ is known as the α-Hermite SVP (α-HSVP). Our algorithm (Theorem 2) also solves $\sqrt{\frac{0.2320n}{\pi}}$-HSVP in time $2^{n/2+o(n)}$ and $\sqrt{\frac{n}{2\pi e}}$-HSVP in time $2^{0.63269n+o(n)}$ for random lattices. More generally, we obtain a smooth trade-off between the time complexity and the approximation factor. This improves upon the worst-case algorithm of [ALSD21] which

solves $\tilde{O}(\sqrt{n})$-HSVP in time $2^{n/2+o(n)}$. Indeed, we avoid the extra logarithmic factors in the approximation ratio and obtain a much better constant.

Theorem 2 (Informal, see Theorem 8 and Corollary 4)**.** *There is an algorithm that, for every $n \geqslant 1$ and $\beta \in [0.1514, 0.2320]$ solves $\sqrt{\frac{n\beta}{\pi}}$-SVP on most lattices in time $e^{o(n)}(\beta e^{1-\beta})^{-n/2} + 2^{n/2+o(n)}$ and space $2^{n/2+o(n)}$.*

Our algorithm works by sampling the discrete Gaussian distribution $D_{\mathcal{L},s}$ on the lattice $\mathcal{L}$, a very commonly used distribution in lattice algorithms. This distribution is parametrized by the width s. It is known that sampling from $D_{\mathcal{L},s}$ is easy when s is large but very hard when s is small. An important quantity, known as the smoothing parameter $\eta_\varepsilon(\mathcal{L})$, intuitively characterizes when $D_{\mathcal{L},s}$ transitions from a "smooth" distribution to a discrete one (see Section 2.5). In particular, we use [ADRS15] to sample from $D_{\mathcal{L},s}$ for $s = \sqrt{2}\eta_{1/2}(\mathcal{L})$. Our main technical result is a probabilistic bound on the value of $\eta_\varepsilon(\mathcal{L})$ for a random lattice $\mathcal{L}$ for all $\varepsilon > 0$. This allows us to obtain tigher bounds on the length of vectors sampled from $D_{\mathcal{L},s}$. More precisely, we obtain probabilistic bounds on $\rho_s(\mathcal{L})$ for a random lattice, and more generally on $\rho_s(\mathcal{L} \cap B_n(r))$ for any $r > 0$. The latter could be of independent interesting since tail bounds on the Gaussian mass are extremely useful in the analysis of lattice algorithms.

The sampler from [ADRS15] takes time $2^{n/2+o(n)}$ but produces $2^{n/2+o(n)}$ vectors. Interesingly, we find that already with a single call to sampler we can solve 1.123-SVP but by calling the sampler an exponential number of times, we can decrease the approximation factor and even solve SVP. Therefore, any improvement in those samplers would yield an improvement to the complexity of solving 1.123-SVP (and correspondingly HSVP) for random lattices. Lattice-based cryptography relies on the fact that problems such as α-SVP for small α are hard, even for random lattices, with no subexponential-time algorithms. On the other hand, sampling efficiently from the discrete Gaussian distribution at the smoothing parameter is still an open problem, with no subexponential algorithm currently known. Therefore, we can view our result as an average-case hardness result for discrete Gaussian sampling (DGS) at the smoothing parameter. Plainly, solving DGS at the smoothing parameter in subexponential time for random lattices would have a major impact in lattice-based cryptography.

Approximate GapSVP The security of certain cryptographic primitives, such as fully homomorphic encryption [BV14], can be based on the *worst-case* hardness of a decision version of the approximate SVP problem, known as γ-GapSVP. This problem asks to decide, for a given $r > 0$, if a lattice $\mathcal{L}$ satisfies $\lambda_1(\mathcal{L}) \leqslant r$ or $\lambda_1(\mathcal{L}) \geqslant \gamma r$ (note that this is a promise problem). The hardness of this problem has been studied extensively as well and the best known result is a $2^{n/2+o(n)}$-time algorithm for 1.93-GapSVP [ADRS15].

In this paper, we study *random lattices*, therefore it is natural to wonder if γ-GapSVP remains hard in this setting. This should intuitively not be the case because by the "Gaussian Heuristic", the value of λ_1 for a random lattice is expected to be close to $\sqrt{\frac{n}{2\pi e}}\operatorname{vol}(\mathcal{L})^{1/n}$, which makes the problem easy to decide. We formally prove that this is the case by giving a polynomial-time algorithm (Theorem 3) that solves γ-GapSVP on most lattices, for any $\gamma > 1$. Although this is more of a folklore result, our theorem gives explicit constants and bounds not found in the literature.

Theorem 3 (Informal, see Theorem 10 and Corollary 6)**.** *There is an algorithm that, for every $\gamma > 1$, $n \geqslant 1$ and on most lattices $\mathcal{L} \subset \mathbb{R}^n$, solves γ-GapSVP in polynomial time.*

Organization of the paper Section 2 contains preliminary technical results. Section 3 gives some probabilistic bounds on the Gaussian mass and smoothing parameter of random real lattice. Section 4 give an application of those bounds to the approximate (Hermite) SVP. Section 5 contains some discussion and open problems.

2 Preliminaries

We denote vectors and matrices in bold case. We denote by $\mathbf{x}^T$ the transpose of the (column) vector $\mathbf{x}$, which is therefore a row vector. For any vector $\mathbf{x} \in \mathbb{R}^n$, we denote by $\|\mathbf{x}\|$ its Euclidean norm. For any $n \geqslant 1$ and $r > 0$, we denote by B_n the open ball of radius 1 in $\mathbb{R}^n$, and by $B_n(r)$ the open ball of radius r.

For any finite set X, we denote by $\mathcal{U}(X)$ the uniform distribution over X. As usual, if P and Q are two probability distributions over X and Y respectively, we denote by PQ the product distribution over $X \times Y$. For any two distributions P and Q, we denote by $\mathrm{d_{TV}}(P, Q)$ the statistical distance (or total variation distance) between P and Q. We say that two distributions P and Q are ε-close if $\mathrm{d_{TV}}(P, Q) \leqslant \varepsilon$.

We denote by ζ the Riemann zeta function, defined for any $s > 1$ by $\zeta(s) = \sum_{k=1}^{\infty} k^{-s}$. Furthermore, it is standard that

$$\zeta(s) - 1 \sim_{s\to\infty} 2^{-s} \tag{1}$$

2.1 Gamma function

We denote by Γ the gamma function, defined for any $a > 0$ by

$$\Gamma(a) = \int_0^{\infty} t^{a-1} e^{-t} \mathrm{d}\, t.$$

Furthermore, we denote by γ the lower incomplete gamma function, defined for any $a > 0$ and $s \geqslant 0$ by

$$\gamma(a, x) = \int_0^{x} t^{a-1} e^{-t} \mathrm{d}\, t.$$

We will make use of the following series expansion[†] for any $a > 0$ and $s \geqslant 0$:

$$\gamma(a, x) = x^a e^{-x} \sum_{k=0}^{\infty} \frac{x^k}{(a)_{k+1}}$$

where $(a)_n = a(a+1)\cdots(a+n-1)$ is Pochhammer's symbol. We easily derive from this that for all $a > 0$ and $x \geqslant 0$,

$$\gamma(a, x) \geqslant \frac{x^a e^{-x}}{a}. \tag{2}$$

We will also use the following bound on Γ [Rob55]: for $x > 0$,

$$\Gamma(1 + x) \leqslant \sqrt{2\pi} x^{x+\frac{1}{2}} e^{-x+\frac{1}{12x}}. \tag{3}$$

2.2 Lambert W function

Recall that the Lambert W function is a multivalued function giving the complex solution(s) w to the equation $we^w = z$. In this paper we will only deal with real numbers. It can be shown that for any $x, y \in \mathbb{R}$, the equation

$$ye^y = x$$

can only be solved (for y) if $x \geqslant -\frac{1}{e}$. For negative numbers $x < 0$, this equation has exactly two solutions $y = W_0(x)$ and $y = W_{-1}(x)$, where W_0 and W_{-1} are the two real branches of the W function. It is known that W_0 is an increasing function while W_{-1} is a decreasing function. Furthermore, for $x \in [-\frac{1}{e}, 0)$, $W_{-1}(x) \leqslant -1 \leqslant W_0(x)$. We will also use the fact that the map $x \in [0, 1] \mapsto xe^{1-x}$ is increasing.

[†]See for example: https://en.wikipedia.org/wiki/Incomplete_gamma_function.

2.3 Lattices

A *lattice* $\mathcal{L}$ is a discrete subgroup of $\mathbb{R}^m$. Equivalently it is the set

$$\mathcal{L}(\mathbf{b}_1, \dots, \mathbf{b}_n) = \left\{ \sum_{i=1}^{n} x_i \mathbf{b}_i \ : \ x_i \in \mathbb{Z} \right\}$$

of all integer combinations of n linearly independent vectors $\mathbf{b}_1, \dots, \mathbf{b}_n \in \mathbb{R}^m$. Such $\mathbf{b}_i$'s form a *basis* of $\mathcal{L}$ and are usually collected in matrix form $\begin{bmatrix} \mathbf{b}_1 & \cdots & \mathbf{b}_n \end{bmatrix}$. The lattice $\mathcal{L}$ is said to be *full-rank* if $n = m$. We denote by $\lambda_1(\mathcal{L})$ the first minimum of $\mathcal{L}$, defined as the length of a shortest non-zero vector of $\mathcal{L}$. We denote by $\mathrm{vol}(\mathcal{L})$ the volume (or determinant) of $\mathcal{L}$. For a full-rank lattice $\mathcal{L}$, $\mathrm{vol}(\mathcal{L}) = \det(\mathbf{A})$ for any basis $\mathbf{A}$ of $\mathcal{L}$. Recall that for two lattices $\mathcal{L} \subseteq \mathcal{L}'$, the *index* of $\mathcal{L}$ in $\mathcal{L}'$ is the size of the quotient $\mathcal{L}' / \mathcal{L}$.

For a rank n lattice $\mathcal{L} \subset \mathbb{R}^m$, the *dual lattice*, denoted $\widehat{\mathcal{L}}$, is defined as the set of all points in $\mathrm{span}(\mathcal{L})$ that have integer inner products with all lattice points,

$$\widehat{\mathcal{L}} = \{\mathbf{w} \in \mathsf{span}(\mathcal{L}) : \forall \mathbf{y} \in \mathcal{L}, \langle \mathbf{w}, \mathbf{y} \rangle \in \mathbb{Z}\}.$$

Similarly, for a lattice basis $\mathbf{B} = (\mathbf{b}_1, \dots, \mathbf{b}_n)$, we define the dual basis $\mathbf{B}^* = (\mathbf{b}_1^*, \dots, \mathbf{b}_n^*)$ to be the unique set of vectors in $\mathsf{span}(\mathcal{L})$ satisfying $\langle \mathbf{b}_i^*, \mathbf{b}_j \rangle = 1$ if $i = j$, and 0, otherwise. It is easy to show that $\widehat{\mathcal{L}}$ is itself a rank n lattice, that $\mathrm{vol}(\widehat{\mathcal{L}}) = \frac{1}{\mathrm{vol}(\mathcal{L})}$, and $\mathbf{B}^*$ is a basis of $\widehat{\mathcal{L}}$. Given a lattice $\mathbf{B} = (\mathbf{b}_1, \dots, \mathbf{b}_n)$, we denote $\| \mathbf{B} \|_2 = \max_i \|\mathbf{b}_i\|$. In this paper, all the lattices that we consider will be full rank, *i.e.* $n = m$.

2.4 Lattice problems

We will study the following lattice problems in this paper.

Definition 1. The search problem SVP (Shortest Vector Problem) is defined as follows: The input is a basis $\mathbf{B}$ for a lattice $\mathcal{L} \subset \mathbb{R}^n$. The goal is to output a vector $\mathbf{y} \in \mathcal{L}$ with $\|\mathbf{y}\| = \lambda_1(\mathcal{L})$.

Definition 2. For $\gamma = \gamma(n)$, the search problem γ-SVP (γ-Approximate Shortest Vector Problem) is defined as follows: The input is a basis $\mathbf{B}$ for a lattice $\mathcal{L} \subset \mathbb{R}^n$. The goal is to output a vector $\mathbf{y} \in \mathcal{L} \setminus \{0\}$ with $\|\mathbf{y}\| \leqslant \gamma \cdot \lambda_1(\mathcal{L})$.

Definition 3. For $\gamma = \gamma(n)$, the search problem γ-HSVP (γ-Hermite Approximate Shortest Vector Problem) is defined as follows: The input is a basis $\mathbf{B}$ for a lattice $\mathcal{L} \subset \mathbb{R}^n$. The goal is to output a vector $\mathbf{y} \in \mathcal{L} \setminus \{0\}$ with $\|\mathbf{y}\| \leqslant \gamma \cdot \det(\mathcal{L})^{1/n}$.

Definition 4. For $\gamma = \gamma(n)$, the decision problem γ-GapSVP (γ-Approximate Gap SVP) is defined as follows: The input is a basis $\mathbf{B}$ for a lattice $\mathcal{L} \subset \mathbb{R}^n$ and a real number $r > 0$. The goal is to accept if $\lambda_1(\mathcal{L}) \leqslant r$ and reject if $\lambda_1(\mathcal{L}) \geqslant \gamma r$. Note that this is a promise problem: the program may accept or reject if neither condition holds.

For convenience reasons, when we discuss the running time of the algorithms solving the problems above, we ignore polynomial factors in the bit-length of the individual input basis vectors (i.e. we assume the input basis has bit-size polynomial in the ambient dimension n).

2.5 Discrete Gaussian distribution

Let $n \in \mathbb{N}$ and $s > 0$. For any $\mathbf{x} \in \mathbb{R}^n$, we let

$$\rho_s(\mathbf{x}) = e^{-\pi \|\mathbf{x}\|^2 / s^2}.$$

As usual, we extend ρ_s to sets by

$$\rho_s(X) = \sum_{\mathbf{x}\in X} \rho_s(\mathbf{x})$$

for any set X. For any lattice $\mathcal{L} \subset \mathbb{R}^n$, we denote the *discrete Gaussian distribution* over $\mathcal{L}$ by $D_{\mathcal{L},s}(\mathbf{x}) = \frac{\rho_s(\mathbf{x})}{\rho_s(\mathcal{L})}$ for any $\mathbf{x} \in \mathcal{L}$. We denote $D_{\mathcal{L},1}$ by $D_{\mathcal{L}}$ for simplicity. It is well-known by the Poisson summation formula that for any lattice $\mathcal{L}$ and any $s > 0$,

$$\rho_{1/s}(\widehat{\mathcal{L}}) = \frac{s^{-n}}{\mathrm{vol}(\mathcal{L})}\rho_s(\mathcal{L}).$$

See e.g. [Ste17] for a good introduction on this topic. The discrete Gaussian distribution plays an essential role in lattice-based cryptography and an important problem is to be able to sample efficiently from it: this is known as the *discrete Gaussian sampling (DGS)* problem.

Definition 5. For $\delta = \delta(n) \geq 0$, σ a function that maps lattices to non-negative real numbers, and $m = m(n) \in \mathbb{N}$, δ-DGS_σ^m is defined as follows. The input is a basis $\mathbf{B}$ for a lattice $\mathcal{L} \subset \mathbb{R}^n$ and a parameter $s > \sigma(\mathcal{L})$. The goal is to output a sequence of m vectors whose joint distribution is δ-close to m independent samples from $D_{\mathcal{L},s}$.

We omit the parameter δ if $\delta = 0$, and the parameter m if $m = 1$. We stress that δ bounds the statistical distance between the *joint* distribution of the output vectors and m independent samples from $D_{\mathcal{L},s}$.

In general, the smaller s is, the harder it is to construct a sampler for $D_{\mathcal{L},s}$. The notion of smoothing parameter [MR04] captures the idea that sampling for a value of s above this threshold is significantly easier than sampling below because the distribution looks more like a continuous Gaussian. Formally, for any $\varepsilon > 0$, the smoothing parameter of a lattice $\mathcal{L}$ is defined by

$$\eta_\varepsilon(\mathcal{L}) = \inf\Big\{ s > 0 : \rho_{1/s}(\widehat{\mathcal{L}}) \leqslant 1 + \varepsilon \Big\}.$$

Observe that $\eta_\varepsilon(\mathcal{L})$ is a decreasing function of ε.

There are many algorithms to sample above the smoothing parameter [Kle00, GPV08, BLP+13], including a time-space trade-off [ACKS21]. Sampling below the smoothing parameter is much more challenging and usually inefficient [ADRS15]. At the extreme, sampling for sufficiently small values of s allows one to solve the Shortest Vector problem (SVP) [ADRS15] which is known to be NP-hard under randomized reduction [Ajt98]. The Monte Carlo Markov Chain based algorithm of [WL19] works for all values of s but the complexity significantly depends on s and the shape of the basis [PS24]. Finally, it should be noted that the problem of estimating the smoothing parameter is provably harder than BDD and LWE in certain parameter ranges [CDLP13].

In this paper, we will use the following sampler that works (almost) up to the smoothing parameter and takes time $2^{n/2+o(n)}$ to produce a sample.

Theorem 4 ([ADRS15, Theorem 5.11])**.** *There is a probabilistic algorithm that, given a lattice $\mathcal{L} \subset \mathbb{R}^n$ and $s \geq \sqrt{2}\eta_{1/2}(\mathcal{L})$ as input, outputs $2^{n/2}$ samples from a distribution $2^{-\Omega(n^2)}$-close to $D_{\mathcal{L},s}$ in expected time $2^{n/2+o(n)}$.*

2.6 Random real lattices

Recall that a lattice L is the integer span of a real basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ in $\mathbb{R}^n$. If $\mathbf{B}$ is the matrix whose columns are the $\mathbf{b}_i$, then $L = \mathbf{B}\mathbb{Z}^n$. The classical approach to defining a probability on the real lattices is the following. First we usually consider lattices modulo

scales, so that L and αL are equivalent for any $\alpha \in \mathbb{R}$. Therefore, a lattice is represented by an invertible matrix of determinant 1, that is an element of $\mathrm{SL}_n(\mathbb{R})$. Second, it is clear that many matrices in $\mathrm{SL}_n(\mathbb{R})$ span the same lattice: for instance permuting columns or changing the sign of an even number of columns. In general, matrices $\mathbf{B} \in \mathrm{SL}_n(\mathbb{R})$ and $\mathbf{B}U$ spans the same lattice for any $U \in \mathrm{SL}_n(\mathbb{Z})$. The converse is also true and hence we wish to define a probability measure on the homogenous space $X_n := \mathrm{SL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{Z})$.

Let μ be a measure on X_n, Y be a measurable set of lattices in X_n and $\mathbf{B} \in \mathrm{SL}_n(\mathbb{Z})$: a natural measure μ should assign the same probability to Y and $\mathbf{B}Y$ since those are the same lattices up to the change of basis. Therefore, μ should be (left) $\mathrm{SL}_n(\mathbb{Z})-$invariant: $\mu(Y) = \mu(\mathbf{B}Y)$. Furthermore, X_n inherits the natural topology of $\mathbb{R}^{n^2}$ through the quotient and we want the open sets to be measurable, therefore μ should be a Borel measure. Such a measure is called a (left-)invariant Haar measure and Siegel showed [Sie45] that it is unique up to a multiplicative factor. We are interested in the unique one which is a probability measure ($\mu(X_n) = 1$) which we denote by μ_n.

In this paper, we will identity the set of lattices modulo scaling and the set X_n. This means that we will view an element of X_n either as a lattice or as matrix of determinant of 1, depending on what is more convenient. We also note that the map $X_n \to X_n, \mathcal{L} \mapsto \widehat{\mathcal{L}}$ preserves μ_n so that if $\mathcal{L}$ is distributed according to μ_n then so is its dual $\widehat{\mathcal{L}}$.

The above measure was introduced by Siegel in [Sie45] who proved the following averaging theorem.

Theorem 5 (Siegel [Sie45])**.** *Let $n \geqslant 1$ and f be a Lebesgue integrable function on $\mathbb{R}^n$, then*

$$\int_{X_n} \sum_{\mathbf{x} \in \mathcal{L} \setminus \{0\}} f(\mathbf{x}) \mathrm{d}\,\mu_n(\mathcal{L}) = \int_{\mathbb{R}^n} f(\mathbf{x}) \mathrm{d}\,\lambda(\mathbf{x}).$$

where λ denotes the usual Lebesgue measure on $\mathbb{R}^n$

This result was later generalized (Theorem 6) by Rogers [Rog55], and the presentation simplified in [MR58] which is probably the most readable reference on the topic. It should be noted that a gap was recently found in the original proof of Rogers but fortunately the result still holds [Kim24].

For any $\ell \leqslant n$, we say that a matrix $M \in \mathbb{Z}^{n \times \ell}$ is *primitive* if $n - \ell$ columns can be added to it to make up a unimodular matrix. Equivalently, a matrix is primitive if its columns form a primitive set of vectors for $\mathbb{Z}^n$, *i.e.* this set can be extended to form an integer basis of $\mathbb{Z}^n$. Let $\mathrm{PR}_{n,\ell} \subset \mathbb{Z}^{n \times \ell}$ be the set of primitive matrices and $\mathrm{LI}_{n,\ell} \subset \mathbb{Z}^{n \times \ell}$ be the set of matrices whose columns are linearly independent. Macbeath and Rogers' theorem can be stated as follows. Here, recall again that we identify elements of X_n as both lattices modulo scale, or matrices of determinant 1.

Theorem 6 ([MR58, Theorems 1, 2 and (13)])**.** *Let $1 \leqslant \ell \leqslant n-1$ and f be Lebesgue integrable on $\mathbb{R}^{n \times \ell}$, then*

$$\begin{aligned}\int_{X_n} \sum_{\mathbf{M} \in \mathrm{LI}_{n,\ell}} f(\mathbf{A}\mathbf{M}) \mathrm{d}\,\mu(\mathbf{A}) &= \zeta(n) \cdots \zeta(n-\ell+1) \int_{X_n} \sum_{\mathbf{P} \in \mathrm{PR}_{n,\ell}} f(\mathbf{A}\mathbf{P}) \mathrm{d}\,\mu(\mathbf{A}) \\ &= \int_{\mathbb{R}^{n \times \ell}} f(X) \mathrm{d}\,\lambda(X).\end{aligned}$$

It is clear that this theorem implies Siegel's theorem when $\ell = 1$ since the set of linearly independent points of $\mathcal{L}$ is exactly $\mathcal{L} \setminus \{0\}$. In fact, the result about linearly independent vectors follows easily from the statement about primitive matrices which is the main technical result of [MR58]. In this paper, we will only make use of the following special case.

Recall that a vector $\mathbf{x} \in \mathbb{Z}^n$ is primitive if and only if $\mathbf{x} \in \mathrm{PR}_{n,1}$. One can check that this is equivalent to saying that $\frac{1}{\alpha}\mathbf{x} \notin \mathbb{Z}^n$ for all integers $\alpha \geqslant 2$, *i.e.* $\mathbf{x}$ is not an integer multiple of an integer vector (except by multiplying by 1 and -1).

Corollary 1. *Let $n \geqslant 2$ and f be Lebesgue integrable on $\mathbb{R}^{n\times\ell}$, then*

$$\int_{X_n} \sum_{\mathbf{x}\in\mathcal{L}} f(\mathbf{x}) \mathrm{d}\,\mu_n(\mathcal{L}) = f(0) + \int_{\mathbb{R}^n} f(\mathbf{x}) \mathrm{d}\,\lambda(\mathbf{x}),$$

$$\int_{X_n} \left(\sum_{\mathbf{x}\in\mathcal{L}} f(\mathbf{x})\right)^2 \mathrm{d}\,\mu_n(\mathcal{L}) = \left(\int_{X_n} \sum_{\mathbf{x}\in\mathcal{L}} f(\mathbf{x}) \mathrm{d}\,\mu_n(\mathcal{L})\right)^2 + \frac{1}{\zeta(n)} \sum_{\alpha\in\mathbb{N}\setminus\{0\}} \sum_{\beta\in\mathbb{Z}\setminus\{0\}} \int_{\mathbb{R}^n} f(\alpha\mathbf{x}) f(\beta\mathbf{x}) \mathrm{d}\,\lambda(\mathbf{x}).$$

Proof. The first inequality follows directly from Theorem 5:

$$\int_{X_n} \sum_{\mathbf{x}\in\mathcal{L}} f(\mathbf{x}) \mathrm{d}\,\mu_n(\mathcal{L}) = f(0) + \int_{X_n} \sum_{\mathbf{x}\in\mathcal{L}\setminus\{0\}} f(\mathbf{x}) \mathrm{d}\,\mu_n(\mathcal{L}) = f(0) + \int_{\mathbb{R}^n} f(\mathbf{x}) \mathrm{d}\,\lambda(\mathbf{x}).$$

For the second equality, first observe that

$$\int_{X_n} \left(\sum_{\mathbf{x}\in\mathcal{L}} f(\mathbf{x})\right)^2 \mathrm{d}\,\mu_n(\mathcal{L}) = \int_{X_n} \sum_{\mathbf{x},\mathbf{y}\in\mathcal{L}} f(\mathbf{x}) f(\mathbf{y}) \mathrm{d}\,\mu_n(\mathcal{L}).$$

Now let $g : \mathbb{R}^{n\times 2} \to \mathbb{R}$ be defined by $g(\begin{bmatrix}\mathbf{x} & \mathbf{y}\end{bmatrix}) = f(\mathbf{x})f(\mathbf{y})$ which is clearly Lebesgue integrable. Let $\mathcal{L} \in X_n$ be a lattice and $\mathbf{A}$ be a basis of $\mathcal{L}$. Then

$$\sum_{\mathbf{x},\mathbf{y}\in\mathcal{L}} f(\mathbf{x})f(\mathbf{y}) = \sum_{\mathbf{u},\mathbf{v}\in\mathbb{Z}^n} f(\mathbf{A}\mathbf{u})f(\mathbf{A}\mathbf{v}) = \sum_{\mathbf{u},\mathbf{v}\in\mathbb{Z}^n} g(\mathbf{A}\begin{bmatrix}\mathbf{u} & \mathbf{v}\end{bmatrix}).$$

Now there are three cases for $\mathbf{u}$ and $\mathbf{v}$: either $\mathbf{u} = \mathbf{v} = 0$; or $\mathbf{u}$ and $\mathbf{v}$ are linearly independent *i.e.* $\begin{bmatrix}\mathbf{u} & \mathbf{v}\end{bmatrix} \in \mathrm{LI}_{n,2}$; or $\mathbf{u} = 0$ and $\mathbf{v} \neq 0$; or they are linearly dependent and both non zero. The last case is the most interesting: it is not hard to see that if $\mathbf{u}, \mathbf{v} \in \mathbb{Z}^n \setminus \{0\}$ are linearly dependent, then $\mathbf{u} = \alpha\mathbf{p}$ and $\mathbf{v} = \beta\mathbf{p}$ for some unique primitive vector $\mathbf{p} \in \mathbb{Z}^n$, unique $\alpha \in \mathbb{N} \setminus \{0\}$ and unique $\beta \in \mathbb{Z} \setminus \{0\}$. Since $\mathbf{p}$, α and β are unique, and that conversely the vectors $\alpha\mathbf{p}$ and $\beta\mathbf{p}$ are always linearly dependent and nonzero, there is a bijection between

$$\left\{(\mathbf{u}, \mathbf{v}) \in (\mathbb{Z}^n \setminus \{0\})^2 : \text{linearly dependent}\right\}$$

and

$$\{(\alpha\mathbf{p}, \beta\mathbf{p}) : \mathbf{p} \in \mathbb{Z}^n \text{ primitive}, \alpha \in \mathbb{N} \setminus \{0\}, \beta \in \mathbb{Z} \setminus \{0\}\}.$$

Therefore,

$$\begin{aligned}
&\sum_{\mathbf{x},\mathbf{y}\in\mathcal{L}} f(\mathbf{x})f(\mathbf{y}) \\
&= f(0)^2 + \sum_{\mathbf{M}\in\mathrm{LI}_{n,2}} g(\mathbf{A}\mathbf{M}) + 2f(0) \sum_{\mathbf{v}\in\mathbb{Z}^n\setminus\{0\}} f(\mathbf{A}\mathbf{v}) \\
&\quad + \sum_{\mathbf{p}\in\mathbb{Z}^n:\text{prim.}} \sum_{\alpha\in\mathbb{N}\setminus\{0\}} \sum_{\beta\in\mathbb{Z}\setminus\{0\}} f(\mathbf{A}\alpha\mathbf{p}) f(\mathbf{A}\beta\mathbf{p}) \\
&= f(0)^2 + \sum_{\mathbf{M}\in\mathrm{LI}_{n,2}} g(\mathbf{A}\mathbf{M}) + 2f(0) \sum_{\mathbf{y}\in\mathcal{L}\setminus\{0\}} f(\mathbf{y})
\end{aligned}$$

$$+ \sum_{\alpha\in\mathbb{N}\setminus\{0\}} \sum_{\beta\in\mathbb{Z}\setminus\{0\}} \sum_{\mathbf{p}\in\mathbb{Z}^n:\text{prim.}} f(\alpha\mathbf{Ap})f(\beta\mathbf{Ap}).$$

The integral of the first term is trivial to compute since μ is chosen to be a probability measure. We can compute the middle term by Theorem 5:

$$\int_{X_n} f(0) \sum_{\mathbf{y}\in\mathcal{L}\setminus\{0\}} f(\mathbf{y})\mathrm{d}\,\mu_n(\mathcal{L}) = f(0)\int_{\mathbb{R}^n} f(\mathbf{x})\mathrm{d}\,\lambda(\mathbf{x}).$$

And the other two by Theorem 6:

$$\begin{aligned}\int_{X_n} \sum_{\mathbf{M}\in\mathrm{LI}_{n,2}} g(\mathbf{AM})\mathrm{d}\,\mu_n(\mathbf{A}) &= \int_{\mathbb{R}^{n\times 2}} g(\mathbf{M})\mathrm{d}\,\lambda(\mathbf{M})\\ &= \int_{\mathbb{R}^n}\int_{\mathbb{R}^n} f(\mathbf{x})f(\mathbf{y})\mathrm{d}\,\lambda(\mathbf{x})\mathrm{d}\,\lambda(\mathbf{y})\\ &= \left(\int_{\mathbb{R}^n} f(\mathbf{x})\mathrm{d}\,\lambda(\mathbf{x})\right)^2\end{aligned}$$

and

$$\begin{aligned}\int_{X_n} \sum_{\mathbf{p}\in\mathbb{Z}^n:\text{prim.}} f(\alpha\mathbf{Ap})f(\beta\mathbf{Ap})\mathrm{d}\,\mu_n(\mathbf{A}) &= \int_{X_n} \sum_{\mathbf{p}\in\mathrm{PR}_{n,1}} f(\alpha\mathbf{Ap})f(\beta\mathbf{Ap})\mathrm{d}\,\mu_n(\mathbf{A})\\ &= \tfrac{1}{\zeta(n)}\int_{\mathbb{R}^n} f(\alpha\mathbf{x})f(\beta\mathbf{x})\mathrm{d}\,\lambda(\mathbf{x}).\end{aligned}$$

Therefore,

$$\begin{aligned}\int_{X_n} \sum_{\mathbf{x},\mathbf{y}\in\mathcal{L}} f(\mathbf{x})f(\mathbf{y})\mathrm{d}\,\mu_n(\mathcal{L}) = f(0)^2 + 2f(0)\int_{\mathbb{R}^n} f(\mathbf{x})\mathrm{d}\,\lambda(\mathbf{x}) + \left(\int_{\mathbb{R}^n} f(\mathbf{x})\mathrm{d}\,\lambda(\mathbf{x})\right)^2\\ + \sum_{\alpha\in\mathbb{N}\setminus\{0\}}\sum_{\beta\in\mathbb{Z}\setminus\{0\}} \tfrac{1}{\zeta(n)}\int_{\mathbb{R}^n} f(\alpha\mathbf{x})f(\beta\mathbf{x})\mathrm{d}\,\lambda(\mathbf{x})\end{aligned}$$

which shows the result. □

The following result is a well-known consequence of Theorem 6. There are many ways to prove similar results, see e.g. [Rog56] or the survey [AEN]. Since we could not find a proof with explicit constants in both the length bound and the probability bound, we provide one for completeness.

Lemma 1. *Let $n \geqslant 2$ and $r > 0$, then*

$$\begin{aligned}\mathbb{E}_{\mathcal{L}\sim\mu_n}[|\,\mathcal{L}\cap B_n(r)|] &= 1 + \mathrm{vol}(B_n(r)),\\ \mathbb{V}_{\mathcal{L}\sim\mu_n}[|\,\mathcal{L}\cap B_n(r)|] &\leqslant 2A(n)\,\mathrm{vol}(B_n(r))\end{aligned}$$

where $A(n) := 1 + \frac{n}{n-1}\frac{\zeta(n-1)-1}{\zeta(n)} = 1 + 2^{1-n}(1+o(1))$ as $n\to\infty$.

Proof. Let f_r be the indicator function of the n-dimensional ball $B_n(r)$ of radius r. By Corollary 1, we have that

$$\mu_r := \mathbb{E}_{\mathcal{L}\sim\mu_n}[|\,\mathcal{L}\cap B_n(r)|] = 1 + \int_{\mathbb{R}^n} f_r(\mathbf{x})\mathrm{d}\,\lambda(\mathbf{x}) = 1 + \mathrm{vol}(B_n(r)).$$

and

$$\begin{aligned}\sigma_r^2 &:= \mathbb{V}_{\mathcal{L}\sim\mu_n}[|\,\mathcal{L}\cap B_n(r)|] \\ &= \frac{1}{\zeta(n)}\sum_{\alpha\in\mathbb{N}\setminus\{0\}}\sum_{\beta\in\mathbb{Z}\setminus\{0\}}\int_{\mathbb{R}^n} f_r(\alpha\mathbf{x})f_r(\beta\mathbf{x})\mathrm{d}\,\lambda(\mathbf{x}).\end{aligned}$$

But we observe that for any $\alpha \geqslant 1$ and $\beta \in \mathbb{Z}$, $f_r(\alpha\mathbf{x})f_r(\beta\mathbf{x}) = f_r(\max(\alpha,|\beta|)\mathbf{x})$. Therefore,

$$\begin{aligned}\sigma_r^2 &= \frac{1}{\zeta(n)}\sum_{\alpha\in\mathbb{N}\setminus\{0\}}\sum_{\beta\in\mathbb{Z}\setminus\{0\}}\int_{\mathbb{R}^n} f_r(\max(\alpha,|\beta|)\mathbf{x})\mathrm{d}\,\lambda(\mathbf{x}) \\ &= \frac{1}{\zeta(n)}\sum_{\alpha\in\mathbb{N}\setminus\{0\}}\sum_{\beta\in\mathbb{Z}\setminus\{0\}}\max(\alpha,|\beta|)^{-n}\operatorname{vol}(B_n(r)) \\ &= 2\frac{\operatorname{vol}(B_n(r))}{\zeta(n)}\sum_{\alpha\in\mathbb{N}\setminus\{0\}}\sum_{\beta\in\mathbb{N}\setminus\{0\}}\max(\alpha,\beta)^{-n}.\end{aligned}$$

We now observe that

$$\begin{aligned}&\sum_{\alpha\in\mathbb{N}\setminus\{0\}}\sum_{\beta\in\mathbb{N}\setminus\{0\}}\max(\alpha,\beta)^{-n} \\ &= \sum_{\alpha\in\mathbb{N}\setminus\{0\}}\left(\sum_{\beta=1}^{\alpha}\alpha^{-n}+(\alpha+1)^{-n}+\sum_{\beta=\alpha+2}^{\infty}\beta^{-n}\right) \\ &\leqslant \sum_{\alpha\in\mathbb{N}\setminus\{0\}}\left(\alpha^{1-n}+(\alpha+1)^{-n}+\int_{\alpha+1}^{\infty}x^{-n}\mathrm{d}\,x\right) \\ &= \zeta(n-1)+\zeta(n)-1+\sum_{\alpha\in\mathbb{N}\setminus\{0\}}\frac{(\alpha+1)^{1-n}}{n-1} \\ &= \zeta(n-1)+\zeta(n)-1+\frac{\zeta(n-1)}{n-1} \\ &= \zeta(n)+\tfrac{n}{n-1}(\zeta(n-1)-1).\end{aligned}$$

It follows that

$$\sigma_r^2 \leqslant 2\operatorname{vol}(B_n(r))\cdot(1+\tfrac{n}{n-1}\tfrac{\zeta(n-1)-1}{\zeta(n)}).$$

□

As a consequence, we can formalize what is usually known as the *Gaussian heuristic* which says that heuristically, a "random" lattice $\mathcal{L}\subset\mathbb{R}^n$ satisfies that $\lambda_1(\mathcal{L}) \approx \sqrt{\frac{n}{2\pi e}}\operatorname{vol}(\mathcal{L})^{1/n}$. For the notion of real random lattices that we use in this paper, the volume is always 1.

Theorem 7. *Let $n \geqslant 2$. For any $\alpha > 0$,*

$$\Pr_{\mathcal{L}\sim\mu_n}\left[\lambda_1(\mathcal{L}) \leqslant \alpha\operatorname{vol}(B_n)^{-1/n}\right]\begin{cases}\leqslant \frac{2\alpha^n A(n)}{(2-\alpha^n)^2} & \text{if } \alpha < 2^{1/n},\\ \geqslant 1-\frac{2\alpha^n A(n)}{(\alpha^n-2)^2} & \text{if } \alpha > 2^{1/n}.\end{cases}$$

where $A(n)$ is defined in Lemma 1.

Proof. By Lemma 1, we have that

$$\mu_r := \mathbb{E}_{\mathcal{L}\sim\mu_n}[|\,\mathcal{L}\cap B_n(r)|] = 1+\operatorname{vol}(B_n(r))$$

and

$$\sigma_r^2 := \mathbb{V}_{\mathcal{L}\sim\mu_n}[|\,\mathcal{L}\cap B_n(r)|] \leqslant 2A(n)\operatorname{vol}(B_n(r)).$$

It follows by Chebyshev's inequality that for any $X > 0$,

$$\Pr_{\mathcal{L}}\left[\left|\,|\,\mathcal{L}\cap B_n(r)| - \mu_r\right| > X\right] \leqslant \frac{\sigma_r^2}{X^2}.$$

We apply the above inequality to study λ_1. Observe that for any $r > 0$, $\lambda_1(\mathcal{L}) \leqslant r$ if and only if $|\,\mathcal{L}\cap B_n(r)| \geqslant 3$ since as soon as there is a nonzero vector, there are at least two (a point and its opposite), as the origin is in every ball. Assume that $\mu_r \leqslant 3$, *i.e.* $r^n \operatorname{vol}(B_n) \leqslant 2$. Then we can let $X = 3 - \mu_r$ and apply the above inequality to get that

$$\begin{aligned}
\Pr_{\mathcal{L}}[\lambda_1(\mathcal{L}) \leqslant r] &= \Pr_{\mathcal{L}}[|\,\mathcal{L}\cap B_n(r)| \geqslant 3] \\
&= \Pr_{\mathcal{L}}[|\,\mathcal{L}\cap B_n(r)| - \mu_r \geqslant X] \\
&\leqslant \Pr_{\mathcal{L}}\left[\left|\,|\,\mathcal{L}\cap B_n(r)| - \mu_r\right| \geqslant X\right] \\
&\leqslant \frac{\sigma_r^2}{X^2}.
\end{aligned}$$

If we let r_0 be such that $\operatorname{vol}(B_n(r_0)) = 1$ and write $r = \alpha r_0$ then

$$\sigma_r^2 = 2\operatorname{vol}(B_n(\alpha r_0))A(n) = 2\alpha^n A(n)$$

where $A(n) := 1 + \frac{n}{n-1}\frac{\zeta(n-1)-1}{\zeta(n)}$, and at the same time

$$X = 3 - \mu_r = 2 - \operatorname{vol}(B_n(\alpha r_0)) = 2 - \alpha^n.$$

Finally, we check that the condition $\mu_r \geqslant 3$ is equivalent to $\alpha^n < 2$.

Conversely, let $Y = \mu_r - 3$ and assume that $Y > 0$, *i.e.* $\alpha^n > 2$. If $\left|\,|\,\mathcal{L}\cap B_n(r)| - \mu_r\right| \leqslant Y$ then in particular $\mu_r - |\,\mathcal{L}\cap B_n(r)| \leqslant Y$ so $|\,\mathcal{L}\cap B_n(r)| \geqslant \mu_r - Y = 3$. Hence,

$$\begin{aligned}
\Pr_{\mathcal{L}}[\lambda_1(\mathcal{L}) \leqslant r] &= \Pr_{\mathcal{L}}[|\,\mathcal{L}\cap B_n(r)| \geqslant 3] \\
&\geqslant \Pr_{\mathcal{L}}\left[\left|\,|\,\mathcal{L}\cap B_n(r)| - \mu_r\right| \leqslant Y\right] \\
&= 1 - \Pr_{\mathcal{L}}\left[\left|\,|\,\mathcal{L}\cap B_n(r)| - \mu_r\right| > Y\right] \\
&\geqslant 1 - \frac{\sigma_r^2}{Y^2}.
\end{aligned}$$

□

3 On the Gaussian mass of random lattices

In this section, we give a probabilistic estimate of the value of $\rho_s(\mathcal{L})$ when $\mathcal{L}$ is a random real lattice. We derive from this a probabilistic bound on the smoothing parameter of a random lattice. A similar result was shown for "standard" random q-ary lattices (i.i.d. from uniform entries) in [LLBS14, Lemma 3] but only gives the expected value, whereas we also bound the variance. A closely related result is available in [KNSW20] which studies matrices with each entry independently and identically distributed from an integer Gaussian distribution. Similarly, [CPS+20, Appendix A], [LPR13, Section 7] and [SS11, Theorem 2] analyzes the Gaussian mass of a random q-ary lattice over cyclotomic fields.

Recall that by random real lattice, we mean $\mathcal{L} \in X_n$ distributed according to μ_n, *i.e.* the Haar measure. See Section 2.6 for more details. Our first technical result is to obtain the expected value and variance of $\rho_s(\mathcal{L})$ for a random lattice $\mathcal{L}$. We derive from this a probabilistic bound on $\rho_s(\mathcal{L})$ and the smoothing parameter. For reasont that will become clear in the proof of Theorem 8, we prove a more general result on $\rho_s(\mathcal{L}\cap B_n(\ell))$, *i.e.* the Gaussian mass of a lattice restricted to a ball.

Lemma 2. *For any $n \in \mathbb{N}$, $\ell > 0$ and $s > 0$, let $\mathcal{L} \in X_n$ be distributed according to μ_n. Then*

$$\mathbb{E}_{\mathcal{L}}[\rho_s(\mathcal{L} \cap B_n(\ell))] = 1 + s^n\theta, \qquad \mathbb{V}_{\mathcal{L}}[\rho_s(\mathcal{L} \cap B_n(\ell))] \leqslant As^n\theta$$

where $A = \frac{2}{\zeta(n)} \sum_{\alpha,\beta=1}^{\infty} (\alpha^2+\beta^2)^{-n/2} \leqslant 2^{1-n/2}(1+o(1))$ and $\theta = \frac{\gamma(n/2, \pi\ell^2/s^2)}{\Gamma(n/2)}$ where γ denotes the lower incomplete gamma function. In particular,

$$\mathbb{E}_{\mathcal{L}}[\rho_s(\mathcal{L})] = 1 + s^n, \qquad \mathbb{V}_{\mathcal{L}}[\rho_s(\mathcal{L})] \leqslant As^n.$$

Proof. Let f_ℓ be the identify function of $B_n(\ell)$. By Corollary 1, we have that

$$\mathbb{E}_{\mathcal{L}}[\rho_s(\mathcal{L} \cap B_n(\ell))] = \rho_s(0) + \int_{\mathbb{R}^n} \rho_s(\mathbf{x}) f_\ell(\mathbf{x}) \mathrm{d}\,\lambda(\mathbf{x}).$$

To compute this integral, we perform a polar change of coordinate. Let σ^n denote the spherical measure of the n-sphere S^n. Then

$$\begin{aligned}
&\int_{\mathbb{R}^n} \rho_s(\mathbf{x}) f_\ell(\mathbf{x}) \mathrm{d}\,\lambda(\mathbf{x}) \\
&= \int_{S^{n-1}} \int_0^\ell e^{-\pi\frac{r^2}{s^2}} r^{n-1} \mathrm{d}\,r \mathrm{d}\,\sigma^{n-1}(\omega) \\
&= \sigma^{n-1}(S^{n-1}) \int_0^\ell e^{-\pi\frac{r^2}{s^2}} r^{n-1} \mathrm{d}\,r \\
&= \frac{2\pi^{n/2}}{\Gamma(\frac{n}{2})} \int_0^{\pi\frac{\ell^2}{s^2}} e^{-t} \left(s\sqrt{\tfrac{t}{\pi}}\right)^{n-2} \frac{s^2}{2\pi} \mathrm{d}\,t \qquad \text{by the change } t = \pi\tfrac{r^2}{s^2} \\
&= \frac{s^n}{\Gamma(\frac{n}{2})} \int_0^{\pi\frac{\ell^2}{s^2}} e^{-t} t^{\frac{n}{2}-1} \mathrm{d}\,t \\
&= s^n \frac{\gamma(\frac{n}{2}, \pi\frac{\ell^2}{s^2})}{\Gamma(\frac{n}{2})}.
\end{aligned}$$

By Corollary 1, and a similar integral calculation, we also have that

$$\begin{aligned}
&\mathbb{V}_{\mathcal{L}\sim\mu_n}[\rho_s(\mathcal{L} \cap B_n(\ell))] \\
&= \frac{1}{\zeta(n)} \sum_{\alpha\in\mathbb{N}\setminus\{0\}} \sum_{\beta\in\mathbb{Z}\setminus\{0\}} \int_{\mathbb{R}^n} \rho_s(\alpha\mathbf{x})\rho_s(\beta\mathbf{x}) f_\ell(\alpha\mathbf{x}) f_r(\beta\mathbf{x}) \mathrm{d}\,\lambda(\mathbf{x}) \\
&= \frac{1}{\zeta(n)} \sum_{\alpha\in\mathbb{N}\setminus\{0\}} \sum_{\beta\in\mathbb{Z}\setminus\{0\}} \int_{\mathbb{R}^n} \rho_{s/\sqrt{\alpha^2+\beta^2}}(\mathbf{x}) f_\ell(\max(\alpha, |\beta|)\mathbf{x}) \mathrm{d}\,\lambda(\mathbf{x}) \\
&= 2\frac{s^n}{\zeta(n)} \sum_{\alpha,\beta=1}^{\infty} (\alpha^2+\beta^2)^{-n/2} \frac{\gamma\left(\frac{n}{2}, \pi\frac{\ell^2}{s^2\max(\alpha^2,\beta^2)}\right)}{\Gamma(\frac{n}{2})} \\
&\leqslant 2\frac{s^n}{\zeta(n)} \sum_{\alpha,\beta=1}^{\infty} (\alpha^2+\beta^2)^{-n/2} \frac{\gamma\left(\frac{n}{2}, \pi\frac{\ell^2}{s^2}\right)}{\Gamma(\frac{n}{2})} \quad \text{since } \gamma(\tfrac{n}{2}, \cdot) \text{ is increasing} \\
&= 2\frac{s^n}{\zeta(n)} \frac{\gamma(\frac{n}{2}, \pi\frac{\ell^2}{s^2})}{\Gamma(\frac{n}{2})} \sum_{\alpha,\beta=1}^{\infty} (\alpha^2+\beta^2)^{-n/2}.
\end{aligned}$$

Furthermore,

$$\sum_{\alpha,\beta=1}^{\infty} (\alpha^2+\beta^2)^{-n/2} = \sum_{\alpha=1}^{\infty} \left((\alpha^2+1)^{-n/2} + \sum_{\beta=2}^{\infty} (\alpha^2+\beta^2)^{-n/2} \right)$$

$$
\begin{aligned}
&\leqslant \sum_{\alpha=1}^{\infty}\left((\alpha+1)^{-n/2}+\sum_{\beta=2}^{\infty}(\alpha^2+\beta^2)^{-n/2}\right)\\
&\leqslant \zeta(\tfrac{n}{2})-1+\sum_{\alpha=1}^{\infty}\int_1^{\infty}(\alpha+\beta)^{-n/2}\mathrm{d}\,\beta\\
&= \zeta(\tfrac{n}{2})-1+\sum_{\alpha=1}^{\infty}2\frac{(\alpha+1)^{1-\frac{n}{2}}}{n-2}\\
&= \zeta(\tfrac{n}{2})-1+\tfrac{2}{n-2}(\zeta(\tfrac{n}{2}-1)-1)\\
&= 2^{-n/2}(1+o(1))
\end{aligned}
$$

as $n\to\infty$. The final part of the result follows by letting $\ell\to\infty$ and noting that $\theta\to 1$ since $\Gamma(\frac{n}{2})=\lim_{x\to\infty}\gamma(\frac{n}{2},x)$ by definition. □

Corollary 2. *For any $n\in\mathbb{N}$, $s>0$, $\ell>0$ and $\alpha>0$,*

$$\Pr_{\mathcal{L}\sim\mu_n}[|\rho_s(\mathcal{L}\cap B_n(\ell))-1-s^n\theta|>\alpha]\leqslant\frac{2^{1-n/2}s^n\theta(1+o_n(1))}{\alpha^2}$$

where θ is defined in Lemma 2 and $o_n(1)\to 0$ as $n\to\infty$ is independent of α and ℓ.

Proof. This is a direct application of Lemma 2 and Chebyshev's inequality. □

The previous lemma allows us to derive a probabilistic bound on the smoothing paragraph $\eta_\varepsilon(\mathcal{L})$ of a random lattice $\mathcal{L}$.

Corollary 3. *For any $n\in\mathbb{N}$ and $\varepsilon>0$, let $s_\varepsilon=\left(\frac{\varepsilon+1+\sqrt{2\varepsilon+1}}{\varepsilon^2}\right)^{1/n}$. Then*

$$\Pr_{\mathcal{L}\sim\mu_n}[\eta_\varepsilon(\mathcal{L})>s_\varepsilon]\leqslant 2^{-n/2}(1+o(1)).$$

Proof. Recall that if $\mathcal{L}\in X_n$ is distributed according to μ_n then its dual $\widehat{\mathcal{L}}$ is also distributed according to μ_n. Let $\alpha=\varepsilon-s_\varepsilon^{-n}$ and check that $\alpha>0$. We can therefore apply Corollary 2 to get that

$$
\begin{aligned}
\Pr_{\mathcal{L}}\left[\rho_{1/s_\varepsilon}(\widehat{\mathcal{L}})>1+\varepsilon\right] &= \Pr_{\mathcal{L}}\left[\rho_{1/s_\varepsilon}(\widehat{\mathcal{L}})-1-s_\varepsilon^{-n}>\alpha\right]\\
&\leqslant \Pr_{\mathcal{L}}\left[\left|\rho_{1/s}(\widehat{\mathcal{L}})-1-s_\varepsilon^{-n}\right|>\alpha\right]\\
&\leqslant \frac{2^{1-n/2}(1+o(1))}{s_\varepsilon^n\alpha^2}.
\end{aligned}
$$

A routine calculation shows that[‡] $s_\varepsilon^n\alpha^2=s_\varepsilon^n(\varepsilon-s_\varepsilon^{-n})^2=2$. Furthermore, for any lattice $\mathcal{L}$, if $\rho_{1/s_\varepsilon}(\widehat{\mathcal{L}})\leqslant 1+\varepsilon$ then $\eta_\varepsilon(\mathcal{L})\leqslant s_\varepsilon$. Therefore,

$$\Pr_{\mathcal{L}}[\eta_\varepsilon(\mathcal{L})>s_\varepsilon]\leqslant\Pr_{\mathcal{L}}\left[\rho_{1/s_\varepsilon}(\mathcal{L})>1+\varepsilon\right]\leqslant 2^{-n/2}(1+o(1)). \tag{4}$$

□

[‡]Technically, there is second choice $\tilde{s_\varepsilon}=\left(\frac{\varepsilon+1-\sqrt{2\varepsilon+1}}{\varepsilon^2}\right)^{1/n}$ which satisfies that $\tilde{s_\varepsilon}^n(\varepsilon-\tilde{s_\varepsilon}^{-n})^2=2$. However note that $\tilde{s_\varepsilon}\leqslant\varepsilon^{-1/n}$ so if we applied Corollary 2, we would get the probability that $\rho_{1/\tilde{s_\varepsilon}}(\widehat{\mathcal{L}})>1+\tilde{s_\varepsilon}^{-n}+\alpha$ for some positive $\alpha>0$, but since $1+\tilde{s_\varepsilon}^{-n}>1+\varepsilon$, this would not help us bound the smoothing parameter η_ε.

4 Application to the Hermite and approximate SVP

In this section, we use our probabilistic bound on the smoothing parameter $\eta_\varepsilon(\mathcal{L})$ to solve the approximate (Hermite) SVP for random lattices. Our algorithm is conceptually simple: we sample a large number of vectors from $D_{\mathcal{L},s}$ for $s = \sqrt{2}\eta_{1/2}(\mathcal{L})$ and we return the shortest nonzero vector among them. The trade-off lies in the number of samples: the more we have, the more likely we are to find a short vector but more expensive the algorithm becomes. The sampler that we used (Theorem 4) runs in time $2^{n/2+o(n)}$ but gives us $2^{n/2+o(n)}$ vectors at a time. Surprisingly, this already allows us to solve 1.123-SVP but by calling the sampler an exponential number of times, we can decrease the approximation factor and even solve SVP.

Theorem 8. *There is a randomized algorithm that for every $n \geqslant 1$ and $\beta \in (\beta_0, 1)$ where $\beta_0 := -W_0\left(-\frac{1}{4e}\right) \approx 0.1018284311$, and on a fraction at least $1 - 2^{-n/2+o(n)} - \frac{1}{X}$, where $X \geqslant (4\beta e^{1-\beta})^{n/2} > 1$, of random lattices $\mathcal{L}$ according to μ_n, outputs in time $e^{o(n)}(\beta e^{1-\beta})^{-n/2} + 2^{n/2+o(n)}$ and space $2^{n/2+o(n)}$ a nonzero vector of $\mathcal{L}$ of length at most $s_{1/2}\sqrt{\frac{n\beta}{\pi}}$ with probability at least $1/2$, where $s_{1/2} = (6+4\sqrt{2})^{1/n} = 1 + o(1)$ is defined in Corollary 3.*

Remark 1. Although this theorem can be applied up to $\beta = 1$, it is actually pointless to go beyond $\beta_{\max} = -W_0\left(-\frac{1}{2e}\right) \approx 0.2319609530$. Indeed, for $\beta = \beta_{\max}$, the time complexity of the algorithm is exactly $2^{n/2+o(n)}$ and it cannot become any smaller by increasing β.

Proof. Let $s_{1/2}$ be given by Corollary 3, $\sigma = \sqrt{2}s_{1/2}$, $\ell = s_{1/2}\sqrt{\frac{n\beta}{\pi}}$ and N to be fixed later. Consider the following algorithm:

- Sample N vectors independently according to $D_{\mathcal{L},\sigma}$ by Theorem 4.
- Return the shortest nonzero vector.

We will analyze this algorithm. First the running time is clear by Theorem 4 the algorithm takes time $(N + 2^{n/2}) \cdot 2^{o(n)}$. Next we observe that by Corollary 3 for $\varepsilon = 1/2$, and with probability at least $1 - 2^{-n/2}(1 + o(n))$ over the choice of $\mathcal{L}$ we have

$$\eta_{1/2}(\mathcal{L}) \leqslant s_{1/2}. \tag{5}$$

Furthermore, by Corollary 2 for $\alpha = \frac{1}{2}\sigma^n\theta$, and with probability at least $1 - \frac{2^{3-n/2}}{\sigma^n\theta}(1+o(n))$ over the choice of $\mathcal{L}$ we have

$$|\rho_s(\mathcal{L} \cap B_n(\ell)) - 1 - \sigma^n\theta| > \tfrac{1}{2}\sigma^n\theta \tag{6}$$

where $\theta = \frac{\gamma(n/2,\pi\ell^2/\sigma^2)}{\Gamma(n/2)}$. Finally, by the same argument, and with probability at least $1 - 2^{-n/2}(1 + o(n))$ over the choice of $\mathcal{L}$ we have

$$|\rho_s(\mathcal{L}) - 1 - \sigma^n| > \sqrt{2\sigma^n}. \tag{7}$$

By a union bound, we have that (5), (6) and (7) hold at the same time for a fraction at least $1 - 2^{-n/2+o(n)} - \frac{1}{X}$ of random lattices where $X = 2^{n/2-3}\sigma^n\theta(1 + o(n))$. Assume that we are in this case. It will be useful to note that $s_{1/2} = (6+4\sqrt{2})^{1/n}$. Therefore

$$11^{1/n} \leqslant s_{1/2} \leqslant 12^{1/n}.$$

Since $\sqrt{2}\eta_{1/2}(\mathcal{L}) \leqslant \sqrt{2}s_{1/2} = \sigma$ we can indeed apply Theorem 4 to sample from $D_{\mathcal{L},\sigma}$. Therefore, the probability that each sample is nonzero and of length at most ℓ is

$$p := \frac{\rho_\sigma(\mathcal{L} \setminus \{0\} \cap B_n(\ell))}{\rho_\sigma(\mathcal{L})} \geqslant \frac{\frac{1}{2}\sigma^n\theta}{1 + \sigma^n + \sqrt{2\sigma^n}} \qquad \text{by (6) and (7)}$$

$$\geqslant \frac{\frac{1}{2}\sigma^n\theta}{2\sigma^n} = \frac{\theta}{4} \qquad \text{since } \sigma^n \geqslant 4.$$

Therefore if we sample $N = \Omega(1/p)$ vector from $D_{\mathcal{L},\sigma}$, then with constant probability we will get a vector in $\mathcal{L}\setminus\{0\} \cap B_n(\ell)$.

We now need to obtain a lower bound on θ: let $a = n/2$ and $x = \pi\ell^2/\sigma^2$. Check that $x = \beta a$. Since $\beta \leqslant 1$, we have $x \leqslant a$ so

$$\begin{aligned}
\theta = \frac{\gamma(a,x)}{\Gamma(a)} &\geqslant \frac{\gamma(a,x)}{\Gamma(a+1)} \\
&\geqslant \frac{x^a e^{-x}}{a\cdot\sqrt{2\pi}a^{a+\frac{1}{2}}e^{-a+\frac{1}{12a}}} && \text{by (2) and (3)} \\
&= \frac{1}{a^{3/2}\sqrt{2\pi}}\left(\tfrac{x}{a}\right)^a e^{a-x-\frac{1}{12a}} \\
&= e^{o(n)}(\beta e^{1-\beta})^{n/2}.
\end{aligned}$$

Recall that this holds for a fraction at least $1 - 2^{-n/2+o(n)} - \frac{1}{X}$ of lattices, where

$$X = 2^{n/2-3}\sigma^n\theta \geqslant (4\beta e^{1-\beta})^{n/2}.$$

Recall (Section 2.2) that $\beta \in [0,1] \mapsto \beta e^{1-\beta}$ is increasing, and since $\beta > \beta_0$,

$$X > \left(4\beta_0 e^{1-\beta_0}\right)^{n/2} = 1$$

by elementary calculations involving the lambert W function. □

The previous result allows us to show that we have an algorithm that returns relatively short vectors on average but note that the bound does not depend on the lattice (more precisely, it is related to the volume of the lattice because our random lattices are scaled to have volume 1). This is known as the α-Hermite SVP (HSVP). The following corollary is a simplified version of Theorem 8.

Corollary 4. *There is a randomized algorithm that for every $n \geqslant 1$ and $\beta \in [\beta_1, \beta_{\max}]$ where $\beta_1 := -W_0\left(-\frac{\sqrt{2}}{4e}\right) \approx 0.1514 < \frac{1}{2e}$ and $\beta_{\max}$ is defined in Remark 1, solves $(1 + o(1))\sqrt{\frac{n\beta}{\pi}}$-HSVP in time $e^{o(n)}(\beta e^{1-\beta})^{-n/2}$ and space $2^{n/2+o(n)}$ with probability at least $1/2$ on a fraction at least $1 - 2^{-n/4+o(n)}$ of random lattices $\mathcal{L}$ according to μ_n.*

Proof. This is a direct consequence of Theorem 8 since $\beta_1 \geqslant \beta_0$ and $s_{1/2} \leqslant 12^{1/n} = 1+o(1)$. The only thing to check is that the fraction of lattices on which the algorithm succeeds. Recall (Section 2.2) that $\beta \in [0,1] \mapsto \beta e^{1-\beta}$ is increasing, and since $\beta \geqslant \beta_1$,

$$X \geqslant \left(4\beta_1 e^{1-\beta_1}\right)^{n/2} = 2^{n/4}$$

by elementary calculations involving the lambert W function. Finally, note that the time complexity is

$$e^{o(n)}(\beta e^{1-\beta})^{-n/2} + 2^{n/2+o(n)}$$

but by Remark 1, the first term is always larger than the second when $\beta \leqslant \beta_{\max}$. □

The more common γ-SVP problem asks to relate the length of the vectors to the first minimum $\lambda_1(\mathcal{L})$. To do so, we rely on a probabilistic lower bound on λ_1 for random lattices.

Theorem 9. *There is a randomized algorithm that for every $n \geqslant 1$, $\gamma \in [1, \sqrt{2e\beta_{\max}}]$ and $\beta \in (\beta_0, \frac{\gamma^2}{2e})$, where β_0 is defined in Theorem 8 and $\beta_{\max}$ is defined in Remark 1, solves γ-SVP in time $e^{o(n)}(\beta e^{1-\beta})^{-n/2}$ and space $2^{n/2+o(n)}$ with probability at least $1/2$ on a fraction at least $1 - (4\beta e^{1-\beta})^{-n/2} - e^{o(n)}\left(\frac{2e\beta}{\gamma^2}\right)^{n/2}$ of random lattices $\mathcal{L}$ according to μ_n.*

Remark 2. If we let $\beta \to \frac{\gamma^2}{2e}$ then the complexity of the algorithm will tend to $e^{o(n)}(\frac{\gamma^2}{2}e^{-\gamma^2/2e})^{-n/2}$ although in this case the algorithm will only succeed on a fraction $1 - \frac{1}{\mathsf{poly}(n)}$ of random lattices. In particular, for $\gamma = 1$ the complexity will be $2^{0.63269n+o(n)}$ and for $\gamma = \sqrt{2e\beta_{\max}} \approx 1.122973948$, the complexity will be $2^{n/2+o(n)}$.

Proof. Let $\beta \in (\beta_0, \beta_{\max})$ to be fixed later where $\beta_{\max}$ is defined in Remark 1. We apply Theorem 8 to get an algorithm that returns a nonzero vector on a lattice $\mathcal{L}$ with probability at least $1/2$ and of length at most $\ell = s_{1/2}\sqrt{\frac{n\beta}{\pi}}$, where $s_{1/2} = (6+4\sqrt{2})^{1/n} \leqslant 12^{1/n}$. This algorithm works on a fraction at least $1 - 2^{-n/2+o(n)} - \frac{1}{X}$ of lattices where $X = (4\beta e^{1-\beta})^{n/2}$.

Let $\alpha = \frac{\ell}{\gamma}\operatorname{vol}(B_n)^{1/n}$. Assuming for now that $\alpha < 2^{1/n}$, we apply Theorem 7 to get that for a fraction at least $1-\varepsilon$ of lattices, where $\varepsilon = \frac{2\alpha^n(1+o(1))}{(2-\alpha^n)^2}$, we have $\lambda_1(\mathcal{L}) \geqslant \alpha \operatorname{vol}(B_n)^{-1/n}$. Therefore, for a fraction at least $1 - \varepsilon - \frac{1}{X} - 2^{-n/2+o(n)}$ of lattices, the nonzero vector returned by the algorithm is of length at most

$$\ell = \gamma\alpha \operatorname{vol}(B_n)^{-1/n} \leqslant \gamma\lambda_1(\mathcal{L}).$$

Recall that we need to satisfy the constraint $\alpha < 2^{1/n}$. Check that

$$\begin{aligned}\alpha^n &\leqslant 12\left(\frac{n\beta}{\pi\gamma^2}\right)^{n/2}\operatorname{vol}(B_n)\\ &\sim 12\left(\frac{n\beta}{\pi\gamma^2}\right)^{n/2}\frac{1}{\sqrt{n\pi}}\left(\frac{2\pi e}{n}\right)^{n/2}\\ &= \frac{12}{\sqrt{n\pi}}\left(\frac{2e\beta}{\gamma^2}\right)^{n/2}.\end{aligned}$$

In particular, if $2e\beta < \gamma^2$ then $\alpha \to 0$ as $n \to \infty$ so the condition $\alpha < 2^{1/n}$ is clearly satisfied for large enough n. If we further restrict $\gamma \leqslant \gamma_{\max}$ so that $\gamma_{\max}^2/2e = \beta_{\max}$ then by Remark 1 we can simplify the time complexity as in the proof of Corollary 4. □

The previous theorem is difficult to use because of the parameter β which balances the complexity and the fraction of lattices on which the algorithm succeeds. The following corollary is a simplified version for a hardcoded fraction of lattices.

Corollary 5. *There is a randomized algorithm that for every $n \geqslant 1$ and $\gamma \in [1, \gamma_{\max}]$ where $\gamma_{\max} = \sqrt{2e\beta_{\max}} \approx 1.122973948$, solves γ-SVP and space $2^{n/2+o(n)}$ and time $\left(0.1821\gamma^2 e^{1-0.1821\gamma^2}\right)^{-n/2}$ with probability at least $1/2$ on a fraction at least $1 - 0.99^{n/2}$ of random lattices $\mathcal{L}$ according to μ_n.*

Proof. Apply Theorem 9 with $\beta = 0.99\frac{\gamma^2}{2e}$. Then it is clear that the fraction of lattices on which the algorithm works is $1 - 0.99^{n/2}$. Substituting into the runtime complexity gives the result. □

Finally, we observe that the strong bounds on λ_1 for a random lattices give a polynomial time algorithm for $(1+\varepsilon)$-GapSVP. Although this is more of a folklore result, our theorem gives explicit constants and bounds not found in the literature.

Theorem 10. *There is a deterministic algorithm that for any $n \geqslant 1$ and $\gamma = \gamma(n) > 2^{2/n}$, and on a fraction at least $1 - \epsilon - \epsilon'$ of random lattices according to μ_n, solves γ − GapSVP in polynomial time (independent of γ), where $\varepsilon = \frac{2\alpha^n A(n)}{(\alpha^n-2)^2}$, $\varepsilon' = \frac{2\beta^n A(n)}{(2-\beta^n)^2}$, $\alpha = \sqrt{\gamma}$ and $\beta = 1/\sqrt{\gamma}$ and $A(n)$ is defined in Theorem 7.*

Proof. The algorithm is trivial: on input $\mathcal{L} \subseteq \mathbb{R}^n$ and $r > 0$, accept if $\mathrm{vol}(B_n)^{-1/n} < r\sqrt{\gamma}$ and reject otherwise.

We now analyze the algorithm: let $\alpha = \sqrt{\gamma}$ and note that $\alpha > 2^{1/n}$. Apply Theorem 7 to get that for a fraction at least $1 - \varepsilon$ of lattices $\mathcal{L}$, where $\varepsilon = \frac{2\alpha^n A(n)}{(\alpha^n-2)^2}$, we have $\lambda_1(\mathcal{L}) \leqslant \alpha \,\mathrm{vol}(B_n)^{-1/n}$. Similarly, let $\beta = 1/\sqrt{\gamma}$ and note that $\beta < 2^{-1/n} < 2^{1/n}$. Therefore, for a fraction at least $1 - \varepsilon'$ of lattices $\mathcal{L}$, where $\varepsilon' = \frac{2\beta^n A(n)}{(2-\beta^n)^2}$, we have $\lambda_1(\mathcal{L}) > \beta \,\mathrm{vol}(B_n)^{-1/n}$. By a union bound, for a fraction at least $1 - \varepsilon - \varepsilon'$ of lattices $\mathcal{L}$, we have

$$\beta \,\mathrm{vol}(B_n)^{-1/n} < \lambda_1(\mathcal{L}) \leqslant \alpha \,\mathrm{vol}(B_n)^{-1/n}. \tag{8}$$

Assume that the input lattice satisfies (8) and let $r > 0$. There are two cases to consider:

- If $\lambda_1(\mathcal{L}) \leqslant r$ then $\mathrm{vol}(B_n)^{-1/n} < r/\beta = r\sqrt{\gamma}$ so the algorithm accepts.
- If $\lambda_1(\mathcal{L}) \geqslant \gamma r$ then $\mathrm{vol}(B_n)^{-1/n} \geqslant r\gamma/\alpha = r\sqrt{\gamma}$ so the algorithm rejects.

Therefore the algorithm solves γ-GapSVP on $\mathcal{L}$. The running time is clearly polynomial. □

Since the statement of Theorem 10 is quite hard to decipher, we give a weaker result in the case of a constant approximation factor, which can be arbitrarily close to 1.

Corollary 6. *There is a deterministic algorithm that for any $\gamma > 1$ solves γ-GapSVP for $n \geqslant \frac{4\ln 2}{\ln \gamma}$ in polynomial time (independent of γ) and on a fraction at least $1 - 10\gamma^{-n/2}(1 + o(1))$ of random lattices according to μ_n.*

Proof. Apply Theorem 10 with γ. Note that since $n \geqslant 4\ln(2)/\ln(\gamma)$, we have $\gamma \geqslant 4^{2/n} > 2^{2/n}$. Therefore the algorithm solves γ-GapSVP on a fraction at least $1 - \varepsilon - \varepsilon'$ of lattices. Now observe that $\alpha^n = \gamma^{n/2} > 4$, therefore[§]

$$\varepsilon = \frac{2\alpha^n A(n)}{(\alpha^n - 2)^2} \leqslant \frac{8A(n)}{\alpha^n} = 8\gamma^{-n/2}(1 + o(1)).$$

The bound of ε' is easier since $\beta = 1/\sqrt{\gamma} \leqslant 1$ so

$$\varepsilon' = \frac{2\beta^n A(n)}{(2 - \beta^n)^2} \leqslant 2\beta^n A(n) = 2\gamma^{-n/2}(1 + o(1)).$$

□

5 Discussion and open questions

We have shown a conceptually simple algorithm to solve SVP and HSVP for random lattices by discrete Gaussian sampling. Perhaps the most intriguing consequence of these results is that it implies that sampling from a discrete Gaussian at the smoothing parameter cannot be done in subexponential time (even for random lattices) without major consequences on lattice-based cryptography. This, however, does not quite settle the question of the exact complexity of DGS at the smoothing parameter. Indeed, all existing algorithms that run in time $2^{n/2+o(n)}$ use exponential space and it is open whether it is possible to

[§]We use that $\frac{x}{(x-2)^2} \leqslant \frac{4}{x}$ for $x \geqslant 4$ which follows by a simple analysis.

sample in subexponential space. If such an algorithm exists, it's not hard to see that all our algorithms will also run in subexponential space on random lattices.

Another open question concerns our probabilistic bound (Corollary 3) on $\eta_\varepsilon(\mathcal{L})$. Indeed, recall that for any $\varepsilon > 0$ we have shown that almost all lattices $\mathcal{L}$ satisfy that

$$\eta_\varepsilon(\mathcal{L}) \leqslant s_\varepsilon = \left(\frac{\varepsilon + 1 + \sqrt{2\varepsilon+1}}{\varepsilon^2}\right)^{1/n}.$$

When ε becomes sufficiently small, $s_\varepsilon \sim 2^{1/n}\varepsilon^{-2/n}$. Combining this with the upper bound (Theorem 7) on $\lambda_1(\mathcal{L})$ we get that for small values of ε,

$$\lambda_1(\mathcal{L})\eta_\varepsilon(\widehat{\mathcal{L}}) \leqslant (1+o(1))\sqrt{\tfrac{n}{2\pi e}}\varepsilon^{-2/n}. \tag{9}$$

This should be compared with the unconditional result of [ADRS15, Lemma 6.1] that shows that

$$\sqrt{\frac{\log(1/\varepsilon)}{\pi}} < \lambda_1(\mathcal{L})\eta_\varepsilon(\widehat{\mathcal{L}}) < \sqrt{\frac{\beta(\mathcal{L})^2 n}{2\pi e}} \cdot \varepsilon^{-1/n} \cdot (1+o(1)) \tag{10}$$

where $\beta(\mathcal{L}) \leqslant 2^{0.401}$ is the generalized kissing number [ACKS21]. It is reasonable to believe that $\beta(\mathcal{L}) \approx 1$ for a random lattice $\mathcal{L}$. If this were the case, then it remains a discrepancy between our bound (9) and the bound (10) of [ADRS15]: $\varepsilon^{-2/n}$ in our case compared to $\varepsilon^{-1/n}$ in theirs. We leave as an open question to explain this discrepancy which may point to our upper bound (Corollary 3) being suboptimal.

References

[ABLR21] Martin R. Albrecht, Shi Bai, Jianwei Li, and Joe Rowell. Lattice reduction with approximate enumeration oracles. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology – CRYPTO 2021*, pages 732–759, Cham, 2021. Springer International Publishing.

[ACKS21] Divesh Aggarwal, Yanlin Chen, Rajendra Kumar, and Yixin Shen. Improved (provable) algorithms for the shortest vector problem via bounded distance decoding. In Markus Bläser and Benjamin Monmege, editors, *38th International Symposium on Theoretical Aspects of Computer Science, STACS 2021, March 16-19, 2021, Saarbrücken, Germany (Virtual Conference)*, volume 187 of *LIPIcs*, pages 4:1–4:20. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021. doi:10.4230/LIPIcs.STACS.2021.4.

[ADRS15] Divesh Aggarwal, Daniel Dadush, Oded Regev, and Noah Stephens-Davidowitz. Solving the shortest vector problem in 2^n time using discrete gaussian sampling: Extended abstract. In Rocco A. Servedio and Ronitt Rubinfeld, editors, *Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing, STOC 2015, Portland, OR, USA, June 14-17, 2015*, pages 733–742. ACM, 2015. doi:10.1145/2746539.2746606.

[AEN] Yoshinori Aono, , THOMAS ESPITAU, and Phong Q. Nguyen. Random lattices: Theory and practice. URL: https://api.semanticscholar.org/CorpusID:271090054.

[Ajt98] Miklós Ajtai. The shortest vector problem in l2 is np-hard for randomized reductions (extended abstract). In *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, STOC '98, page 10–19, New York, NY, USA, 1998. Association for Computing Machinery. doi:10.1145/276698.276705.

[ALNSD20] Divesh Aggarwal, Jianwei Li, Phong Q. Nguyen, and Noah Stephens-Davidowitz. Slide reduction, revisited—filling the gaps in svp approximation. In Daniele Micciancio and Thomas Ristenpart, editors, *Advances in Cryptology – CRYPTO 2020*, pages 274–295, Cham, 2020. Springer International Publishing.

[ALSD21] Divesh Aggarwal, Zeyong Li, and Noah Stephens-Davidowitz. A $2^{n/2}$-time algorithm for $\sqrt{n}$-svp and $\sqrt{n}$-hermite svp, and an improved time-approximation tradeoff for (h)svp. In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology – EUROCRYPT 2021*, pages 467–497, Cham, 2021. Springer International Publishing.

[AUV19] Divesh Aggarwal, Bogdan Ursu, and Serge Vaudenay. Faster sieving algorithm for approximate SVP with constant approximation factors. Cryptology ePrint Archive, Paper 2019/1028, 2019. URL: https://eprint.iacr.org/2019/1028.

[BDGL16] Anja Becker, Léo Ducas, Nicolas Gama, and Thijs Laarhoven. New directions in nearest neighbor searching with applications to lattice sieving. In Robert Krauthgamer, editor, *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2016, Arlington, VA, USA, January 10-12, 2016*, pages 10–24. SIAM, 2016. URL: https://doi.org/10.1137/1.9781611974331.ch2, doi:10.1137/1.9781611974331.CH2.

[BDK+18] Joppe Bos, Leo Ducas, Eike Kiltz, T Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehle. Crystals - kyber: A cca-secure module-lattice-based kem. In *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 353–367, 2018. doi:10.1109/EuroSP.2018.00032.

[BLP+13] Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev, and Damien Stehlé. Classical hardness of learning with errors. In *Proceedings of the Forty-Fifth Annual ACM Symposium on Theory of Computing*, STOC '13, page 575–584, New York, NY, USA, 2013. Association for Computing Machinery. doi:10.1145/2488608.2488680.

[BN24] Henry Bambury and Phong Q. Nguyen. Improved provable reduction of ntru and hypercubic lattices. In *Post-Quantum Cryptography: 15th International Workshop, PQCrypto 2024, Oxford, UK, June 12–14, 2024, Proceedings, Part I*, page 343–370, Berlin, Heidelberg, 2024. Springer-Verlag. doi:10.1007/978-3-031-62743-9_12.

[Bri84] Ernest F. Brickell. Breaking iterated knapsacks. In *Advances in Cryptology, Proceedings of CRYPTO '84, Santa Barbara, California, USA, August 19-22, 1984, Proceedings*, pages 342–358, 1984. doi:10.1007/3-540-39568-7_27.

[BV14] Zvika Brakerski and Vinod Vaikuntanathan. Lattice-based fhe as secure as pke. In *Proceedings of the 5th Conference on Innovations in Theoretical Computer Science*, ITCS '14, page 1–12, New York, NY, USA, 2014. Association for Computing Machinery. doi:10.1145/2554797.2554799.

[CDLP13] Kai-Min Chung, Daniel Dadush, Feng-Hao Liu, and Chris Peikert. On the lattice smoothing parameter problem. In *2013 IEEE Conference on Computational Complexity*, pages 230–241, 2013. doi:10.1109/CCC.2013.31.

[CPS+20] Chitchanok Chuengsatiansup, Thomas Prest, Damien Stehlé, Alexandre Wallet, and Keita Xagawa. Modfalcon: Compact signatures based on module-ntru lattices. In *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*, ASIA CCS '20, page 853–866, New York, NY, USA, 2020. Association for Computing Machinery. doi:10.1145/3320269.3384758.

[dB89] Rudi de Buda. Some optimal codes have structure. *IEEE Journal on Selected Areas in Communications*, 7(6):893–899, 1989. doi:10.1109/49.29612.

[DKL+18] Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehlé. Crystals-dilithium: A lattice-based digital signature scheme. *Transactions on Cryptographic Hardware and Embedded Systems*, 2018, Issue 1:238–268, 2018. URL: https://tches.iacr.org/index.php/TCHES/article/view/839, doi:10.13154/tches.v2018.i1.238-268.

[DvW22] Léo Ducas and Wessel P. J. van Woerden. On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography. In Orr Dunkelman and Stefan Dziembowski, editors, *Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part III*, volume 13277 of *Lecture Notes in Computer Science*, pages 643–673. Springer, 2022. doi:10.1007/978-3-031-07082-2_23.

[FHK+19] Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Prest, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang. Falcon: Fast-fourier lattice-based compact signatures over ntru. 2019. URL: https://api.semanticscholar.org/CorpusID:231637439.

[FT87] András Frank and Éva Tardos. An application of simultaneous diophantine approximation in combinatorial optimization. *Combinatorica*, 7(1):49–65, 1987. doi:10.1007/BF02579200.

[GN08] Nicolas Gama and Phong Q. Nguyen. Finding short lattice vectors within mordell's inequality. In *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*, STOC '08, page 207–216, New York, NY, USA, 2008. Association for Computing Machinery. doi:10.1145/1374376.1374408.

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*, STOC '08, page 197–206, New York, NY, USA, 2008. Association for Computing Machinery. doi:10.1145/1374376.1374407.

[Jr.83] Hendrik W. Lenstra Jr. Integer programming with a fixed number of variables. *Math. Oper. Res.*, 8(4):538–548, 1983. doi:10.1287/moor.8.4.538.

[Kan87] Ravi Kannan. Minkowski's convex body theorem and integer programming. *Math. Oper. Res.*, 12(3):415–440, 1987. doi:10.1287/moor.12.3.415.

[Kim24] Seungki Kim. Adelic rogers integral formula. *Journal of the London Mathematical Society*, 109(1):e12830, 2024. doi:10.1112/jlms.12830.

[Kle00] Philip Klein. Finding the closest lattice vector when it's unusually close. In *Proceedings of the Eleventh Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '00, page 937–941, USA, 2000. Society for Industrial and Applied Mathematics.

[KNSW20] Elena Kirshanova, Huyen Nguyen, Damien Stehlé, and Alexandre Wallet. On the smoothing parameter and last minimum of random orthogonal lattices. *Des. Codes Cryptogr.*, 88(5):931–950, 2020. URL: https://doi.org/10.1007/s10623-020-00719-w, doi:10.1007/S10623-020-00719-W.

[LLBS14] Cong Ling, Laura Luzzi, Jean-Claude Belfiore, and Damien Stehlé. Semantically secure lattice codes for the gaussian wiretap channel. *IEEE Transactions on Information Theory*, 60(10):6399–6416, 2014. doi:10.1109/TIT.2014.2343226.

[LLL82] A.K. Lenstra, H.W. Lenstra, and László Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261:515–534, 1982.

[LO85] J. C. Lagarias and Andrew M. Odlyzko. Solving low-density subset sum problems. *J. ACM*, 32(1):229–246, 1985. doi:10.1145/2455.2461.

[LPR13] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. A toolkit for ring-lwe cryptography. In Thomas Johansson and Phong Q. Nguyen, editors, *Advances in Cryptology – EUROCRYPT 2013*, pages 35–54, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

[MR58] A. M. Macbeath and C. A. Rogers. Siegel's mean value theorem in the geometry of numbers. *Mathematical Proceedings of the Cambridge Philosophical Society*, 54(2):139–151, 1958. doi:10.1017/S0305004100033302.

[MR04] D. Micciancio and O. Regev. Worst-case to average-case reductions based on gaussian measures. In *45th Annual IEEE Symposium on Foundations of Computer Science*, pages 372–381, 2004. doi:10.1109/FOCS.2004.72.

[PS24] Amaury Pouly and Yixin Shen. Provable dual attacks on learning with errors. In *Advances in Cryptology – EUROCRYPT 2024: 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zurich, Switzerland, May 26–30, 2024, Proceedings, Part VII*, page 256–285, Berlin, Heidelberg, 2024. Springer-Verlag. doi:10.1007/978-3-031-58754-2_10.

[Rob55] Herbert Robbins. A remark on stirling's formula. *The American Mathematical Monthly*, 62, no. 1:26–29, 1955. doi:10.2307/2308012.

[Rog55] C. A. Rogers. Mean values over the space of lattices. *Acta Mathematica*, 94(0):249–287, 1955. doi:10.1007/BF02392493.

[Rog56] C. A. Rogers. The number of lattice points in a set. *Proceedings of the London Mathematical Society*, s3-6(2):305–320, 1956. doi:10.1112/plms/s3-6.2.305.

[Sch87] C.P. Schnorr. A hierarchy of polynomial time lattice basis reduction algorithms. *Theoretical Computer Science*, 53(2):201–224, 1987. URL: https://www.sciencedirect.com/science/article/pii/0304397587900648, doi:10.1016/0304-3975(87)90064-8.

[Sha84] Adi Shamir. A polynomial-time algorithm for breaking the basic merkle-hellman cryptosystem. *IEEE Trans. Information Theory*, 30(5):699–704, 1984. doi:10.1109/TIT.1984.1056964.

[Sie45] Carl Ludwig Siegel. A Mean Value Theorem in Geometry of Numbers. *The Annals of Mathematics*, 46(2):340, April 1945. URL: https://www.jstor.org/stable/1969027?origin=crossref, doi:10.2307/1969027.

[SS11] Damien Stehlé and Ron Steinfeld. Making ntru as secure as worst-case problems over ideal lattices. In Kenneth G. Paterson, editor, *Advances in Cryptology – EUROCRYPT 2011*, pages 27–47, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[Ste17] Noah Stephens-Davidowitz. *On the Gaussian measure over lattices*. Phd thesis, New York University, 2017.

[WL19] Zheng Wang and Cong Ling. Lattice gaussian sampling by markov chain monte carlo: Bounded distance decoding and trapdoor sampling. *IEEE Transactions on Information Theory*, 65(6):3630–3645, 2019. doi:10.1109/TIT.2019.2901497.

[WLW15] Wei Wei, Mingjie Liu, and Xiaoyun Wang. Finding shortest lattice vectors in the presence of gaps. In Kaisa Nyberg, editor, *Topics in Cryptology — CT-RSA 2015*, pages 239–257, Cham, 2015. Springer International Publishing.