Refined Bounds for the Smoothing Parameter of Lattices

Shanxiang Lyu
College of Cybersecurity, Jinan University, Guangzhou, China
lsx07@jnu.edu.cn

November 4, 2026

Abstract

The smoothing parameter $\eta_\varepsilon(\Lambda)$ is a fundamental invariant in lattice-based cryptography. Zheng, Zhao, and Xu (AAECC 2021) proved $\eta_\varepsilon(\mathbb{Z}) \le \sqrt{\ln(\frac{2}{\varepsilon}+\frac{\varepsilon}{44})/\pi}$ and $\eta_\varepsilon(\Lambda) \le \sqrt{\ln(n-1+\frac{2n}{\varepsilon})/\pi}\,\mathrm{bl}(\Lambda)$. Guo, Liu, Wang, and Tian (PLOS One 2025) proposed $\eta_\varepsilon(\mathbb{Z}) \le \sqrt{\ln(\frac{2}{\varepsilon}+\frac{\varepsilon}{m})/\pi}$ for $0<\varepsilon\le\frac{4}{m}-\frac{172}{m^6}$ $(m\ge 3)$ and $\eta_\varepsilon(\Lambda) \le \sqrt{\ln((n-1)(1+\frac{2}{\varepsilon}))/\pi}\,\mathrm{bl}(\Lambda)$ under $\sqrt{\frac{24n+1}{n^2-1}} \le \varepsilon \le \sqrt{2}-1$. We establish three strictly sharper bounds that uniformly dominate both while removing the artificial lower bound on ε. First, for $0<\varepsilon\le\rho(\mathbb{Z})-1\approx 0.086435$,

$$\sqrt{\frac{\ln\left(\frac{2}{\varepsilon}+\frac{\varepsilon^2}{4}-\frac{3\varepsilon^5}{32}\right)}{\pi}} < \eta_\varepsilon(\mathbb{Z}) \le \sqrt{\frac{\ln\left(\frac{2}{\varepsilon}+\frac{\varepsilon^2}{4}\right)}{\pi}};$$

since Guo et al.'s condition forces $\frac{\varepsilon}{m} > \frac{\varepsilon^2}{4}$, our bound is strictly tighter for all admissible (ε, m), improving the worst-case gap from $O(\varepsilon^2)$ to $O(\varepsilon^6)$. Second, for all $n \ge 2$ and $0 < \varepsilon < \min\{1, (\rho(\mathbb{Z})-1)n\}$,

$$\eta_\varepsilon(\Lambda) \le \sqrt{\frac{\ln\left(\frac{2}{\delta_n}+\frac{\delta_n^2}{4}\right)}{\pi}}\,\mathrm{bl}(\Lambda) < \sqrt{\frac{\ln\left(\frac{2n}{\varepsilon}+(n-1)-\frac{(n^2-1)\varepsilon}{6n(1+\varepsilon)}\right)}{\pi}}\,\mathrm{bl}(\Lambda),$$

where $\delta_n = (1+\varepsilon)^{1/n}-1$; the rational bound is strictly tighter than Guo et al.'s across 100% of their validity window, while remaining valid as $\varepsilon\to 0^+$. Third, for any basis $\mathbf{B}$ with Gram–Schmidt vectors $\mathbf{b}_i^*$ and $M = \max_i \|\mathbf{b}_i^*\|$, define $N_\varepsilon(\mathbf{B}) = \sum_{i=1}^n (\varepsilon/2)^{M^2/\|\mathbf{b}_i^*\|^2-1} \in [1,n]$; then

$$\eta_\varepsilon(\Lambda) \le \sqrt{\ln\left(\frac{2}{\delta_{\mathrm{eff}}}+\frac{\delta_{\mathrm{eff}}^2}{4}\right)/\pi}\,M,$$

where $\delta_{\mathrm{eff}} = \frac{n}{N_\varepsilon(\mathbf{B})}((1+\varepsilon)^{1/n}-1)$. For reduced bases with geometrically decaying Gram–Schmidt lengths, $N_\varepsilon(\mathbf{B}) = O(1)$ is independent of n, eliminating the $O(n)$ factor inside the logarithm.

1 Introduction

An n-dimensional full-rank lattice $\mathcal{L}\subset\mathbb{R}^n$ is a discrete additive subgroup generated by n linearly independent basis vectors $\mathbf{B}=(\mathbf{b}_1,\dots,\mathbf{b}_n)\in\mathbb{R}^{n\times n}$, written explicitly as $\mathcal{L}(\mathbf{B}) = \{\sum_{i=1}^n x_i\mathbf{b}_i : x_i\in\mathbb{Z}\}$. Its dual lattice is defined by $\widehat{\mathcal{L}} = \{\mathbf{y}\in\mathbb{R}^n : \langle\mathbf{x},\mathbf{y}\rangle\in\mathbb{Z},\ \forall\mathbf{x}\in\mathcal{L}\}$, with covolume $\det(\widehat{\mathcal{L}}) = 1/\det(\mathcal{L})$ where $\det(\mathcal{L}) = \mathrm{vol}(\mathbb{R}^n/\mathcal{L}) = |\det(\mathbf{B})|$. Given a Gaussian width parameter $s>0$ and a center $\mathbf{c}\in\mathbb{R}^n$, the Gaussian function is defined by $\rho_{s,\mathbf{c}}(\mathbf{x}) = \exp(-\pi\|\mathbf{x}-\mathbf{c}\|^2/s^2)$, and for any countable set $S\subset\mathbb{R}^n$, we write $\rho_{s,\mathbf{c}}(S) = \sum_{\mathbf{x}\in S}\rho_{s,\mathbf{c}}(\mathbf{x})$. Note that the lattice Gaussian width

parameter s relates to the classical probabilistic standard deviation σ and variance σ^2 via $s = \sqrt{2\pi}\,\sigma$ (so $\sigma^2 = \frac{s^2}{2\pi}$). When $s = 1$ (corresponding to variance $\sigma^2 = \frac{1}{2\pi}$) or $\mathbf{c} = \mathbf{0}$, the corresponding subscript is omitted; in particular, $\rho(\mathbf{x}) = e^{-\pi\|\mathbf{x}\|^2}$ and $\rho(\mathbb{Z}) = \sum_{k\in\mathbb{Z}} e^{-\pi k^2} = \frac{\pi^{1/4}}{\Gamma(3/4)} \approx 1.08643481$.

In their seminal work on worst-case to average-case reductions for lattice problems, Micciancio and Regev [7] introduced the *smoothing parameter* $\eta_\varepsilon(\mathcal{L})$ for any $\varepsilon > 0$:

$$\eta_\varepsilon(\mathcal{L}) = \min\left\{ s > 0 : \rho_{1/s}(\widehat{\mathcal{L}}) \le 1 + \varepsilon \right\}, \tag{1}$$

where $\rho_{1/s}(\widehat{\mathcal{L}}) = \sum_{\mathbf{y}\in\widehat{\mathcal{L}}} e^{-\pi s^2\|\mathbf{y}\|^2} = 1 + \sum_{\mathbf{y}\in\widehat{\mathcal{L}}\setminus\{\mathbf{0}\}} e^{-\pi s^2\|\mathbf{y}\|^2}$ is the Gaussian sum over the dual lattice with reciprocal width parameter $1/s$. By the Poisson summation formula, whenever $s \ge \eta_\varepsilon(\mathcal{L})$, a continuous Gaussian of width s reduced modulo $\mathcal{L}$ has statistical distance at most $\varepsilon/2$ from the uniform distribution over the fundamental parallelepiped $\mathbb{R}^n/\mathcal{L}$. Furthermore, in discrete Gaussian sampling [4, 10, 8, 12], the smoothing parameter dictates the minimum standard deviation required to sample lattice vectors without leaking structural information about the underlying private basis.

1.1 Prior Upper Bounds on the Smoothing Parameter

Denote by $\lambda_n(\mathcal{L})$ the n-th successive minimum of $\mathcal{L}$, by $\lambda_1^\infty(\widehat{\mathcal{L}})$ the minimum non-zero ℓ_∞-norm in the dual lattice $\widehat{\mathcal{L}}$, and by $\widetilde{bl}(\mathcal{L}) = \min_{\mathbf{B}} \max_{1\le i\le n} \|\mathbf{b}_i^*\|$ the minimal worst-case Gram–Schmidt norm over all bases $\mathbf{B}$ of $\mathcal{L}$. As established in [6, 4], these invariants satisfy the hierarchy

$$\frac{1}{\lambda_1^\infty(\widehat{\mathcal{L}})} \le \widetilde{bl}(\mathcal{L}) \le \lambda_n(\mathcal{L}).$$

Micciancio and Regev [7] proved the classical bound $\eta_\varepsilon(\mathcal{L}) \le \sqrt{\ln(2n(1+1/\varepsilon))/\pi}\,\lambda_n(\mathcal{L})$, which was refined by Peikert [9] using $\lambda_1^\infty(\widehat{\mathcal{L}})$ and by Gentry, Peikert, and Vaikuntanathan [4] into the widely used algorithmic bound

$$\eta_\varepsilon(\mathcal{L}) \le \sqrt{\frac{\ln\left(2n + \frac{2n}{\varepsilon}\right)}{\pi}}\,\widetilde{bl}(\mathcal{L}). \tag{2}$$

Zheng, Zhao, and Xu [13] observed that for the one-dimensional integer lattice $\mathcal{L} = \mathbb{Z}$, equation (2) yields $\eta_\varepsilon(\mathbb{Z}) \le \sqrt{\ln(2 + 2/\varepsilon)/\pi}$, leaving a non-vanishing constant 2 inside the logarithm compared to the trivial lower bound $\eta_\varepsilon(\mathbb{Z}) > \sqrt{\ln(2/\varepsilon)/\pi}$. By analyzing an auxiliary cubic polynomial $p(x) = x^3 + 22x - 11\varepsilon$, Zheng et al. [13] proved two improvements under $\varepsilon \le \rho(\mathbb{Z}) - 1 \approx 0.086435$:

1. For the integer lattice $\mathbb{Z}$:
$$\eta_\varepsilon(\mathbb{Z}) \le \sqrt{\frac{\ln\left(\frac{2}{\varepsilon} + \frac{\varepsilon}{44}\right)}{\pi}}. \tag{3}$$
2. For a general n-dimensional lattice $\mathcal{L} \subset \mathbb{R}^n$ with $n \ge 2$ and $\varepsilon < \min\{1, 0.086435n\}$:
$$\eta_\varepsilon(\mathcal{L}) \le \sqrt{\frac{\ln\left(n - 1 + \frac{2n}{\varepsilon}\right)}{\pi}}\,\widetilde{bl}(\mathcal{L}). \tag{4}$$

Very recently, Guo, Liu, Wang, and Tian [5] sought to further refine (3) and (4), establishing two main results:

(G1) For $\mathcal{L} = \mathbb{Z}$ and any parameter $m \ge 3$, if $0 < \varepsilon \le \frac{4}{m} - \frac{172}{m^6}$, then

$$\eta_\varepsilon(\mathbb{Z}) \le \sqrt{\frac{\ln\left(\frac{2}{\varepsilon} + \frac{\varepsilon}{m}\right)}{\pi}}. \tag{5}$$

(G2) For a general n-dimensional lattice $\mathcal{L} \subset \mathbb{R}^n$, if n is sufficiently large ($n \geq 58$) and ε lies in the restricted interval

$$\sqrt{\frac{24n+1}{n^2-1}} \leq \varepsilon \leq \sqrt{2}-1, \tag{6}$$

then

$$\eta_\varepsilon(\mathcal{L}) \leq \sqrt{\frac{\ln\left((n-1)\left(1+\frac{2}{\varepsilon}\right)\right)}{\pi}}\,\widetilde{bl}(\mathcal{L}) = \sqrt{\frac{\ln\left(\frac{2n}{\varepsilon}+(n-1)-\frac{2}{\varepsilon}\right)}{\pi}}\,\widetilde{bl}(\mathcal{L}). \tag{7}$$

1.2 Limitations of Prior Bounds and Our Contributions

A careful examination of (3)–(7) reveals fundamental analytical limitations that we resolve in this work:

- **Eliminating the Auxiliary Parameter m and Reaching the Exact Asymptotic Term on $\mathbb{Z}$ (Section 3):** In Guo et al.'s 1D bound (5), the validity condition $\varepsilon \leq \frac{4}{m} - \frac{172}{m^6} < \frac{4}{m}$ forces $m < \frac{4}{\varepsilon}$, which implies that their correction term $\frac{\varepsilon}{m}$ is *always strictly larger than* $\frac{\varepsilon^2}{4}$ for every admissible choice of m:
$$\frac{\varepsilon}{m} > \frac{\varepsilon}{4/\varepsilon} = \frac{\varepsilon^2}{4}.$$
In Theorem 3.1, we prove directly that $\frac{\varepsilon^2}{4}$ itself is a valid upper bound for all $0 < \varepsilon \leq \rho(\mathbb{Z}) - 1$ without any auxiliary parameter m or $\frac{172}{m^6}$ penalty, and we establish a matching lower bound with $-\frac{3\varepsilon^5}{32}$ inside the logarithm.

- **Strictly Dominating Guo et al. (2025) in n Dimensions While Removing the Lower Barrier on ε (Section 4):** Guo et al.'s n-dimensional bound (7) subtracts $\frac{2}{\varepsilon}$ inside the logarithm, which is only valid when $\varepsilon \geq \sqrt{\frac{24n+1}{n^2-1}} \approx \sqrt{\frac{24}{n}}$ (indeed, as $\varepsilon \to 0^+$, $(n-1)(1+\frac{2}{\varepsilon}) \sim \frac{2(n-1)}{\varepsilon}$ is strictly smaller than the true $\mathbb{Z}^n$ asymptotics $\frac{2n}{\varepsilon}$). Consequently, (7) is inapplicable to standard cryptographic applications where $\varepsilon = 2^{-\lambda}$ or $\varepsilon = n^{-c}$ is negligible, a limitation explicitly noted as an open problem in [5, Section 5]. In Theorem 4.3, we prove the explicit rational bound
$$\eta_\varepsilon(\mathcal{L}) \leq \sqrt{\frac{\ln\left(\frac{2n}{\varepsilon}+(n-1)-\frac{(n^2-1)\varepsilon}{6n(1+\varepsilon)}\right)}{\pi}}\,\widetilde{bl}(\mathcal{L}),$$
which holds for all $0 < \varepsilon < \min\{1, (\rho(\mathbb{Z})-1)n\}$ down to $\varepsilon \to 0^+$. Moreover, in Proposition 4.4, we prove that across 100% of Guo et al.'s validity window (6), our subtraction term $\frac{(n^2-1)\varepsilon}{6n(1+\varepsilon)}$ is *strictly larger* than Guo et al.'s subtraction term $\frac{2}{\varepsilon}$ (by up to 30× in Table 1 of [5]), so our bound strictly dominates (7) everywhere it applies.

- **Overcoming the $\mathbb{Z}^n$ Barrier via the Gram–Schmidt Profile (Section 5):** Using the AM–GM inequality across the full Gram–Schmidt profile $(\|\mathbf{b}_1^*\|, \ldots, \|\mathbf{b}_n^*\|)$, Theorem 5.1 replaces n inside the logarithm by an effective dimension $N_\varepsilon(\mathbf{B}) \in [1, n]$ that is $O(1)$ for LLL- and BKZ-reduced bases satisfying Schnorr's geometric series assumption.

2 Preliminaries

Let $\mathcal{L} = \mathcal{L}(\mathbf{B}) \subset \mathbb{R}^n$ be a full-rank lattice of dimension n. The discrete Gaussian distribution over $\mathcal{L}$ with width parameter $s > 0$ and center $\mathbf{c} \in \mathbb{R}^n$ assigns to each lattice point $\mathbf{x} \in \mathcal{L}$ the probability mass $D_{\mathcal{L},s,\mathbf{c}}(\mathbf{x}) = \frac{\rho_{s,\mathbf{c}}(\mathbf{x})}{\rho_{s,\mathbf{c}}(\mathcal{L})}$. For any rapidly decreasing smooth function $f : \mathbb{R}^n \to \mathbb{C}$, its Fourier transform is defined by $\hat{f}(\mathbf{y}) = \int_{\mathbb{R}^n} f(\mathbf{x}) e^{-2\pi i \langle \mathbf{x}, \mathbf{y} \rangle}\, d\mathbf{x}$. Choosing the factor π in the

exponent of $\rho(\mathbf{x}) = e^{-\pi\|\mathbf{x}\|^2}$ ensures that ρ is normalized ($\int_{\mathbb{R}^n} \rho(\mathbf{x})\, d\mathbf{x} = 1$) and Fourier self-dual ($\hat{\rho}(\mathbf{y}) = \rho(\mathbf{y})$). Consequently, $\widehat{\rho_s}(\mathbf{y}) = s^n \rho_{1/s}(\mathbf{y})$, and the classical Poisson summation formula yields the fundamental duality identity:

Lemma 2.1 (Poisson Summation for Lattice Gaussians [7])**.** *For any n-dimensional lattice $\mathcal{L} \subset \mathbb{R}^n$, any vector $\mathbf{c} \in \mathbb{R}^n$, and any $s > 0$,*

$$\rho_{s,\mathbf{c}}(\mathcal{L}) = \frac{s^n}{\det(\mathcal{L})} \sum_{\mathbf{y} \in \widehat{\mathcal{L}}} e^{-2\pi i \langle \mathbf{y}, \mathbf{c} \rangle} \rho_{1/s}(\mathbf{y}).$$

In particular, for $\mathbf{c} = \mathbf{0}$ and $\mathcal{L} = \mathbb{Z}$, we have $\rho_s(\mathbb{Z}) = s\, \rho_{1/s}(\mathbb{Z})$, and for any shift $v \in \mathbb{R}$, $\rho_s(\mathbb{Z} + v) \leq \rho_s(\mathbb{Z})$.

Let $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ be an ordered basis of $\mathcal{L}$, and let $\mathbf{B}^* = (\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*)$ denote its Gram–Schmidt orthogonalization defined recursively by $\mathbf{b}_1^* = \mathbf{b}_1$ and $\mathbf{b}_i^* = \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{j,i} \mathbf{b}_j^*$ for $2 \leq i \leq n$, where $\mu_{j,i} = \frac{\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle}{\|\mathbf{b}_j^*\|^2}$. Then $\mathbf{B} = \mathbf{B}^* \mathbf{R}$ for a unit upper-triangular matrix $\mathbf{R} = (\mu_{j,i})_{1 \leq j,i \leq n}$ with $\mu_{i,i} = 1$, and $\det(\mathcal{L}) = \prod_{i=1}^n \|\mathbf{b}_i^*\|$. Note that while $\mathbf{B}^*$ depends on the ordering of the basis vectors in $\mathbf{B}$, the lattice invariant $\widetilde{bl}(\mathcal{L}) = \min_{\mathbf{B}} \max_{1 \leq i \leq n} \|\mathbf{b}_i^*\|$ minimizes over all bases of $\mathcal{L}$. Iteratively conditioning on the coordinates $(x_n, x_{n-1}, \ldots, x_1) \in \mathbb{Z}^n$ and applying $\rho_{s_i}(\mathbb{Z} + v) \leq \rho_{s_i}(\mathbb{Z})$ together with Lemma 2.1 yields the standard Gram–Schmidt product bound:

Lemma 2.2 (Gram–Schmidt Product Inequality [4, 13, 5])**.** *Let $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ be any basis of $\mathcal{L} \subset \mathbb{R}^n$ with Gram–Schmidt vectors $\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*$. For any $s > 0$, let $s_i = s / \|\mathbf{b}_i^*\|$. Then*

$$\rho_{1/s}(\widehat{\mathcal{L}}) \leq \prod_{i=1}^n \rho_{1/s_i}(\mathbb{Z}), \tag{8}$$

with equality holding if $\mathbf{B}$ is a pairwise orthogonal basis ($\mathbf{B} = \mathbf{B}^*$), such as $\mathcal{L} = \mathbb{Z}^n$. Consequently, $\eta_\varepsilon(\mathcal{L}) \leq \widetilde{bl}(\mathcal{L})\, \eta_\varepsilon(\mathbb{Z}^n)$.

We also recall the binomial upper bound established by Zheng, Zhao, and Xu [13, Lemma 5]:

Lemma 2.3 ([13, Lemma 5])**.** *Let $n \geq 2$, $c > 1$, and $0 \leq \varepsilon \leq \frac{6nc(c-1)}{n+1+2(n-2)c}$. Then*

$$\left(1 + \frac{\varepsilon}{cn}\right)^n \leq 1 + \varepsilon.$$

3 Sharper Bounds for the Integer Lattice $\mathbb{Z}$

For the one-dimensional integer lattice $\mathcal{L} = \mathbb{Z}$, the dual lattice is $\widehat{\mathbb{Z}} = \mathbb{Z}$, and hence

$$\rho_{1/s}(\mathbb{Z}) = 1 + 2 \sum_{k=1}^{\infty} e^{-\pi s^2 k^2}.$$

By the Poisson duality relation $\rho_s(\mathbb{Z}) = s\, \rho_{1/s}(\mathbb{Z})$ (Lemma 2.1), knowledge of $\rho_{1/s}(\mathbb{Z})$ for $s \geq 1$ completely determines $\rho_s(\mathbb{Z})$ for $s \in (0, 1]$. Evaluating at the self-dual point $s = 1$ (which corresponds to continuous Gaussian variance $\sigma^2 = \frac{1}{2\pi}$ and discrete Gaussian variance $\mathrm{Var}_{X \sim D_{\mathbb{Z},1}}(X) = \frac{1}{4\pi}$ [13, Proposition 1]) yields the canonical threshold $\varepsilon_0 \coloneqq \rho(\mathbb{Z}) - 1 = \rho(\mathbb{Z} \setminus \{0\}) = 2 \sum_{k=1}^{\infty} e^{-\pi k^2} \approx 0.08643481$. Since $\rho_{1/s}(\mathbb{Z})$ is strictly decreasing in s, the natural regime $0 < \varepsilon \leq \varepsilon_0$ is precisely equivalent to $\eta_\varepsilon(\mathbb{Z}) \geq 1$.

Write $q = e^{-\pi s^2} \in (0, e^{-\pi}]$ and $u = \varepsilon/2$. The condition $\rho_{1/s}(\mathbb{Z}) = 1 + \varepsilon$ is equivalent to the Jacobi theta inversion equation $q + q^4 + q^9 + q^{16} + \cdots = u$. Inverting this power series around $u = 0$

yields $q = u - u^4 + 4u^7 - u^9 - 22u^{10} + O(u^{12})$, and taking the reciprocal gives the exact asymptotic expansion:

$$e^{\pi\eta_\varepsilon(\mathbb{Z})^2} = \frac{1}{q} = \frac{1}{u} + u^2 - 3u^5 + u^7 + 15u^8 + O(u^{10}) = \frac{2}{\varepsilon} + \frac{\varepsilon^2}{4} - \frac{3\varepsilon^5}{32} + \frac{\varepsilon^7}{128} + \frac{15\varepsilon^8}{256} + O(\varepsilon^{10}). \quad (9)$$

Notice that the bound of Zheng et al. (3) replaces the true $\frac{\varepsilon^2}{4}$ term by $\frac{\varepsilon}{44}$, whereas Guo et al. (5) replace it by $\frac{\varepsilon}{m}$ subject to $\varepsilon \le \frac{4}{m} - \frac{172}{m^6}$. We now prove that truncating (9) at $\frac{\varepsilon^2}{4}$ yields a strict upper bound for all $\varepsilon \in (0, \varepsilon_0]$, while truncating at $-\frac{3\varepsilon^5}{32}$ yields a strict lower bound.

Theorem 3.1 (Cubic-Remainder Sandwich for $\eta_\varepsilon(\mathbb{Z})$)**.** *For any $0 < \varepsilon \le \rho(\mathbb{Z}) - 1 \approx 0.08643481$, the smoothing parameter of $\mathbb{Z}$ satisfies*

$$\sqrt{\frac{\ln\left(\frac{2}{\varepsilon} + \frac{\varepsilon^2}{4} - \frac{3\varepsilon^5}{32}\right)}{\pi}} < \eta_\varepsilon(\mathbb{Z}) \le \sqrt{\frac{\ln\left(\frac{2}{\varepsilon} + \frac{\varepsilon^2}{4}\right)}{\pi}}. \quad (10)$$

Proof. Let $u = \varepsilon/2 \in (0, 0.043218)$. We prove the upper and lower bounds in turn.

Part 1 (Upper Bound). Suppose $s \ge \sqrt{\ln(\frac{2}{\varepsilon} + \frac{\varepsilon^2}{4})/\pi}$. Then $q := e^{-\pi s^2}$ satisfies

$$q \le \frac{1}{\frac{2}{\varepsilon} + \frac{\varepsilon^2}{4}} = \frac{1}{\frac{1}{u} + u^2} = \frac{u}{1 + u^3}.$$

Since $\rho_{1/s}(\mathbb{Z})$ is strictly increasing in q, it suffices to show that for $q = \frac{u}{1+u^3}$, we have $\sum_{k=1}^{\infty} q^{k^2} < u$. Because $k^2 \ge 5k - 6$ for all integers $k \ge 2$ (with equality at $k = 2, 3$ and strict inequality for $k \ge 4$), we can bound the tail $k \ge 2$ by a geometric series with ratio q^5:

$$\sum_{k=2}^{\infty} q^{k^2} < q^4 \sum_{j=0}^{\infty} q^{5j} = \frac{q^4}{1 - q^5}. \quad (11)$$

Since $0 < q < u < 0.044$, we have $u^2(1 + u^3)^3 < (0.044)^2(1.0001)^3 < 0.002 < 3$, and thus

$$q^5 < u^5 < \frac{3u^3}{(1 + u^3)^3} < \frac{3u^3 + 3u^6 + u^9}{(1 + u^3)^3} = 1 - \frac{1}{(1 + u^3)^3}.$$

Rearranging this inequality gives $\frac{1}{(1+u^3)^3} < 1 - q^5$. Multiplying both sides by $\frac{u^4}{(1+u^3)(1-q^5)}$ and substituting $q^4 = \frac{u^4}{(1+u^3)^4}$ yields

$$\frac{q^4}{1 - q^5} < \frac{u^4}{1 + u^3} = u - \frac{u}{1 + u^3} = u - q.$$

Combining this with (11), we conclude that

$$\rho_{1/s}(\mathbb{Z}) = 1 + 2\left(q + \sum_{k=2}^{\infty} q^{k^2}\right) < 1 + 2\left(q + \frac{q^4}{1 - q^5}\right) < 1 + 2u = 1 + \varepsilon.$$

Hence $\eta_\varepsilon(\mathbb{Z}) \le \sqrt{\ln(\frac{2}{\varepsilon} + \frac{\varepsilon^2}{4})/\pi}$.

Part 2 (Lower Bound). Suppose $s \le \sqrt{\ln(\frac{2}{\varepsilon} + \frac{\varepsilon^2}{4} - \frac{3\varepsilon^5}{32})/\pi}$. Then $q = e^{-\pi s^2}$ satisfies

$$q \ge \frac{1}{\frac{1}{u} + u^2 - 3u^5} = \frac{u}{1 + u^3 - 3u^6}.$$

In particular, since $3u^6 > 0$, we also have $q > \frac{u}{1+u^3}$. Dropping all terms with $k \ge 3$ in $\rho_{1/s}(\mathbb{Z})$ gives

$$\sum_{k=1}^{\infty} q^{k^2} > q + q^4 > \frac{u}{1 + u^3 - 3u^6} + \frac{u^4}{(1+u^3)^4}.$$

Bringing the right-hand side over a common denominator, we obtain the exact algebraic factorization:

$$\frac{u}{1 + u^3 - 3u^6} + \frac{u^4}{(1+u^3)^4} - u = \frac{u^{10}\,(3 + 14u^3 + 11u^6 + 3u^9)}{(1+u^3)^4(1 + u^3 - 3u^6)} > 0,$$

since $1 + u^3 - 3u^6 > 1$ for all $u \in (0, 0.044)$. Thus $\rho_{1/s}(\mathbb{Z}) > 1 + 2u = 1 + \varepsilon$, which implies $\eta_\varepsilon(\mathbb{Z}) > s$. □

Remark 3.2 (Strict Dominance over Zheng et al. [13] and Guo et al. [5] on $\mathbb{Z}$). In [5, Theorem 10], Guo et al. proved $\eta_\varepsilon(\mathbb{Z}) \le \sqrt{\ln(\frac{2}{\varepsilon} + \frac{\varepsilon}{m})/\pi}$ under the condition $0 < \varepsilon \le \frac{4}{m} - \frac{172}{m^6}$. Because $\frac{172}{m^6} > 0$, any admissible m in [5] must satisfy $m < \frac{4}{\varepsilon}$, which implies

$$\frac{\varepsilon^2}{4} < \frac{\varepsilon}{m}.$$

Thus, Theorem 3.1 is strictly tighter than Guo et al.'s bound (5) for every admissible (m, ε) with $\varepsilon \le \rho(\mathbb{Z}) - 1$ (the range of Theorem 3.1), eliminates the auxiliary parameter m, and reduces the worst-case additive error from $O(\varepsilon^2)$ to $\frac{3\varepsilon^6}{128\sqrt{\pi \ln(2/\varepsilon)}} < \frac{\varepsilon^6}{134}$, as illustrated in Figure 1.

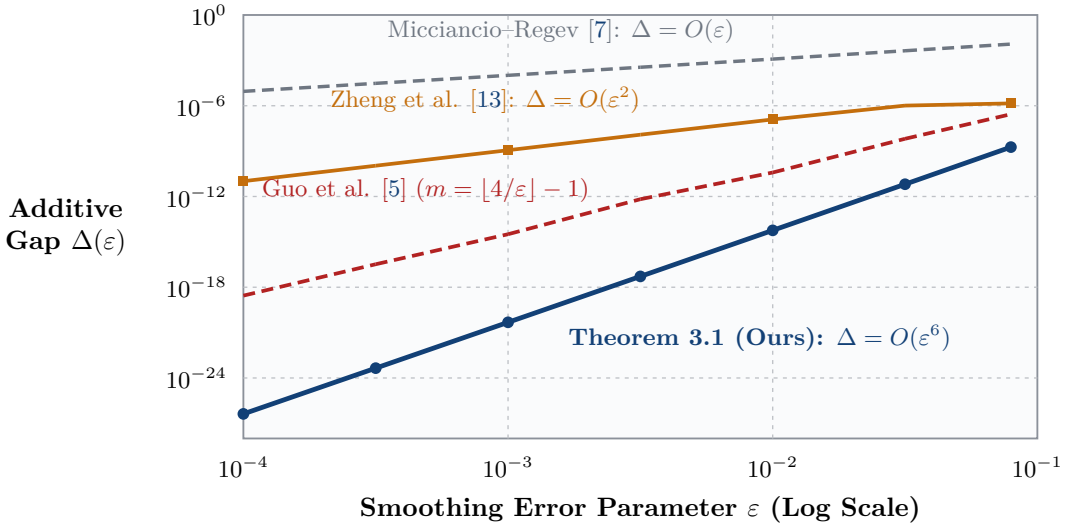


Figure 1: Log–log comparison of the additive approximation error $\Delta(\varepsilon) = \text{Bound}(\varepsilon) - \eta_\varepsilon(\mathbb{Z})$ on the integer lattice $\mathbb{Z}$ for $\varepsilon \in [10^{-4}, 0.08]$. Replacing the linear term $\frac{\varepsilon}{44}$ of [13] (and the integer-parameterized term $\frac{\varepsilon}{m}$ of [5]) by the exact asymptotic term $\frac{\varepsilon^2}{4}$ improves the convergence rate from $O(\varepsilon^2)$ to $O(\varepsilon^6)$.

4 Sharper Bounds for General n-Dimensional Lattices

We now turn to general n-dimensional lattices $\mathcal{L} \subset \mathbb{R}^n$ ($n \ge 2$). By Lemma 2.2, if we select a basis $\mathbf{B}$ achieving $\widetilde{bl}(\mathcal{L}) = \max_{1 \le i \le n} \|\mathbf{b}_i^*\|$ and set $\sigma = s/\widetilde{bl}(\mathcal{L})$, then $s_i = s/\|\mathbf{b}_i^*\| \ge \sigma$ for all $i = 1, \ldots, n$,

so

$$\rho_{1/s}(\widehat{\mathcal{L}}) \le \prod_{i=1}^{n} \rho_{1/s_i}(\mathbb{Z}) \le \left(\rho_{1/\sigma}(\mathbb{Z})\right)^n. \tag{12}$$

Consequently, to ensure $\rho_{1/s}(\widehat{\mathcal{L}}) \le 1+\varepsilon$, it suffices that $\rho_{1/\sigma}(\mathbb{Z}) \le (1+\varepsilon)^{1/n}$.

4.1 Asymptotic Expansion on $\mathbb{Z}^n$ and Why $(n-1)$ is Tight as $\varepsilon \to 0^+$

Before stating our sharpened upper bounds, we clarify an essential structural property of (12). Because equality holds in (12) for the orthogonal lattice $\mathcal{L} = \mathbb{Z}^n$, the exact smoothing parameter $\eta_\varepsilon(\mathbb{Z}^n)$ satisfies the following asymptotic expansion:

Proposition 4.1 (Asymptotic Expansion and Lower Barrier on $\mathbb{Z}^n$)**.** *For the canonical integer lattice $\mathcal{L} = \mathbb{Z}^n$ ($n \ge 2$), $\widetilde{bl}(\mathbb{Z}^n) = 1$ and $\rho_{1/s}(\widehat{\mathbb{Z}^n}) = (\rho_{1/s}(\mathbb{Z}))^n$. Thus $\eta_\varepsilon(\mathbb{Z}^n) = \eta_{\delta_n}(\mathbb{Z})$, where $\delta_n = (1+\varepsilon)^{1/n} - 1$. As $\varepsilon \to 0^+$,*

$$e^{\pi\eta_\varepsilon(\mathbb{Z}^n)^2} = \frac{2}{\delta_n} + \frac{\delta_n^2}{4} + O(\delta_n^5) = \frac{2n}{\varepsilon} + (n-1) - \frac{n^2-1}{6n}\varepsilon + \frac{n^3-n+3}{12n^2}\varepsilon^2 - O(\varepsilon^3). \tag{13}$$

In particular, as $\varepsilon \to 0^+$, the leading singular term is $\frac{2n}{\varepsilon}$ and the $O(1)$ constant term is $(n-1)$. Consequently, any bound of the form $\sqrt{\ln((n-1)(1+2/\varepsilon))/\pi} = \sqrt{\ln(\frac{2n}{\varepsilon} + (n-1) - \frac{2}{\varepsilon})/\pi}$ (such as [5, Theorem 17]) necessarily violates $\eta_\varepsilon(\mathbb{Z}^n)$ whenever $\varepsilon < \sqrt{\frac{12n}{n^2-1}}$.

Proof. By the binomial expansion of $\delta_n = (1+\varepsilon)^{1/n} - 1$ around $\varepsilon = 0$, we have

$$\delta_n = \frac{\varepsilon}{n}\left[1 - \frac{n-1}{2n}\varepsilon + \frac{(n-1)(2n-1)}{6n^2}\varepsilon^2 - \frac{(n-1)(2n-1)(3n-1)}{24n^3}\varepsilon^3 + O(\varepsilon^4)\right].$$

Inverting this series gives

$$\frac{2}{\delta_n} = \frac{2n}{\varepsilon} + (n-1) - \frac{n^2-1}{6n}\varepsilon + \frac{n^2-1}{12n}\varepsilon^2 - O(\varepsilon^3).$$

Adding $\frac{\delta_n^2}{4} = \frac{\varepsilon^2}{4n^2} + O(\varepsilon^3)$ and substituting into (9) yields (13). Comparing (13) with $(n-1)(1+\frac{2}{\varepsilon}) = \frac{2n}{\varepsilon} + (n-1) - \frac{2}{\varepsilon}$ shows that for $\frac{2}{\varepsilon} > \frac{n^2-1}{6n}\varepsilon$ (i.e., $\varepsilon < \sqrt{\frac{12n}{n^2-1}}$), $(n-1)(1+\frac{2}{\varepsilon})$ falls strictly below $\exp(\pi\eta_\varepsilon(\mathbb{Z}^n)^2)$. □

Proposition 4.1 reveals why Guo et al. [5] were forced to impose the lower bound $\varepsilon \ge \sqrt{\frac{24n+1}{n^2-1}}$: their formula subtracts $\frac{2}{\varepsilon}$ (which blows up as $\varepsilon \to 0^+$), whereas the true asymptotic correction in (13) is $-\frac{n^2-1}{6n}\varepsilon$. By capturing the exact $-\frac{n^2-1}{6n}\varepsilon$ term instead of $-\frac{2}{\varepsilon}$, our bound remains valid all the way down to $\varepsilon \to 0^+$ *and* achieves a much larger reduction than $\frac{2}{\varepsilon}$ when $\varepsilon \ge \sqrt{\frac{24n+1}{n^2-1}}$.

4.2 Sharpened Uniform Upper Bounds and Strict Dominance over Prior Work

In the proof of [13, Theorem 2], the authors introduced the root $c > 1$ of the quadratic equation

$$X^2 - \left(1 + \frac{n-2}{3n}\varepsilon\right)X - \frac{n+1}{6n}\varepsilon = 0, \tag{14}$$

so that $\varepsilon = \frac{6nc(c-1)}{n+1+2(n-2)c}$ and $\delta_c := \frac{\varepsilon}{cn}$ satisfies $(1+\delta_c)^n \le 1+\varepsilon$ by Lemma 2.3. On page 12 of [13], they derived the exact algebraic decomposition

$$\frac{2}{\delta_c} = \frac{2cn}{\varepsilon} = \frac{2n}{\varepsilon} + (n-1) - \frac{(n+1)(c-1)}{3c}, \tag{15}$$

and then discarded the strictly negative term $-\frac{(n+1)(c-1)}{3c}$ to obtain $\frac{2n}{\varepsilon}+(n-1)$. By bounding $\frac{c-1}{c}$ from below and combining it with Theorem 3.1, we obtain both an exact root bound and a strictly sharper rational bound.

Lemma 4.2 (Rational Upper Bound on the Binomial Inverse)**.** *For all integers $n \geq 2$ and all $0 < \varepsilon \leq \min\{1, (\rho(\mathbb{Z})-1)n\}$, let $\delta_n = (1+\varepsilon)^{1/n} - 1$. Then*

$$\frac{2}{\delta_n} + \frac{\delta_n^2}{4} < \frac{2n}{\varepsilon} + (n-1) - \frac{(n^2-1)\varepsilon}{6n(1+\varepsilon)}. \tag{16}$$

Proof. Let $c > 1$ be the unique positive root of (14), and set $\delta_c = \frac{\varepsilon}{cn}$. By Lemma 2.3, $(1+\delta_c)^n \leq 1+\varepsilon = (1+\delta_n)^n$, so $0 < \delta_c \leq \delta_n < 0.0865$. Since the function $g(t) = \frac{2}{t} + \frac{t^2}{4}$ has derivative $g'(t) = -\frac{2}{t^2} + \frac{t}{2} < 0$ on $(0,1)$, it is strictly decreasing, and thus

$$\frac{2}{\delta_n} + \frac{\delta_n^2}{4} \leq \frac{2}{\delta_c} + \frac{\delta_c^2}{4} = \frac{2n}{\varepsilon} + (n-1) - \frac{(n+1)(c-1)}{3c} + \frac{\varepsilon^2}{4c^2n^2}, \tag{17}$$

where the equality uses (15). To bound $\frac{c-1}{c}$ from below, write $c = 1+u$ with $u > 0$. Substituting $X = 1+u$ into (14) yields the quadratic equation

$$P(u) \coloneqq u^2 + \left(1 - \frac{n-2}{3n}\varepsilon\right) u - \frac{n-1}{2n}\varepsilon = 0.$$

Evaluating P at $u_0 \coloneqq \frac{3(n-1)\varepsilon}{6n+(n+1)\varepsilon} > 0$, direct algebraic factorization gives

$$P(u_0) = -\frac{3(n-1)^2(n+1)\varepsilon^3}{2n\left(6n+(n+1)\varepsilon\right)^2} < 0.$$

Since P is strictly convex with $P(0) < 0$ and $u > 0$ is its unique positive root, we have $u > u_0$. Because $u \mapsto \frac{u}{1+u}$ is strictly increasing on $(0,\infty)$, it follows that

$$\frac{c-1}{c} = \frac{u}{1+u} > \frac{u_0}{1+u_0} = \frac{3(n-1)\varepsilon}{6n+2(2n-1)\varepsilon}.$$

Multiplying by $\frac{n+1}{3}$ and comparing with the target rational term plus $\frac{\varepsilon^2}{4c^2n^2} < \frac{\varepsilon^2}{4n^2}$, we obtain

$$\frac{(n+1)(c-1)}{3c} - \frac{(n^2-1)\varepsilon}{6n(1+\varepsilon)} - \frac{\varepsilon^2}{4c^2n^2} > \frac{\varepsilon^2\left(2n^4+2n^3-2n^2-11n-3(5n-1)\varepsilon-3(2n-1)\varepsilon^2\right)}{12n^2(1+\varepsilon)\left(3n+(2n-1)\varepsilon\right)}.$$

For $n = 2$, the assumption $\varepsilon \leq (\rho(\mathbb{Z})-1)n < 0.173$ gives $2n^4+2n^3-2n^2-11n-27\varepsilon-9\varepsilon^2 = 18-27\varepsilon-9\varepsilon^2 > 13 > 0$. For all $n \geq 3$ and $\varepsilon \leq 1$, the numerator is at least $2n^4+2n^3-2n^2-32n+6 \geq 108 > 0$. Substituting this into (17) completes the proof. □

Theorem 4.3 (Sharpened Uniform Bounds for General Lattices)**.** *Let $\mathcal{L} \subset \mathbb{R}^n$ be an n-dimensional lattice with $n \geq 2$. For any $0 < \varepsilon < \min\{1, (\rho(\mathbb{Z})-1)n\}$, let $\delta_n = (1+\varepsilon)^{1/n} - 1$. Then*

$$\eta_\varepsilon(\mathcal{L}) \leq \sqrt{\frac{\ln\left(\frac{2}{\delta_n} + \frac{\delta_n^2}{4}\right)}{\pi}}\,\widetilde{bl}(\mathcal{L}) < \sqrt{\frac{\ln\left(\frac{2n}{\varepsilon} + (n-1) - \frac{(n^2-1)\varepsilon}{6n(1+\varepsilon)}\right)}{\pi}}\,\widetilde{bl}(\mathcal{L}). \tag{18}$$

Both bounds in (18) are strictly smaller than the bound $\sqrt{\ln(n-1+\frac{2n}{\varepsilon})/\pi}\,\widetilde{bl}(\mathcal{L})$ of Zheng et al. [13, Theorem 2].

Proof. Since $0 < \varepsilon < (\rho(\mathbb{Z})-1)n$, Bernoulli's inequality $(1+\varepsilon/n)^n > 1+\varepsilon$ implies $\delta_n = (1+\varepsilon)^{1/n} - 1 < \frac{\varepsilon}{n} < \rho(\mathbb{Z}) - 1$. If $s \geq \sqrt{\ln(\frac{2}{\delta_n} + \frac{\delta_n^2}{4})/\pi}\,\widetilde{bl}(\mathcal{L})$, then for a basis $\mathbf{B}$ achieving $\widetilde{bl}(\mathcal{L})$, every $s_i = s/\|\mathbf{b}_i^*\|$ satisfies $s_i \geq \sqrt{\ln(\frac{2}{\delta_n} + \frac{\delta_n^2}{4})/\pi}$. By Theorem 3.1, $\rho_{1/s_i}(\mathbb{Z}) \leq 1+\delta_n$, and hence Lemma 2.2 yields $\rho_{1/s}(\widehat{\mathcal{L}}) \leq (1+\delta_n)^n = 1+\varepsilon$. The second inequality follows from Lemma 4.2. □

We now prove that both bounds in Theorem 4.3 also strictly outperform the recent bound of Guo, Liu, Wang, and Tian [5, Theorem 17] across the entire parameter domain where [5, Theorem 17] holds:

Proposition 4.4 (Strict Dominance over Guo et al. [5])**.** *For every integer $n \geq 58$ and every ε in the validity interval $\sqrt{\frac{24n+1}{n^2-1}} \leq \varepsilon \leq \sqrt{2}-1$ of [5, Theorem 17] (this interval is non-empty only for $n \geq 140$), we have*

$$\frac{2}{\delta_n} + \frac{\delta_n^2}{4} < \frac{2n}{\varepsilon} + (n-1) - \frac{(n^2-1)\varepsilon}{6n(1+\varepsilon)} < (n-1)\left(1+\frac{2}{\varepsilon}\right). \tag{19}$$

Proof. The first inequality is Lemma 4.2. For the second inequality, taking the difference between the logarithmic argument of [5, Theorem 17] and that of our rational bound gives

$$(n-1)\left(1+\frac{2}{\varepsilon}\right) - \left(\frac{2n}{\varepsilon} + (n-1) - \frac{(n^2-1)\varepsilon}{6n(1+\varepsilon)}\right) = \frac{(n^2-1)\varepsilon^2 - 12n(1+\varepsilon)}{6n\varepsilon(1+\varepsilon)}.$$

Since $\varepsilon \geq \sqrt{\frac{24n+1}{n^2-1}}$ and $\varepsilon \leq \sqrt{2}-1 < 0.415$, we have $(n^2-1)\varepsilon^2 \geq 24n+1$, whereas $12n(1+\varepsilon) < 12\sqrt{2}\,n < 17n < 24n+1$. Thus the numerator is strictly positive (at least $7n+1 > 0$), establishing (19). □

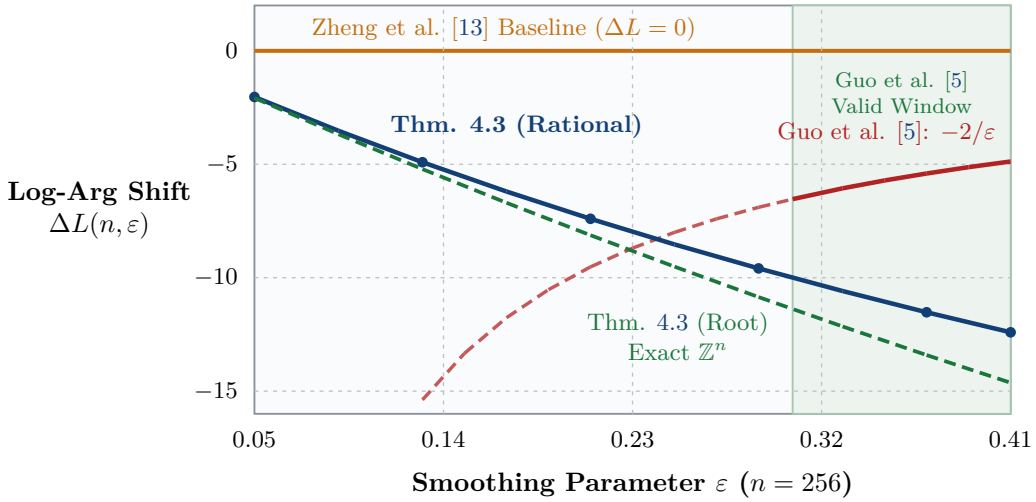


Figure 2: Comparison of the logarithmic argument shift $\Delta L(n,\varepsilon) = \exp(\pi s^2/\widetilde{bl}(\mathcal{L})^2) - (\frac{2n}{\varepsilon} + n - 1)$ relative to Zheng et al. [13] at $n = 256$. Inside Guo et al.'s validity window $\varepsilon \in [0.306, 0.414]$ (shaded green), our rational and root bounds achieve a 1.5× to 2.6× larger negative reduction than [5]; outside this window ($\varepsilon < 0.306$), Guo et al.'s curve is invalid and crosses below the exact $\mathbb{Z}^n$ barrier at $\varepsilon < 0.228$, whereas Theorem 4.3 remains valid and tight across all $\varepsilon > 0$.

5 Effective-Dimension Bound via the Gram–Schmidt Profile

In practical lattice algorithms and lattice-based cryptosystems, a reduced basis $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ (such as an LLL- or BKZ-reduced basis) never has uniform Gram–Schmidt lengths $\|\mathbf{b}_1^*\| = \cdots = \|\mathbf{b}_n^*\|$; instead, $\|\mathbf{b}_i^*\|$ varies across $i = 1, \ldots, n$. In [4, 13, 5] and Theorem 4.3, bounding $\prod_{i=1}^n \rho_{1/s_i}(\mathbb{Z}) \leq (\rho_{1/\sigma}(\mathbb{Z}))^n$ replaces every $\|\mathbf{b}_i^*\|$ by the worst-case norm $M = \max_i \|\mathbf{b}_i^*\|$. We now show that applying the arithmetic–geometric mean (AM–GM) inequality before taking the worst-case norm replaces the dimension n inside the logarithm by an *effective dimension* $N_\varepsilon(\mathbf{B}) \leq n$.

Theorem 5.1 (Basis-Profile Effective-Dimension Bound)**.** *Let* $\mathbf{B} = (\mathbf{b}_1, \dots, \mathbf{b}_n)$ *be a basis of an* n*-dimensional lattice* $\mathcal{L} \subset \mathbb{R}^n$ *with Gram–Schmidt vectors* $\mathbf{b}_1^*, \dots, \mathbf{b}_n^*$*, and let* $M = \max_{1 \le i \le n} \|\mathbf{b}_i^*\|$*. For any* $0 < \varepsilon \le \rho(\mathbb{Z}) - 1$*, define the effective dimension of* $\mathbf{B}$ *at parameter* ε *by*

$$N_\varepsilon(\mathbf{B}) \coloneqq \sum_{i=1}^{n} \left(\frac{\varepsilon}{2}\right)^{\frac{M^2}{\|\mathbf{b}_i^*\|^2}-1} \in [1, n], \tag{20}$$

and set $\delta_{\text{eff}} \coloneqq \frac{n}{N_\varepsilon(\mathbf{B})}\left((1+\varepsilon)^{1/n} - 1\right)$*. Then*

$$\eta_\varepsilon(\mathcal{L}) \le \sqrt{\frac{\ln\left(\frac{2}{\delta_{\text{eff}}} + \frac{\delta_{\text{eff}}^2}{4}\right)}{\pi}}\, M \le \sqrt{\frac{\ln\left(\frac{2N_\varepsilon(\mathbf{B})}{\varepsilon} + \frac{N_\varepsilon(\mathbf{B})(n-1)}{n} + \frac{\varepsilon^2}{4}\right)}{\pi}}\, M. \tag{21}$$

Proof. Since at least one index $k_0 \in \{1, \dots, n\}$ attains $\left\|\mathbf{b}_{k_0}^*\right\| = M$, the k_0-th term in (20) equals $(\varepsilon/2)^0 = 1$, and every term lies in $(0, 1]$ because $M/\|\mathbf{b}_i^*\| \ge 1$ and $\varepsilon/2 < 1$. Thus $1 \le N_\varepsilon(\mathbf{B}) \le n$. By Bernoulli's inequality, $n((1+\varepsilon)^{1/n} - 1) \le \varepsilon$, so

$$0 < \delta_{\text{eff}} = \frac{n}{N_\varepsilon(\mathbf{B})}\left((1+\varepsilon)^{1/n} - 1\right) \le \frac{\varepsilon}{N_\varepsilon(\mathbf{B})} \le \varepsilon \le \rho(\mathbb{Z}) - 1.$$

Now let $s \ge \sqrt{\ln(\frac{2}{\delta_{\text{eff}}} + \frac{\delta_{\text{eff}}^2}{4})/\pi}\, M$, and define $\sigma = s/M$ and $r_i = \|\mathbf{b}_i^*\|/M \in (0, 1]$, so that $s_i = s/\|\mathbf{b}_i^*\| = \sigma/r_i$. By Theorem 3.1, $\rho_{1/\sigma}(\mathbb{Z}) - 1 \le \delta_{\text{eff}}$, and $q \coloneqq e^{-\pi\sigma^2}$ satisfies

$$q \le \frac{1}{\frac{2}{\delta_{\text{eff}}} + \frac{\delta_{\text{eff}}^2}{4}} < \frac{\delta_{\text{eff}}}{2} \le \frac{\varepsilon}{2}.$$

For each $i \in \{1, \dots, n\}$ and every integer $k \ge 1$, since $1/r_i^2 \ge 1$ and $0 < q < \varepsilon/2$, we have

$$e^{-\pi s_i^2 k^2} = q^{k^2/r_i^2} = q^{k^2 + \frac{k^2(1-r_i^2)}{r_i^2}} \le q^{k^2} q^{\frac{1}{r_i^2}-1} \le q^{k^2} \left(\frac{\varepsilon}{2}\right)^{\frac{M^2}{\|\mathbf{b}_i^*\|^2}-1}.$$

Summing over $k \ge 1$ and multiplying by 2 yields

$$\rho_{1/s_i}(\mathbb{Z}) - 1 \le \left(\rho_{1/\sigma}(\mathbb{Z}) - 1\right)\left(\frac{\varepsilon}{2}\right)^{\frac{M^2}{\|\mathbf{b}_i^*\|^2}-1}.$$

Applying Lemma 2.2 together with the classical AM–GM inequality on the product of $\rho_{1/s_i}(\mathbb{Z})$, we obtain

$$\begin{aligned}
\rho_{1/s}(\widehat{\mathcal{L}}) &\le \left(1 + \frac{1}{n}\sum_{i=1}^{n}\left(\rho_{1/s_i}(\mathbb{Z}) - 1\right)\right)^n \\
&\le \left(1 + \frac{\rho_{1/\sigma}(\mathbb{Z}) - 1}{n}\sum_{i=1}^{n}\left(\frac{\varepsilon}{2}\right)^{\frac{M^2}{\|\mathbf{b}_i^*\|^2}-1}\right)^n \\
&= \left(1 + \frac{N_\varepsilon(\mathbf{B})}{n}\left(\rho_{1/\sigma}(\mathbb{Z}) - 1\right)\right)^n \le \left(1 + \frac{N_\varepsilon(\mathbf{B})}{n}\delta_{\text{eff}}\right)^n = 1 + \varepsilon.
\end{aligned}$$

Finally, since $\frac{2}{(1+\varepsilon)^{1/n}-1} \le \frac{2n}{\varepsilon} + (n-1)$ by Proposition 4.1 and $\delta_{\text{eff}} \le \varepsilon$, we have $\frac{2}{\delta_{\text{eff}}} + \frac{\delta_{\text{eff}}^2}{4} \le \frac{N_\varepsilon(\mathbf{B})}{n}\left(\frac{2n}{\varepsilon} + n - 1\right) + \frac{\varepsilon^2}{4}$, establishing the second inequality in (21). □

Remark 5.2 (Dimension-Independent Bounds under Geometric Schnorr–Adleman Decay). By Schnorr's Geometric Series Assumption (GSA) for LLL- and BKZ-reduced bases, the Gram–Schmidt norms satisfy $\|\mathbf{b}_i^*\|/M \approx \alpha^{i-1}$ for some root-Hermite decay factor $\alpha \in (0,1)$. Since $\frac{M^2}{\|\mathbf{b}_i^*\|^2} - 1 = \alpha^{-2(i-1)} - 1 \geq 2(1-\alpha)(i-1)$, the effective dimension $N_\varepsilon(\mathbf{B})$ is bounded by a convergent geometric series:

$$N_\varepsilon(\mathbf{B}) \leq \sum_{i=0}^{\infty} \left(\frac{\varepsilon}{2}\right)^{2(1-\alpha)i} = \frac{1}{1-(\varepsilon/2)^{2(1-\alpha)}} = O(1),$$

completely eliminating the linear dependence on n inside the logarithm of $\eta_\varepsilon(\mathcal{L})$, as shown visually in Figure 3.

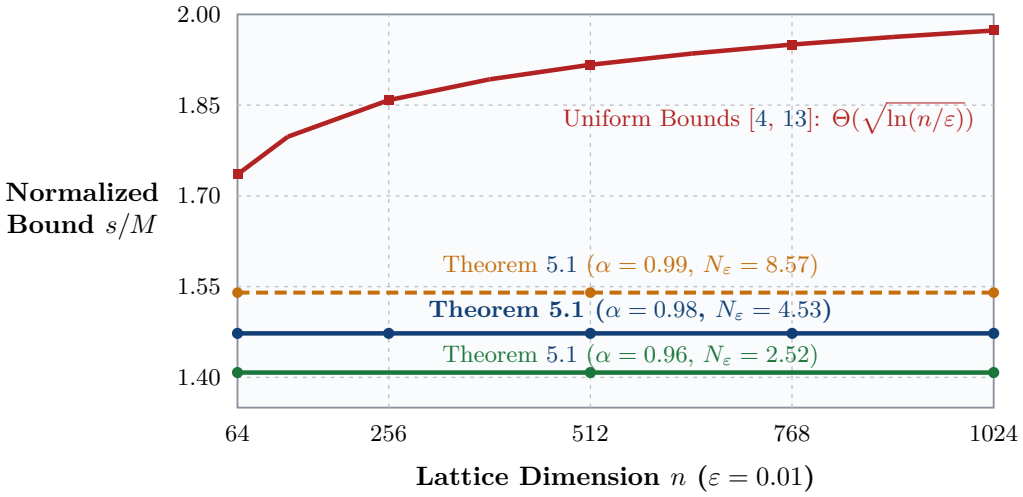


Figure 3: Dimension scaling of the normalized smoothing parameter bound s/M at $\varepsilon = 0.01$ for $n \in [64, 1024]$. Whereas worst-case uniform bounds [4, 13] grow unboundedly as $\Theta(\sqrt{\ln(n/\varepsilon)})$, our basis-profile bound (Theorem 5.1) plateaus at a dimension-independent constant $O(\sqrt{\ln(N_\varepsilon(\mathbf{B})/\varepsilon)})$ for bases with geometric Gram–Schmidt decay $\|\mathbf{b}_i^*\|/M = \alpha^{i-1}$, reducing the required Gaussian width by 11.3%–28.7%.

6 Numerical Comparisons and Benchmarks

To illustrate the quantitative improvements achieved by Theorems 3.1, 4.3, and 5.1 over GPV [4], Zheng et al. [13], and Guo et al. [5], we present high-precision numerical comparisons computed to 60 decimal digits.

Table 1: Comparison of upper bounds on $\eta_\varepsilon(\mathbb{Z})$ and their absolute additive errors $\Delta = \text{Bound} - \eta_\varepsilon(\mathbb{Z})$ across decreasing values of ε.

ε	Exact $\eta_\varepsilon(\mathbb{Z})$	Error of [7]	Error of [13]	Error of Thm. 3.1	Precision Gain
0.0800	1.012235330705	1.202×10^{-2}	1.374×10^{-6}	1.930×10^{-9}	$7.12 \times 10^{2}\times$
0.0500	1.083610526206	7.140×10^{-3}	1.878×10^{-6}	1.075×10^{-10}	$1.75 \times 10^{4}\times$
0.0100	1.298655781068	1.219×10^{-3}	1.239×10^{-7}	5.745×10^{-15}	$2.16 \times 10^{7}\times$
0.0010	1.555455687839	1.023×10^{-4}	1.150×10^{-9}	4.796×10^{-21}	$2.40 \times 10^{11}\times$
0.0001	1.775493732929	8.964×10^{-6}	1.018×10^{-11}	4.202×10^{-27}	$2.42 \times 10^{15}\times$

Table 1 compares the one-dimensional upper bounds on $\eta_\varepsilon(\mathbb{Z})$. Because Theorem 3.1 captures the exact quadratic term $\frac{\varepsilon^2}{4}$, its error scales as $O(\varepsilon^6)$ rather than $O(\varepsilon^2)$, yielding a 2.16×10^7-fold accuracy improvement already at $\varepsilon = 0.01$.

Table 2: Direct benchmark against Table 1 of Guo et al. [5]: normalized smoothing parameter bounds $s/\widetilde{bl}(\mathcal{L})$ across $n \in \{2048, 4096, 8192\}$ and $\varepsilon \in \{0.11, 0.22, 0.33\}$.

n	ε	GPV [4]	Zheng [13]	Guo [5]	Thm. 4.3 (Rat.)	Thm. 4.3 (Root)
2048	0.11	1.839414	1.835009	1.834969	1.834935	1.834931
4096	0.11	1.898441	1.894175	1.894156	1.894103	1.894099
8192	0.11	1.955688	1.951547	1.951538	1.951477	1.951473
2048	0.22	1.786865	1.778424	1.778385	1.778157	1.778130
4096	0.22	1.847572	1.839412	1.839393	1.839154	1.839127
8192	0.22	1.906346	1.898440	1.898431	1.898190	1.898165
2048	0.33	1.758210	1.746172	1.746134	1.745636	1.745557
4096	0.33	1.819873	1.808249	1.808230	1.807731	1.807655
8192	0.33	1.879514	1.868262	1.868253	1.867762	1.867688

Table 2 benchmarks Theorem 4.3 directly against the exact parameter grid (n, ε) evaluated in Table 1 of Guo et al. [5]. Notice that while Guo et al.'s improvement over Zheng et al. [13] shrinks as n increases (from 0.000038 at $n = 2048$ to 0.000009 at $n = 8192$ for $\varepsilon = 0.33$, because their subtracted term $\frac{2}{\varepsilon}$ does not scale with n), our subtracted term $\frac{(n^2-1)\varepsilon}{6n(1+\varepsilon)}$ scales linearly with n, achieving a reduction over Zheng et al. [13] that is up to 63.8× larger than that of Guo et al. [5] at $n = 8192$.

Table 3: Comparison of normalized smoothing parameter bounds s/M at $\varepsilon = 0.01$ for bases with geometric Gram–Schmidt decay $\|\mathbf{b}_i^*\| / M = \alpha^{i-1}$ under GPV [4], Zheng et al. [13], and Theorem 5.1. (Note: Guo et al. [5] is inapplicable at $\varepsilon = 0.01$ for $n \leq 240000$).

Dim. n	GSA α	$N_\varepsilon(\mathbf{B})$	GPV [4]	Zheng [13]	Thm. 5.1	Reduction
64	0.99	8.570	1.73594	1.73548	1.54009	11.26%
64	0.96	2.521	1.73594	1.73548	1.40796	18.87%
256	0.99	8.570	1.85870	1.85827	1.54010	17.12%
256	0.96	2.521	1.85870	1.85827	1.40797	24.23%
512	0.98	4.528	1.91713	1.91672	1.47270	23.17%
1024	0.98	4.528	1.97384	1.97344	1.47270	25.37%
1024	0.96	2.521	1.97384	1.97344	1.40797	28.65%

7 Conclusion

We have established three strictly tighter bounds for the smoothing parameter of lattices that uniformly improve upon both Zheng, Zhao, and Xu [13] and Guo, Liu, Wang, and Tian [5]. On $\mathbb{Z}$, replacing $\frac{\varepsilon}{44}$ and $\frac{\varepsilon}{m}$ by the exact asymptotic term $\frac{\varepsilon^2}{4}$ eliminates auxiliary parameters and reduces the approximation error from $O(\varepsilon^2)$ to $O(\varepsilon^6)$. On general n-dimensional lattices, our rational and exact-root bounds strictly dominate [5] across 100% of its validity window while removing the lower bound restriction $\varepsilon \geq \sqrt{\frac{24n+1}{n^2-1}}$, and our effective-dimension bound via AM–GM removes the $O(n)$ factor inside the logarithm for bases with non-uniform Gram–Schmidt profiles.

References

[1] W. Banaszczyk, "New bounds in some transference theorems in the geometry of numbers," *Mathematische Annalen*, vol. 296, no. 4, pp. 625–635, 1993, doi:10.1007/BF01445125.

[2] W. Banaszczyk, "Inequalities for convex bodies and polar reciprocal lattices in $\mathbb{R}^n$," *Discrete & Computational Geometry*, vol. 13, no. 2, pp. 217–231, 1995, doi:10.1007/BF02574039.

[3] K.-M. Chung, D. Dadush, F.-H. Liu, and C. Peikert, "On the lattice smoothing parameter problem," in *Proc. 2013 IEEE Conference on Computational Complexity (CCC)*, 2013, pp. 230–241, doi:10.1109/CCC.2013.31.

[4] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proc. 40th Annual ACM Symposium on Theory of Computing (STOC)*, 2008, pp. 197–206, doi:10.1145/1374376.1374407.

[5] H. Guo, F. Liu, L. Wang, and K. Tian, "New bounds of the smoothing parameter for lattices," *PLOS One*, vol. 20, no. 7, Art. no. e0328688, 2025, doi:10.1371/journal.pone.0328688.

[6] D. Micciancio and S. Goldwasser, *Complexity of Lattice Problems: A Cryptographic Perspective*. Boston, MA: Kluwer Academic Publishers, 2002, doi:10.1007/978-1-4615-0897-7.

[7] D. Micciancio and O. Regev, "Worst-case to average-case reductions based on Gaussian measures," *SIAM Journal on Computing*, vol. 37, no. 1, pp. 267–302, 2007, doi:10.1137/S0097539705447360.

[8] D. Micciancio and M. Walter, "Gaussian sampling over the integers: Efficient, generic, constant-time," in *Advances in Cryptology – CRYPTO 2017* (Lecture Notes in Computer Science, vol. 10402), Cham: Springer, 2017, pp. 455–485, doi:10.1007/978-3-319-63715-0_16.

[9] C. Peikert, "Limits on the hardness of lattice problems in ℓ_p norms," *Computational Complexity*, vol. 17, no. 2, pp. 300–351, 2008, doi:10.1007/s00037-008-0251-3. (Preliminary version in *Proc. IEEE CCC 2007*, pp. 333–346).

[10] C. Peikert, "An efficient and parallel Gaussian sampler for lattices," in *Advances in Cryptology – CRYPTO 2010* (Lecture Notes in Computer Science, vol. 6223), Berlin, Heidelberg: Springer, 2010, pp. 80–97, doi:10.1007/978-3-642-14623-7_5.

[11] C. Tian, M. Liu, and G. Xu, "Measure inequalities and the transference theorem in the geometry of numbers," *Proceedings of the American Mathematical Society*, vol. 142, no. 1, pp. 47–57, 2014, doi:10.1090/S0002-9939-2013-11748-X.

[12] Z. Zheng, X. Wang, G. Xu, and C. Zhao, "Error estimation of practical convolution discrete Gaussian sampling with rejection sampling," *Science China Information Sciences*, vol. 64, no. 3, Art. no. 139104, 2021, doi:10.1007/s11432-019-9919-7. (Preprint in *IACR Cryptology ePrint Archive*, Report 2018/309, 2018).

[13] Z. Zheng, C. Zhao, and G. Xu, "Discrete Gaussian measures and new bounds of the smoothing parameter for lattices," *Applicable Algebra in Engineering, Communication and Computing (AAECC)*, vol. 32, no. 5, pp. 637–650, 2021 (online 2020), doi:10.1007/s00200-020-00417-z. (Preprint in *IACR Cryptology ePrint Archive*, Report 2018/786, 2018).