# **Smoothing Parameter and Shortest Vector Problem on Random Lattices**

Amaury Pouly<sup>1</sup>  $\bullet$  and Yixin Shen<sup>2</sup>  $\bullet$ 

<sup>1</sup> Centre National de la Recherche Scientifique (CNRS), France <sup>2</sup> Univ Rennes, Inria, CNRS, IRISA, Rennes, France

**Abstract.** Lattice problems have many applications in various domains of 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  $2^{n+o(n)}$  [\[2\]](#page-14-0). However, in practice, people rely on heuristic (unproven) sieving algorithms of time complexity  $2^{0.292n+o(n)}$  [\[11\]](#page-15-0) to assess the security of latticebased cryptography schemes. Those heuristic algorithms are experimentally verified for lattices used in cryptography, which are usually random in some  $way<sup>1</sup>$  $way<sup>1</sup>$  $way<sup>1</sup>$ .

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 [\[36\]](#page-17-0), we show a tighter upper bound on an important lattice parameter called the smoothing parameter that applies to almost all random lattices. This allows us to obtain a  $2^{n/2+o(n)}$  time algorithm for an approximation version of the SVP on random lattices with a small constant approximation factor.

**Keywords:** Random Lattices · Smoothing Parameter · Shortest Vector Problem

E-mail: [amaury.pouly@cnrs.fr](mailto:amaury.pouly@cnrs.fr) (Amaury Pouly), [yixin.shen@inria.fr](mailto:yixin.shen@inria.fr) (Yixin Shen)



<span id="page-0-0"></span><sup>1</sup>There exists several formal notions of 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 [\[12,](#page-15-1) [18,](#page-15-2) [19\]](#page-15-3). Moreover, lattice problems have applications in algorithmic number theory [\[28\]](#page-16-0), convex optimization [\[23,](#page-16-1) [24,](#page-16-2) [20\]](#page-15-4), coding theory [\[16\]](#page-15-5), and cryptanalysis tools [\[35,](#page-16-3) [14,](#page-15-6) [27\]](#page-16-4), 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  $2^{n+o(n)}$  [\[2\]](#page-14-0). However, in practice, people rely on heuristic (unproven) sieving algorithms of time complexity  $2^{0.292n+o(n)}$  [\[11\]](#page-15-0) 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, 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  $\alpha$  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  $2^{0.802n + o(n)}$  [\[39\]](#page-17-1) but only solve  $O(1)$ -SVP for an unspecified constant. More explicit constants are provided in [\[6\]](#page-14-1) but even for  $\alpha = 100$ , the time complexity is still  $2^{0.824n+o(n)}$ . In [\[10\]](#page-14-2), the authors noted that there is no theoretical complexity is still  $2^{2(2-2)(1-1)}$ . In [10], the authors noted that there is no theoretical<br>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 ZLIP which is a recent hardness assumption in lattice-based cryptographic schemes [\[17\]](#page-15-7). If we relax the approximation ratio, better In lattice-based cryptographic schemes [17]. If we relax the approximation ratio, better complexities can be achieved. For example, [\[5\]](#page-14-3) gives an algorithm that solves  $\tilde{O}(\sqrt{n})$ -SVP in time  $2^{n/2+o(n)}$ .

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 [\[36\]](#page-17-0), we obtain a  $2^{n/2+o(n)}$ time algorithm for  $\sqrt{e}$ -SVP on random lattices. Our algorithm (Theorem [1\)](#page-1-0) achieves a much better approximation ratio compared to all worst-case algorithms and is particularly simple compared to [\[5\]](#page-14-3).

Most lattice reduction algorithms rely on solving *α*-SVP in smaller dimension [\[34\]](#page-16-5) for *α* close to 1 [\[8\]](#page-14-4). In certain lattice reduction algorithms such as slide reduction [\[21,](#page-15-8) [4\]](#page-14-5), 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  $\alpha$  vol $(\mathcal{L})^{1/n}$  for a lattice  $\mathcal{L} \subset \mathbb{R}^n$  is known as the  $\alpha$ -Hermite SVP ( $\alpha$ -HSVP). Our algorithm (Theorem [1\)](#page-1-0) also solves  $\sqrt{\frac{n}{2\pi}}$ -HSVP in time  $2^{n/2+o(n)}$  for random lattices. This improves upon the worst-case algorithm of [\[5\]](#page-14-3) 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.

<span id="page-1-0"></span>**Theorem 1** (Informal, see Theorem [5](#page-11-0) and Corollary [3\)](#page-12-0). For every  $n \geq 1$ , there is an *algorithm that on most lattices*  $\mathcal{L} \subset \mathbb{R}^n$ , solves  $(1+o(1))\sqrt{e}$ -SVP and  $(1+o(1))\sqrt{\frac{n}{2n}}$ -HSVF *in time 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. A 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 [2.4\)](#page-3-0). In particular, we use [\[1\]](#page-14-6) to sample from  $D_{\mathcal{L},s}$  for  $s = \eta_{1/3}(\mathcal{L})$ . 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  $D_{\mathcal{L},s}$ . We then show that generating a constant number of samples from  $D_{\mathcal{L},s}$  for  $s = \eta_{1/3}(\mathcal{L})$  is sufficient to approximate the SVP.

Interestingly, the complexity of our algorithm is dominated by the time to sample from  $D_{\mathcal{L},s}$  for  $s = \eta_{1/3}(\mathcal{L}), i.e.$  above the smoothing parameter. Therefore, any improvement  $L_{\mathcal{L},s}$  for  $s = \eta_{1/3}(\mathcal{L})$ , *i.e.* above the smoothing parameter. Therefore, any improvement in those samplers would yield an improvement to the complexity of solving  $\sqrt{e}$ -SVP and  $\sqrt{\frac{n}{2\pi}}$ -HSVP for random lattices. Lattice-based cryptography relies on the fact that and  $\sqrt{\frac{2\pi}{2}}$ -115 VF for random lattices. Lattice-based cryptography refles on the fact that problems such as  $\sqrt{e}$ -SVP 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.

**Organization of the paper** Section [2](#page-2-0) contains preliminary technical results. Section [3](#page-9-0) gives some probabilistic bounds on the Gaussian mass and smoothing parameter of random real lattice. Section [4](#page-11-1) give an application of those bounds to the approximate (Hermite) SVP.

### <span id="page-2-0"></span>**2 Preliminaries**

We denote vectors and matrices in bold case. We denote by  $x^T$  the transpose of the (column) vector **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 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  $d_{TV}(P,Q)$  the statistical distance (or total variation distance) between *P* and *Q*. We say that two distributions *P* and *Q* are *ε*-close if  $d_{TV}(P,Q) \leq \varepsilon$ .

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

<span id="page-2-2"></span>
$$
\zeta(s) - 1 \sim_{s \to \infty} 2^{-s} \tag{1}
$$

#### **2.1 Lambert W function**

Recall that 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  $x \in [-\frac{1}{e}, 0)$ ,  $W_{-1}(x) \leq -1 \leq W_0(x)$ . The following lemma on *W* will be useful

<span id="page-2-1"></span>**Lemma 1** ([\[15,](#page-15-9) Theorem 1]). *For any*  $u > 0$ , -1 – √ **Lemma 1** ([15, Theorem 1]). For any  $u > 0$ ,  $-1 - \sqrt{2u} - u < W_{-1}(-e^{-1-u}) < -1 - \sqrt{2u} - u$  $\overline{2u} - \frac{2}{3}u.$ 

#### **2.2 Lattices**

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

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

of all integer combinations of *n* linearly independent vectors  $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^m$ . 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 vol $(\mathcal{L})$  the volume (or determinant) of  $\mathcal{L}$ . For a full-rank lattice  $\mathcal{L}$ , vol $(\mathcal{L}) = \det(\mathbf{A})$  for any basis **A** of  $\mathcal{L}$ .

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  $\text{span}(\mathcal{L})$  that have integer inner products with all lattice points,

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

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  $\text{span}(\mathcal{L})$  satisfying  $\langle \mathbf{b}_i^*, \mathbf{b}_j \rangle = 1$  if  $i = j$ , and 0, otherwise. It is easy to show that  $\hat{\mathcal{L}}$  is itself a rank *n* lattice and  $\mathbf{B}^*$  is a basis of  $\hat{\mathcal{L}}$ . 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.*  $n = m$ .

#### **2.3 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 **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  $\alpha = \alpha(n)$ , the search problem  $\alpha$ -SVP ( $\alpha$ -Approximate Shortest Vector Problem) is defined as follows: The input is a basis **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  $\|\mathbf{y}\| \leq \alpha \cdot \lambda_1(\mathcal{L})$ .

**Definition 3.** For  $\alpha = \alpha(n)$ , the search problem  $\alpha$ -HSVP ( $\alpha$ -Hermite Approximate Shortest Vector Problem) is defined as follows: The input is a basis **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  $\|\mathbf{y}\| \leq \alpha \cdot \det(\mathcal{L})^{1/n}$ .

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*).

#### <span id="page-3-0"></span>**2.4 Discrete Gaussian distribution and Smoothing Parameter**

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  $\rho_s$  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 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  $s > 0$ ,

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

See e.g. [\[37\]](#page-17-2) 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 4.** For  $\delta = \delta(n) \geq 0$ ,  $\sigma$  a function that maps lattices to non-negative real numbers, and  $m = m(n) \in \mathbb{N}$ ,  $\delta$ -DGS<sup>*m*</sup> is defined as follows. The input is a basis **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  $\delta$ -close to *m* independent samples from  $D_{\ell,s}$ .

We omit the parameter  $\delta$  if  $\delta = 0$ , and the parameter *m* if  $m = 1$ . We stress that  $\delta$ 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 [\[31\]](#page-16-6) 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

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

There are many algorithms to sample above the smoothing parameter [\[26,](#page-16-7) [22,](#page-16-8) [13\]](#page-15-10), including a time-space trade-off [\[1\]](#page-14-6). Sampling below the smoothing parameter is much more challenging and usually inefficient [\[2\]](#page-14-0). At the extreme, sampling for sufficiently small values of *s* allows one to solve the Shortest Vector problem (SVP) [\[2\]](#page-14-0) which is known to be NP-hard under randomized reduction [\[7\]](#page-14-7). The Monte Carlo Markov Chain based algorithm of [\[38\]](#page-17-3) works for all values of *s* but the complexity significantly depends on *s* and the shape of the basis. In this paper, we will use the following sampler from [\[1\]](#page-14-6).

<span id="page-4-0"></span>**Lemma 2** ([\[1,](#page-14-6) Lemma 54]). *There is a probabilistic algorithm that, given a lattice*  $\mathcal{L} \subset \mathbb{R}^n$ ,  $m \in \mathbb{N}$  and  $s \geq \eta_{1/3}(\mathcal{L})$  as input, outputs *m* samples from a distribution  $(m \cdot 2^{-\Omega(n^2)})$ -close *to*  $D_{\mathcal{L},s}$  *in expected time*  $m \cdot 2^{n/2+o(n)}$  *and space*  $(m+2^{n/2}) \cdot 2^{o(n)}$ *. Furthermore, all samples have* poly(*n*) *bit-size.*

We will use the following concentration bound for the discrete Gaussian.

<span id="page-4-1"></span>**Lemma 3** ([\[2,](#page-14-0) Lemma 2.4]). For any lattice  $\mathcal{L} \subset \mathbb{R}^n$ ,  $s > 0$  and  $t \geq 1$ ,

$$
\mathrm{Pr}_{\mathbf{x} \sim D_{\mathcal{L},s}}\Big[\|\mathbf{x}\| > ts\sqrt{\tfrac{n}{2\pi}}\Big] < \Big(t\exp(\tfrac{1-t^2}{2})\Big)^n\,.
$$

Since the right-hand side of the equation of the above lemma is difficult to use directly, we will simplify it using the following lemma.

<span id="page-4-2"></span>**Lemma 4.** For any  $k \geq 1$ ,  $\alpha \in (0,1)$  and  $t^2 \geq 1 + \sqrt{\frac{-4}{k} \log \alpha} - \frac{2}{k} \log \alpha$ , we have  $\int t \exp(\frac{1-t^2}{2})$  $\left(\frac{-t^2}{2}\right)\right)^k \leqslant \alpha.$ 

*Proof.* Check that for  $t \geq 1$ ,

$$
\left(t\exp\left(\frac{1-t^2}{2}\right)\right)^k \leqslant \alpha
$$

 $\Leftrightarrow t^2 \exp(1-t^2) \leqslant \alpha^{2/k}$  $\Leftrightarrow -t^2 \exp(-t^2) \geqslant -\frac{1}{e} \alpha^{2/k}$  $\Leftrightarrow -t^2 \leqslant W_{-1}\left(-\frac{1}{e}\alpha^{2/k}\right)$ by the decreasing behaviour of the function *W*−1.  $\Leftrightarrow -t^2 \leqslant \left(1 + \sqrt{\frac{-4}{k} \log \alpha} - \frac{2}{k} \log \alpha\right)$ by Lemma [1.](#page-2-1)

 $\Box$ 

#### <span id="page-5-2"></span>**2.5 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 **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  $\alpha L$  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  $SL_n(\mathbb{R})$ . Second, it is clear that many matrices in  $SL_n(\mathbb{R})$  span the same lattice: for instance permuting columns or changing the sign of an even number of columns. In general, matrices  $\mathbf{B} \in SL_n(\mathbb{R})$  and **B***U* span the same lattice for any  $U \in SL_n(\mathbb{Z})$ . The converse is also true and hence we wish to define a probability measure on the homogenous space  $X_n := SL_n(\mathbb{R})/SL_n(\mathbb{Z})$ .

Let  $\mu$  be a measure on  $X_n$ ,  $Y$  be a measurable set of lattices in  $X_n$  and  $\mathbf{B} \in SL_n(\mathbb{Z})$ : a natural measure  $\mu$  should assign the same probability to *Y* and **B***Y* since those are the same lattices up to the change of basis. Therefore,  $\mu$  should be (left)  $SL_n(\mathbb{Z})$ −invariant:  $\mu(Y) = \mu(BY)$ . 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  $\mu$  should be a Borel measure. Such a measure is called a (left-)invariant Haar measure and Siegel showed [\[36\]](#page-17-0) 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  $\mu_n$ .

In this paper, we will identity the set of lattices modulo scale 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  $X_n \to X_n$ ,  $\mathcal{L} \mapsto \mathcal{L}$ preserves  $\mu_n$  so that if  $\mathcal L$  is distributed according to  $\mu_n$  then so is its dual  $\mathcal L$ .

The above measure was introduced by Siegel in [\[36\]](#page-17-0) who proved the following averaging theorem.

<span id="page-5-0"></span>**Theorem 2** (Siegel [\[36\]](#page-17-0)). Let  $n \geq 1$  and  $f$  be a Lebesgue integrable function on  $\mathbb{R}^n$ ,

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

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

This result was later generalized by Rogers [\[32\]](#page-16-9), and the presentation simplified in [\[29\]](#page-16-10) which is probably the most readable reference on the topic.

<span id="page-5-1"></span>We say that a matrix  $M \in \mathbb{Z}^{n \times m}$  is *primitive* if 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  $\mathbb{Z}^m$ , *i.e.* this set can be extended to form an integer basis of  $\mathbb{Z}^m$ . Let  $PR_{n,\ell} \subset \mathbb{Z}^{n \times \ell}$  be the set of primitive matrices and  $LI_{n,\ell} \subset \mathbb{Z}^{n \times \ell}$  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  $X_n$  as both the set of lattices modulo scale, or the set of matrices of determinant 1.

**Theorem 3** ([\[30,](#page-16-11) Theorems 1, 2 and (13)]). Let  $1 \leq \ell \leq n-1$  and f be Lebesgue integrable  $\mathbb{R}^{n \times \ell}$ , then

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

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 [\[30\]](#page-16-11). 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  $\mathbf{x} \in \text{PR}_{n,1}$ . 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.* **x** is not an integer multiple of an integer vector (except by multiplying by 1 and  $-1$ ).

<span id="page-6-0"></span>**Corollary 1.** Let  $n \geqslant 2$  and  $f$  be Lebesgue integrable on  $\mathbb{R}^{n \times \ell}$ , then

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

*Proof.* The first inequality follows directly from Theorem [2:](#page-5-0)

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

For the second equality, first oberve that

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

Now let  $g: \mathbb{R}^{n \times 2} \to \mathbb{R}$  be defined by  $g([\mathbf{x} \ \mathbf{y}]) = f(\mathbf{x})f(\mathbf{y})$  which is clearly Lebesgue integrable. Let  $\mathcal{L} \in X_n$  be a lattice and **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 **u** and **v**: either  $\mathbf{u} = \mathbf{v} = 0$ ; or **u** and **v** are linearly independent *i.e.*  $[\mathbf{u} \quad \mathbf{v}] \in \mathbf{LI}_{n,2}$ ; 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  $\mathbf{p}, \alpha$  and *β* are unique, and that conversely the vectors *α***p** and *β***p** are always linearly dependent and nonzero, there is a bijection between  $\{(u, v) \in (\mathbb{Z}^n \setminus \{0\})^2 : \text{linearly dependent}\}\$ 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,

$$
\sum_{\mathbf{x},\mathbf{y}\in\mathcal{L}} f(\mathbf{x})f(\mathbf{y})
$$
\n
$$
= f(0)^2 + \sum_{\mathbf{M}\in\mathbf{L}\mathbf{I}_{n,2}} g(\mathbf{A}\mathbf{M}) + 2f(0) \sum_{\mathbf{v}\in\mathbb{Z}^n\backslash\{0\}} f(\mathbf{A}\mathbf{v}) + \sum_{\mathbf{p}\in\mathbb{Z}^n:\text{prim. }\alpha\in\mathbb{N}\backslash\{0\}} \sum_{\beta\in\mathbb{Z}\backslash\{0\}} f(\mathbf{A}\alpha\mathbf{p})f(\mathbf{A}\beta\mathbf{p})
$$

 $\Box$ 

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

We can now compute one of those terms by Theorem [2:](#page-5-0)

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

And the other two by Theorem [3:](#page-5-1)

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

and

$$
\int_{X_n} \sum_{\mathbf{p} \in \mathbb{Z}^n:\text{prim.}} f(\alpha \mathbf{A} \mathbf{p}) f(\beta \mathbf{A} \mathbf{p}) d \mu_n(\mathbf{A}) = \int_{X_n} \sum_{\mathbf{p} \in \text{PR}_{n,1}} f(\alpha \mathbf{A} \mathbf{p}) f(\beta \mathbf{A} \mathbf{p}) d \mu_n(\mathbf{A})
$$

$$
= \frac{1}{\zeta(n)} \int_{\mathbb{R}^n} f(\alpha \mathbf{x}) f(\beta \mathbf{x}) d \lambda(\mathbf{x}).
$$

The result follows by putting everything together.

The following result is a well-known consequence of Theorem 3. There are many ways to prove similar results, see e.g. [33] or the survey [9]. Since we could not find a proof with explicit constants in both the length bound and the probability bound, we provide one for completeness. This result formalizes what is usually known as the Gaussian heuristic which says that heuristically, a "random" lattice 
$$
\mathcal{L} \subset \mathbb{R}^n
$$
 satisfies that  $\lambda_1(\mathcal{L}) \approx \sqrt{\frac{n}{2\pi e}} \text{vol}(\mathcal{L})^{1/n}$ . For the notion of real random lattices that we use in this paper, the volume is always 1.

<span id="page-7-0"></span>**Theorem 4.** *Let*  $n \geq 2$ *. For any*  $\alpha > 0$ *,* 

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

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

*Proof.* Fix  $r > 0$  and let  $f_r$  be the indicator function of the *n*-dimensional ball  $B_n(r)$  of radius *r*. By Corollary [1,](#page-6-0) 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

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

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

$$
\sigma_r^2 = \frac{1}{\zeta(n)} \sum_{\alpha \in \mathbb{N} \setminus \{0\}} \sum_{\beta \in \mathbb{Z} \setminus \{0\}} \int_{\mathbb{R}^n} f_r(\max(\alpha, |\beta|) \mathbf{x}) d\lambda(\mathbf{x})
$$

$$
= \frac{1}{\zeta(n)} \sum_{\alpha \in \mathbb{N} \setminus \{0\}} \sum_{\beta \in \mathbb{Z} \setminus \{0\}} \max(\alpha, |\beta|)^{-n} \operatorname{vol}(B_n(r))
$$

$$
= 2 \frac{\operatorname{vol}(B_n(r))}{\zeta(n)} \sum_{\alpha \in \mathbb{N} \setminus \{0\}} \sum_{\beta \in \mathbb{N} \setminus \{0\}} \max(\alpha, \beta)^{-n}.
$$

We now observe that

$$
\sum_{\alpha \in \mathbb{N} \setminus \{0\}} \sum_{\beta \in \mathbb{N} \setminus \{0\}} \max(\alpha, \beta)^{-n}
$$
\n
$$
= \sum_{\alpha \in \mathbb{N} \setminus \{0\}} \left( \sum_{\beta=1}^{\alpha} \alpha^{-n} + (\alpha + 1)^{-n} + \sum_{\beta=\alpha+2}^{\infty} \beta^{-n} \right)
$$
\n
$$
\leq \sum_{\alpha \in \mathbb{N} \setminus \{0\}} \left( \alpha^{1-n} + (\alpha + 1)^{-n} + \int_{\alpha+1}^{\infty} x^{-n} dx \right)
$$
\n
$$
= \zeta(n-1) + \zeta(n) - 1 + \sum_{\alpha \in \mathbb{N} \setminus \{0\}} \frac{(\alpha + 1)^{1-n}}{n-1}
$$
\n
$$
= \zeta(n-1) + \zeta(n) - 1 + \frac{\zeta(n-1)}{n-1}
$$
\n
$$
= \zeta(n) + \frac{n}{n-1} (\zeta(n-1) - 1).
$$

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

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

We apply the above inequality to study  $\lambda_1$ . Observe that for any  $r > 0$ ,  $\lambda_1(\mathcal{L}) \leq r$  if and only if  $|\mathcal{L} \cap B_n(r)| \geq 3$  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.*  $r^n$  vol $(B_n) \leq 2$ . Then we can let  $X = 3 - \mu_r$  and apply the above inequality to get that

$$
\Pr_{\mathcal{L}}[\lambda_1(\mathcal{L}) \le r] = \Pr_{\mathcal{L}}[|\mathcal{L} \cap B_n(r)| \ge 3]
$$
  
=  $\Pr_{\mathcal{L}}[|\mathcal{L} \cap B_n(r)| - \mu_r \ge X]$   
 $\le \Pr_{\mathcal{L}}[||\mathcal{L} \cap B_n(r)| - \mu_r| \ge X]$   
 $\le \frac{\sigma_r^2}{X^2}.$ 

If we let  $r_0$  be such that  $vol(B_n(r_0)) = 1$  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  $A(n) := 1 + \frac{n}{n-1}$ *ζ*(*n*−1)−1  $\frac{n-1}{\zeta(n)}$ , and at the same time

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

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

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

$$
\Pr_{\mathcal{L}}[\lambda_1(\mathcal{L}) \le r] = \Pr_{\mathcal{L}}[|\mathcal{L} \cap B_n(r)| \ge 3]
$$
  
\n
$$
\ge \Pr_{\mathcal{L}}[||\mathcal{L} \cap B_n(r)| - \mu_r| \le Y]
$$
  
\n
$$
= 1 - \Pr_{\mathcal{L}}[||\mathcal{L} \cap B_n(r)| - \mu_r| > Y]
$$
  
\n
$$
\ge 1 - \frac{\sigma_r^2}{Y^2}.
$$

 $\Box$ 

# <span id="page-9-0"></span>**3 On the Gaussian mass of random lattices**

In this section, we give a probabilistic estimate of the value of  $\rho_{1/s}(\hat{\mathcal{L}})$  when  $\mathcal L$  is a random real lattice. We derive from this a probabilistic bound on the smoothing parameter of a random lattice. We are not aware of any such results in the literature for this class of random lattices. However, a closely related result is available in [\[25\]](#page-16-13) which studies matrices with each entry independently and identically distributed from an integer Gaussian distribution, and that define a class known as *orthogonal lattices*.

Recall that by random real lattice, we mean  $\mathcal{L} \in X_n$  distributed according to  $\mu_n$ , *i.e.* the Haar measure. See Section [2.5](#page-5-2) for more details. Our first technical result is to obtain the expected value and variance of  $\rho_{1/s}(\hat{\mathcal{L}})$  for a random lattice  $\mathcal{L}$ . We derive from this a probabilistic bound on  $\rho_{1/s}(\mathcal{L})$ .

<span id="page-9-1"></span>**Lemma 5.** For any  $n \in \mathbb{N}$  and  $s > 0$ , let  $\mathcal{L} \in X_n$  be distributed according to  $\mu_n$ . Then  $\mathbb{E}_{\mathcal{L}}\left[\rho_{1/s}(\widehat{\mathcal{L}})\right] = 1 + s^{-n}$  and  $\mathbb{V}_{\mathcal{L}}\left[\rho_{1/s}(\widehat{\mathcal{L}})\right] = 2\frac{s^{-n}}{\zeta(n)}$  $\frac{s^{-n}}{\zeta(n)} \sum_{\alpha,\beta=1}^{\infty} (\alpha^2 + \beta^2)^{-n/2} \leqslant s^{-n} 2^{1-n/2} (1 +$ *o*(1)*). In particular, for any*  $\alpha > 0$ 

$$
\Pr_{\mathcal{L}\sim\mu_n}\left[\left|\rho_{1/s}(\widehat{\mathcal{L}})-1-s^{-n}\right|>\alpha\right] \leqslant \frac{2^{1-n/2}(1+o(1))}{s^n\alpha^2}
$$

*where*  $o(1) \rightarrow 0$  *as*  $n \rightarrow \infty$  *is independent of*  $\alpha$ *.* 

*Proof.* By Corollary [1,](#page-6-0) we have that

$$
\mathbb{E}_{\mathcal{L}\sim\mu_n}[\rho_{1/s}(\mathcal{L})] = \rho_s(0) + \int_{X_n} \rho_s(\mathcal{L}) d\mu_n(\mathcal{L}) = 1 + s^n
$$

where the last equality comes from standard results on the integration of Gaussian functions. By Corollary [1](#page-6-0) we also have that

$$
\mathbb{V}_{\mathcal{L}\sim\mu_n}[\rho_{1/s}(\mathcal{L})] = \frac{1}{\zeta(n)} \sum_{\alpha \in \mathbb{N}\setminus\{0\}} \sum_{\beta \in \mathbb{Z}\setminus\{0\}} \int_{\mathbb{R}^n} \rho_s(\alpha \mathbf{x}) \rho_s(\beta \mathbf{x}) d\lambda(\mathbf{x})
$$
  
\n
$$
= \frac{1}{\zeta(n)} \sum_{\alpha \in \mathbb{N}\setminus\{0\}} \sum_{\beta \in \mathbb{Z}\setminus\{0\}} \int_{\mathbb{R}^n} \rho_{s/\sqrt{\alpha^2 + \beta^2}}(\mathbf{x}) d\lambda(\mathbf{x})
$$
  
\n
$$
= \frac{s^n}{\zeta(n)} \sum_{\alpha \in \mathbb{N}\setminus\{0\}} \sum_{\beta \in \mathbb{Z}\setminus\{0\}} (\alpha^2 + \beta^2)^{-n/2}
$$
  
\n
$$
= 2 \frac{s^n}{\zeta(n)} \sum_{\alpha, \beta = 1}^{\infty} (\alpha^2 + \beta^2)^{-n/2}.
$$

By the Poisson summation formula, we have that  $\rho_{1/s}(\hat{\mathcal{L}}) = s^{-n} \rho_s(\mathcal{L})$  since  $\text{vol}(\mathcal{L}) = 1$  for  $\mathcal{L} \in X_n$ . It follows that

$$
\mu := \mathbb{E}_{\mathcal{L}}\Big[\rho_{1/s}(\widehat{\mathcal{L}})\Big] = s^{-n} \mathbb{E}_{\mathcal{L}}[\rho_s(\mathcal{L})] = s^{-n} + 1
$$

and

$$
\sigma^2 := \mathbb{V}_{\mathcal{L}}\Big[\rho_{1/s}(\widehat{\mathcal{L}})\Big] = s^{-2n} \mathbb{V}_{\mathcal{L}}\Big[\rho_{1/s}(\widehat{\mathcal{L}})\Big] = 2 \frac{s^{-n}}{\zeta(n)} \sum_{\alpha,\beta=1}^{\infty} (\alpha^2 + \beta^2)^{-n/2}.
$$

Furthermore,

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

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

$$
\leqslant \zeta(\frac{n}{2}) - 1 + \sum_{\alpha=1}^{\infty} \int_{1}^{\infty} (\alpha + \beta)^{-n/2} d\beta
$$
  

$$
= \zeta(\frac{n}{2}) - 1 + \sum_{\alpha=1}^{\infty} 2 \frac{(\alpha + 1)^{1 - \frac{n}{2}}}{n - 2}
$$
  

$$
= \zeta(\frac{n}{2}) - 1 + \frac{2}{n - 2} (\zeta(\frac{n}{2} - 1) - 1)
$$
  

$$
= 2^{-n/2} (1 + o(1))
$$

as  $n \to \infty$ . Let  $\mu = \mathbb{E}_{\mathcal{L}}\Big[\rho_{1/s}(\widehat{\mathcal{L}})\Big]$  and  $\sigma^2 = \mathbb{V}_{\mathcal{L}}\Big[\rho_{1/s}(\widehat{\mathcal{L}})\Big]$ . Then by Chebyshev's inequality, for any  $\alpha > 0$ ,

$$
p := \Pr_{\mathcal{L}} \left[ \left| \rho_{1/s}(\widehat{\mathcal{L}}) - \mu \right| > \alpha \right] \leqslant \frac{\sigma^2}{\alpha^2}.
$$

We have shown above that

$$
\mu = 1 + s^{-n}
$$
,  $\sigma^2 \leq \frac{2s^{-n}}{\zeta(n)} 2^{-n/2} (1 + o(1)) = s^{-n} 2^{1-n/2} (1 + o(1))$ 

Furthermore  $\sigma^2 \leqslant s^{-n} 2^{1-n/2} (1 + o_n(1))$  $\sigma^2 \leqslant s^{-n} 2^{1-n/2} (1 + o_n(1))$  $\sigma^2 \leqslant s^{-n} 2^{1-n/2} (1 + o_n(1))$  by (1). Hence,

$$
p \leqslant \frac{2^{1-n/2} (1 + o(1))}{s^n \alpha^2}.
$$

The previous lemma allows us to derive a probabilistic bound on the smoothing paragraph  $\eta_{\varepsilon}(\mathcal{L})$  of a random lattice  $\mathcal{L}$ . For our application to (Hermite) SVP in Section [4,](#page-11-1) we will not only need to bound  $\eta_{\varepsilon}(\mathcal{L})$  but simultaneously bound  $\rho_{\eta_{\varepsilon}}(\hat{\mathcal{L}})$  and  $\eta_{\varepsilon}(\mathcal{L})$ . The following corollary provides both bounds. following corollary provides both bounds.

<span id="page-10-0"></span>**Corollary 2.** 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  $\Pr_{\mathcal{L}\sim\mu_n}[\eta_{\varepsilon}(\mathcal{L}) > s_{\varepsilon}] \leqslant 2^{-n/2}(1+o(1)).$ 

*and*

$$
\Pr_{\mathcal{L}\sim\mu_n}\left[\rho_{s_{\varepsilon}}(\mathcal{L})<1+s_{\varepsilon}^n-\sqrt{2s_{\varepsilon}^n} \quad or \quad \eta_{\varepsilon}(\mathcal{L})>s_{\varepsilon}\right] \leqslant 2^{1-n/2}(1+o(1)).
$$

 $\Box$ 

*Proof.* Let  $\alpha = \varepsilon - s_{\varepsilon}^{-n}$  and check that  $\alpha > 0$ . We can therefore apply Lemma [5](#page-9-1) to get that

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

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  $\rho_{1/s_{\varepsilon}}(\widehat{\mathcal{L}}) \leq 1 + \varepsilon$  then  $\eta_{\varepsilon}(\mathcal{L}) \leq s_{\varepsilon}$ . Therefore,

<span id="page-11-2"></span>
$$
\Pr_{\mathcal{L}}[\eta_{\varepsilon}(\mathcal{L}) > s_{\varepsilon}] \leqslant \Pr_{\mathcal{L}}[\rho_{1/s_{\varepsilon}}(\mathcal{L}) > 1 + \varepsilon] \leqslant 2^{-n/2}(1 + o(1)).\tag{2}
$$

On the other hand, recall that if  $\mathcal{L} \in X_n$  is distributed according to  $\mu_n$  then its  $\mathcal{L}$  is also distributed according to  $\mu_n$ . Therefore, we can also apply Lemma [5](#page-9-1) to  $\alpha = \sqrt{2s_{\varepsilon}^n}$  to get that

<span id="page-11-3"></span>
$$
\Pr_{\mathcal{L}}\left[\rho_{s_{\varepsilon}}(\widehat{\mathcal{L}}) < 1 + s_{\varepsilon}^n - \alpha\right] = \Pr_{\mathcal{L}}\left[\rho_{s_{\varepsilon}}(\widehat{\mathcal{L}}) - 1 - s_{\varepsilon}^n < -\alpha\right] \\
&\leq \Pr_{\mathcal{L}}\left[\left|\rho_{s_{\varepsilon}}(\widehat{\mathcal{L}}) - 1 - s_{\varepsilon}^n\right| > \alpha\right] \\
&\leq \frac{2^{1-n/2}(1 + o(1))}{s_{\varepsilon}^n \alpha^2} \\
&= 2^{-n/2}(1 + o(1)).\n\tag{3}
$$

It follows by a union bound that a random lattice  $\mathcal L$  satisfies [\(2\)](#page-11-2) or [\(3\)](#page-11-3) with probability at  $\text{most } 2^{1-n/2}(1+o(1)).$  $\Box$ 

## <span id="page-11-1"></span>**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 constant number of vectors from  $D_{\mathcal{L},s}$  for  $s = \eta_{1/3}(\mathcal{L})$  and we return the shortest nonzero vector among them. When sampling from  $D_{\mathcal{L},s}$  to get short vectors, there is a tradeoff in the choice of *s*: if *s* is too large small then we will get too long vectors in average, but if *s* is too small then we will mostly get the 0 vector (which has the highest probability according to  $D_{\mathcal{L},s}$ ). Therefore, the difficulty lies in showing that we return a relatively short vector with good probability when  $s = \eta_{1/3}(\mathcal{L})$ .

<span id="page-11-0"></span>**Theorem 5.** For every  $n \geq 1$ , there is a randomized algorithm that on a fraction at *least*  $1 - 2^{1-n/2}(1+o(1))$  *of random lattices*  $\mathcal L$  *according to*  $\mu_n$ *, outputs in time and space*  $2^{n/2+o(n)}$  *a nonzero vector of*  $\mathcal L$  *of length at most*  $t(n)\sqrt{\frac{n}{2\pi}} \cdot 24^{1/n}$  *with probability at least*  $1/2$ *, where*  $t(n)^2 := 1 + \sqrt{\frac{-4}{n} \log \frac{15}{17}} - \frac{2}{n} \log \frac{15}{17}$ *.* 

*Proof.* Let  $s = s_{1/3}$  be given by Corollary [2,](#page-10-0) and N to be fixed later. Consider the following algorithm:

- Sample *N* vectors independently according to  $D_{\mathcal{L},s}$  by Lemma [2.](#page-4-0)
- Return the shortest nonzero vector.

We will analyze this algorithm. First the running time is clear by Lemma [2:](#page-4-0) the algorithm takes time  $N \cdot 2^{n/2 + o(n)}$  and space  $(N + 2^{n/2}) \cdot 2^{o(n)}$ .

Next we observe that by Corollary [2](#page-10-0) for  $\varepsilon = 1/3$ , and with probability at least  $1 - 2^{1-n/2}(1 + o(n))$  we have both

$$
\rho_s(\mathcal{L}) \geq 1 + s^n - \sqrt{2s^n}
$$
 and  $\eta_{1/3}(\mathcal{L}) \leq s$ .

Assume that we are in this case. It will be useful to note that  $s = s_{1/3} = (12 + 3\sqrt{15})^{1/n}$ and  $1 + s^n - \sqrt{2s^n} = 10 + 2\sqrt{5}$ . Therefore

$$
23^{1/n} \leqslant s \leqslant 24^{1/n}, \qquad 1 + s^n - \sqrt{2s^n} \geqslant 17.
$$

Since  $\eta_{1/3}(\mathcal{L}) \leq s$  we can indeed apply Lemma [2](#page-4-0) to sample from  $D_{\mathcal{L},s}$ . It is clear that

$$
\mathrm{Pr}_{\mathbf{x} \sim D_{\mathcal{L},s}}[\mathbf{x} = 0] = \rho_s(0) = \frac{1}{\rho_s(\mathcal{L})} \leq \frac{1}{17}.
$$

Furthermore, by Lemma [3,](#page-4-1) for any  $t \geq 1$ ,

$$
\mathrm{Pr}_{\mathbf{x} \sim D_{\mathcal{L},s}} \left[ \|\mathbf{x}\| > ts\sqrt{\frac{n}{2\pi}} \right] < \left( t \exp(\frac{1-t^2}{2}) \right)^n.
$$

Let  $\alpha = \frac{15}{17}$  and apply Lemma [4](#page-4-2) to get that if  $t^2 = t(n)^2 := 1 + \sqrt{\frac{-4}{n} \log \alpha} - \frac{2}{n} \log \alpha$  then

$$
\mathrm{Pr}_{\mathbf{x} \sim D_{\mathcal{L},s}} \left[ \mathbf{x} = 0 \text{ or } ||\mathbf{x}|| > ts\sqrt{\frac{n}{2\pi}} \right] \leq \frac{1}{17} + \alpha = \frac{16}{17}.
$$

Observe here that the reason why we wanted to simultaneously both  $\rho_{s_{\varepsilon}}(\mathcal{L})$  and  $\eta_{\varepsilon}(\mathcal{L})$  in Corollary [2](#page-10-0) is precisely so that the concentration bound in Lemma [3](#page-4-1) is high (*i.e.* we get short vectors on average) but not so high that we only get the 0 vector with overwhelming probability (by bounding  $\rho_s(0) = 1 \rho_s(\mathcal{L})$ ).

As a result,

$$
\Pr_{\mathbf{x}_1,\dots,\mathbf{x}_N \sim D_{\mathcal{L},s}} \left[ \exists i. \mathbf{x}_i \neq 0 \text{ and } \|\mathbf{x}_i\| \leqslant ts\sqrt{\frac{n}{2\pi}} \right]
$$
\n
$$
\geqslant 1 - \prod_{i=1}^n \Pr_{\mathbf{x}_i \sim D_{\mathcal{L},s}} \left[ \mathbf{x}_i = 0 \text{ or } \|\mathbf{x}_i\| > ts\sqrt{\frac{n}{2\pi}} \right]
$$
\n
$$
\geqslant 1 - \left(\frac{16}{17}\right)^N.
$$

Therefore, it suffices to take *N* sufficiently large (and constant) to get that, with probability at least 1*/*2, the algorithm will return a nonzero vector of length at most

$$
st\sqrt{\frac{n}{2\pi}} \leqslant t(n)\sqrt{\frac{n}{2\pi}} \cdot 24^{1/n}.
$$

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 but our random lattices are scaled to have volume 1). This is known as the  $\alpha$ -Hermite SVP (HSVP). The more common  $\alpha$ -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  $\lambda_1$  for random lattices.

<span id="page-12-0"></span>**Corollary 3.** For every  $n \geq 1$  and  $\alpha \in [0,1]$ , there is a randomized algorithm that *on a fraction at least*  $1 - 2^{1-n/2}(1 + o(1)) - \frac{2\alpha^n(1+o(1))}{(2-\alpha^n)^2}$ (2−*αn*) <sup>2</sup> *of random lattices* L *according to*  $\mu_n$ , outputs in time and space  $2^{n/2+o(n)}$  a nonzero vector of  $\mathcal L$  of length at most  $t(n)\sqrt{e} \cdot 24^{1/n} \alpha^{-1} \lambda_1(\mathcal{L})$  *with probability at least*  $1/2$ *, where*  $t(n)$  *is defined in Theorem [5.](#page-11-0)* 

 $\Box$ 

 $\Box$ 

*Proof.* We apply Theorem [5](#page-11-0) to get an algorithm that returns a nonzero vector on a lattice L with probability at least  $1/2$  and of length at most  $t(n)\sqrt{\frac{n}{2\pi}} \cdot 24^{1/n}$ . This algorithm works on a fraction at least  $1 - \varepsilon$  of lattices *L* where  $\varepsilon = 2^{1-n/2}(1 + o(1))$ . We further apply Theorem [4](#page-7-0) to get that for a fraction at least  $1 - \varepsilon'$  of lattices, where  $\varepsilon' = \frac{2\alpha^n \zeta(n)}{2 - \alpha^n}$ , we have  $\lambda_1 \geq \alpha \text{ vol}(B_n)^{-1/n}$ . Therefore, for a fraction at least  $1 - \varepsilon - \varepsilon'$  of lattices, the nonzero vector returned by the algorithm is of length at most  $\ell \cdot \lambda_1(\mathcal{L})$  where

$$
\ell = \frac{t(n)\sqrt{\frac{n}{2\pi}} \cdot 24^{1/n}}{\lambda_1(\mathcal{L})} \leq \frac{t(n)\sqrt{\frac{n}{2\pi}} \cdot 24^{1/n}}{\alpha \operatorname{vol}(B_n)^{-1/n}}.
$$

But  $\mathrm{vol}(B_n) \sim \frac{1}{\sqrt{n\pi}} \left(\frac{2\pi e}{n}\right)^{n/2}$  so

$$
\text{vol}(B_n)^{1/n} = \sqrt{\frac{2\pi e}{n}} e^{-\frac{1}{2n}\ln(n\pi) + o(1/n)} = \sqrt{\frac{2\pi e}{n}} e^{o(1)} = \sqrt{\frac{2\pi e}{n}} (1 + o(1))
$$

which gives the result.

### **5 Discussion and open questions**

We have shown a conceptually simple algorithm to solve  $(1 + o(1))\sqrt{e}$ -SVP and  $(1 + o(1))$  $o(1)$ ) $\sqrt{\frac{n}{2\pi}}$ -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 sample in subexponential space. With our results, this question becomes even more relevant since any improvement in the space complexity would translate into a similar improvement for for  $(1 + o(1))\sqrt{e}$ -SVP and  $(1+o(1))\sqrt{\frac{n}{2\pi}}$ -HSVP (on random lattices).

Another open question concerns our probabilistic bound (Corollary [2\)](#page-10-0) 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  $\varepsilon$  becomes sufficiently small,  $s_{\varepsilon} \sim 2^{1/n} \varepsilon^{-2/n}$ . Combining this with the upper bound (Theorem [4\)](#page-7-0) on  $\lambda_1(\mathcal{L})$  we get that for small values of  $\varepsilon$ ,

<span id="page-13-0"></span>
$$
\lambda_1(\mathcal{L})\eta_{\varepsilon}(\widehat{\mathcal{L}}) \leqslant (1 + o(1))\sqrt{\frac{n}{2\pi e}}\varepsilon^{-2/n}.
$$
\n(4)

This should be compared with the unconditional result of [\[3,](#page-14-9) Lemma 6.1] that shows that

<span id="page-13-1"></span>
$$
\sqrt{\frac{\log(1/\varepsilon)}{\pi}} < \lambda_1(\mathcal{L})\eta_{\varepsilon}(\widehat{\mathcal{L}}) < \sqrt{\frac{\beta(\mathcal{L})^2 n}{2\pi e}} \cdot \varepsilon^{-1/n} \cdot (1 + o(1)) \tag{5}
$$

where  $\beta(\mathcal{L}) \leq 2^{0.401}$  is the generalized kissing number [\[1\]](#page-14-6). 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 [\(4\)](#page-13-0) and the bound [\(5\)](#page-13-1) of [\[3\]](#page-14-9):  $\varepsilon^{-2/n}$  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 [2\)](#page-10-0) being suboptimal.

### **References**

- <span id="page-14-6"></span>[1] 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](https://doi.org/10.4230/LIPIcs.STACS.2021.4).
- <span id="page-14-0"></span>[2] Divesh Aggarwal, Daniel Dadush, Oded Regev, and Noah Stephens-Davidowitz. Solving the shortest vector problem in  $2<sup>n</sup>$  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:](https://doi.org/10.1145/2746539.2746606) [10.1145/2746539.2746606](https://doi.org/10.1145/2746539.2746606).
- <span id="page-14-9"></span>[3] 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 *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, 2015. [doi:10.1145/2746539.2746606](https://doi.org/10.1145/2746539.2746606).
- <span id="page-14-5"></span>[4] 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.
- <span id="page-14-3"></span>[5] 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.
- <span id="page-14-1"></span>[6] 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>.
- <span id="page-14-7"></span>[7] 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](https://doi.org/10.1145/276698.276705).
- <span id="page-14-4"></span>[8] 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.
- <span id="page-14-8"></span>[9] Yoshinori Aono, , THOMAS ESPITAU, and Phong Q. Nguyen. Random lattices: Theory and practice. URL: [https://api.semanticscholar.org/CorpusID:](https://api.semanticscholar.org/CorpusID:271090054) [271090054](https://api.semanticscholar.org/CorpusID:271090054).
- <span id="page-14-2"></span>[10] 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](https://doi.org/10.1007/978-3-031-62743-9_12).
- <span id="page-15-0"></span>[11] 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:](https://doi.org/10.1137/1.9781611974331.CH2) [10.1137/1.9781611974331.CH2](https://doi.org/10.1137/1.9781611974331.CH2).
- <span id="page-15-1"></span>[12] 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](https://doi.org/10.1109/EuroSP.2018.00032).
- <span id="page-15-10"></span>[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](https://doi.org/10.1145/2488608.2488680).
- <span id="page-15-6"></span>[14] 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](https://doi.org/10.1007/3-540-39568-7_27).
- <span id="page-15-9"></span>[15] Ioannis Chatzigeorgiou. Bounds on the lambert function and their application to the outage analysis of user cooperation. *IEEE Communications Letters*, 17(8):1505–1508, 2013. [doi:10.1109/LCOMM.2013.070113.130972](https://doi.org/10.1109/LCOMM.2013.070113.130972).
- <span id="page-15-5"></span>[16] 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](https://doi.org/10.1109/49.29612).
- <span id="page-15-7"></span>[17] 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](https://doi.org/10.1007/978-3-031-07082-2_23).
- <span id="page-15-2"></span>[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](https://doi.org/10.13154/tches.v2018.i1.238-268).
- <span id="page-15-3"></span>[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>.
- <span id="page-15-4"></span>[20] András Frank and Éva Tardos. An application of simultaneous diophantine approximation in combinatorial optimization. *Combinatorica*, 7(1):49–65, 1987. [doi:](https://doi.org/10.1007/BF02579200) [10.1007/BF02579200](https://doi.org/10.1007/BF02579200).
- <span id="page-15-8"></span>[21] 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](https://doi.org/10.1145/1374376.1374408).
- <span id="page-16-8"></span>[22] 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](https://doi.org/10.1145/1374376.1374407).
- <span id="page-16-1"></span>[23] 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](https://doi.org/10.1287/moor.8.4.538).
- <span id="page-16-2"></span>[24] 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](https://doi.org/10.1287/moor.12.3.415).
- <span id="page-16-13"></span>[25] 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/s10623-020-007](https://doi.org/10.1007/s10623-020-00719-w) [19-w](https://doi.org/10.1007/s10623-020-00719-w), [doi:10.1007/S10623-020-00719-W](https://doi.org/10.1007/S10623-020-00719-W).
- <span id="page-16-7"></span>[26] 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.
- <span id="page-16-4"></span>[27] 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](https://doi.org/10.1145/2455.2461).
- <span id="page-16-0"></span>[28] A.K. Lenstra, H.W. Lenstra, and Lászlo Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261:515–534, 1982.
- <span id="page-16-10"></span>[29] 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, April 1958. URL: [https://www.cambridge.org/core/product/identifier/](https://www.cambridge.org/core/product/identifier/S0305004100033302/type/journal_article) [S0305004100033302/type/journal\\_article](https://www.cambridge.org/core/product/identifier/S0305004100033302/type/journal_article), [doi:10.1017/S0305004100033302](https://doi.org/10.1017/S0305004100033302).
- <span id="page-16-11"></span>[30] 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](https://doi.org/10.1017/S0305004100033302).
- <span id="page-16-6"></span>[31] 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](https://doi.org/10.1109/FOCS.2004.72).
- <span id="page-16-9"></span>[32] C. A. Rogers. Mean values over the space of lattices. *Acta Mathematica*, 94(0):249–287, 1955. [doi:10.1007/BF02392493](https://doi.org/10.1007/BF02392493).
- <span id="page-16-12"></span>[33] C. A. Rogers. The number of lattice points in a set. *Proceedings of the London Mathematical Society*, s3-6(2):305–320, 1956. URL: [https://londmathsoc.on](https://londmathsoc.onlinelibrary.wiley.com/doi/abs/10.1112/plms/s3-6.2.305) [linelibrary.wiley.com/doi/abs/10.1112/plms/s3-6.2.305](https://londmathsoc.onlinelibrary.wiley.com/doi/abs/10.1112/plms/s3-6.2.305), [arXiv:https:](https://arxiv.org/abs/https://londmathsoc.onlinelibrary.wiley.com/doi/pdf/10.1112/plms/s3-6.2.305) [//londmathsoc.onlinelibrary.wiley.com/doi/pdf/10.1112/plms/s3-6.2.305](https://arxiv.org/abs/https://londmathsoc.onlinelibrary.wiley.com/doi/pdf/10.1112/plms/s3-6.2.305), [doi:10.1112/plms/s3-6.2.305](https://doi.org/10.1112/plms/s3-6.2.305).
- <span id="page-16-5"></span>[34] C.P. Schnorr. A hierarchy of polynomial time lattice basis reduction algorithms. *Theoretical Computer Science*, 53(2):201–224, 1987. URL: [https://www.sciencedir](https://www.sciencedirect.com/science/article/pii/0304397587900648) [ect.com/science/article/pii/0304397587900648](https://www.sciencedirect.com/science/article/pii/0304397587900648), [doi:10.1016/0304-3975\(87](https://doi.org/10.1016/0304-3975(87)90064-8) [\)90064-8](https://doi.org/10.1016/0304-3975(87)90064-8).
- <span id="page-16-3"></span>[35] 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/](https://doi.org/10.1109/TIT.1984.1056964) [TIT.1984.1056964](https://doi.org/10.1109/TIT.1984.1056964).
- <span id="page-17-0"></span>[36] 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/196](https://www.jstor.org/stable/1969027?origin=crossref) [9027?origin=crossref](https://www.jstor.org/stable/1969027?origin=crossref), [doi:10.2307/1969027](https://doi.org/10.2307/1969027).
- <span id="page-17-2"></span>[37] Noah Stephens-Davidowitz. *On the Gaussian measure over lattices*. Phd thesis, New York University, 2017.
- <span id="page-17-3"></span>[38] 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](https://doi.org/10.1109/TIT.2019.2901497).
- <span id="page-17-1"></span>[39] 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.