Noname manuscript No.
(will be inserted by the editor)

On the smoothing parameter and last minimum of random orthogonal lattices

Elena Kirshanova[1] · **Huyen Nguyen**[2] ·
Damien Stehlé[2] · **Alexandre Wallet**[3]

Abstract Let $X \in \mathbb{Z}^{n\times m}$, with each entry independently and identically distributed from an integer Gaussian distribution. We consider the orthogonal lattice $\Lambda^\perp(X)$ of X, i.e., the set of vectors $\mathbf{v} \in \mathbb{Z}^m$ such that $X\mathbf{v} = \mathbf{0}$. In this work, we prove probabilistic upper bounds on the smoothing parameter and the $(m-n)$-th minimum of $\Lambda^\perp(X)$. These bounds improve and the techniques build upon prior works of Agrawal, Gentry, Halevi and Sahai [Asiacrypt'13], and of Aggarwal and Regev [Chicago J. Theoret. Comput. Sci.'16].

Keywords: random lattices, last minimum, smoothing parameter, lattice-based cryptography, lattices and convex bodies

1 Introduction

A rank-d Euclidean lattice Λ is a discrete subgroup of $(\mathbb{R}^m, +)$ spanned by the columns of a matrix $B \in \mathbb{R}^{m\times d}$ via integer linear combinations. The columns of B form a $\mathbb{Z}$-basis of Λ. Understanding geometric properties of high-dimensional lattices is a central topic in various areas of mathematics and computer science [22]. Among the most important invariants of a lattice are its so-called *successive minima* $\lambda_1(\Lambda), \ldots, \lambda_d(\Lambda)$, where λ_i is the smallest $r \in \mathbb{R}$ such that Λ has i linearly independent vectors of Euclidean norms $\leq r$. Another important invariant, closely related to the minima, is the *smoothing parameter* $\eta_\varepsilon(\Lambda)$. Informally, it quantifies the smallest standard deviation s needed for a discrete Gaussian distribution over Λ to behave essentially like a continuous one up to a statistical error ε. Formally, the smoothing parameter $\eta_\varepsilon(\Lambda)$ is the minimal $s > 0$ such that the Gaussian mass $\sum_{\mathbf{x}\in\Lambda^*} \exp(-\pi s^2 \|\mathbf{x}\|)$ is at most $1+\varepsilon$. (The dual lattice $\Lambda^\star$ of Λ with basis B is $B(B^{\mathrm{t}}B)^{-1}\mathbb{Z}^d$.) Introduced by Micciancio and Regev in 2004, the smoothing parameter has been used as a central tool in reductions between lattice problems [18] and in lattice-based cryptography. Also, the notion of smoothing parameter can be found in communication theory under the name 'flatness factor' [6].

[1] I. Kant Baltic Federal University, Kaliningrad, Russia. `elenakirshanova@gmail.com` ·
[2] ENS de Lyon, Laboratoire LIP (U. Lyon, CNRS, ENS de Lyon, INRIA, UCBL), France. `{huyen.nguyen,damien.stehle}@ens-lyon.fr` ·
[3] NTT Secure Platform Laboratories, Tokyo, Japan. `alexandre.wallet.th@hco.ntt.co.jp`

In this work, we consider the successive minima and the smoothing parameter of random *orthogonal* lattices. For $X \in \mathbb{Z}^{n\times m}$ with $m > n$, the orthogonal lattice $\Lambda^{\perp}(X)$ is a set of all vectors $\mathbf{v} \in \mathbb{Z}^m$ that belong to the (right) kernel of X. In cryptography, orthogonal lattices first appeared as a cryptanalytic tool in attacking several cryptographic constructions [20,21,10]. Years later, when lattices have turned into a major build block in designing cryptographic primitives, orthogonal lattices were used in various constructions such as cryptographic multilinear maps [2], traitor-tracing schemes [17] and inner product functional encryption [3].

Given $X \in \mathbb{Z}^{n\times m}$, one can find a basis of $\Lambda^{\perp}(X)$ by a Hermite Normal Form computation (see, e.g., [13]). Concretely: let $U \in \mathbb{Z}^{m\times m}$ be a unimodular transformation that brings X into HNF, i.e., $X \cdot U = X^{\mathtt{HNF}}$; if X is of full row-rank n, the last $m-n$ columns of $X^{\mathtt{HNF}}$ are zero vectors; viewing U as a block matrix $U = [U_1|U_2]$ for $U_2 \in \mathbb{Z}^{m\times m-n}$ of rank $m-n$, one can show that the columns of U_2 form a basis of $\Lambda^{\perp}(X)$. Similarly, Nguyen and Stern [20] show how to obtain a short basis of $\Lambda^{\perp}(X)$ by LLL-reducing [16] the lattice spanned by the columns of $[cX^{\mathrm{t}}|I_m]^{\mathrm{t}}$ with some sufficiently large scalar c.

We study the $(m-n)$-th minimum and the smoothing parameter of the orthogonal rank-$(m-n)$ lattice $\Lambda^{\perp}(X)$, where each entry of X is independently and identically distributed according to an integer Gaussian distribution. In particular, we obtain probabilistic upper bounds on $\eta_{\varepsilon}(\Lambda^{\perp}(X))$ and $\lambda_{m-n}(\Lambda^{\perp}(X))$.

Prior results. Consider the following process: sample $a_1, \ldots, a_m$ uniformly in $\mathbb{Z}/q\mathbb{Z}$ for some integer $q > 1$; sample $z_1, \ldots, z_m$ small Gaussian integers. Then, conditioned on the a_i's, the value $\sum_i a_i z_i$ "looks like" a uniform element of $\mathbb{Z}/q\mathbb{Z}$. This statement, due to [12, Lemma 4.2], is a variant of the leftover hash lemma [15] (LHL for short), and its proof crucially relies on the smoothing parameter of the lattice corresponding to the kernel of the map $\mathbf{z} \in \mathbb{Z}^m \mapsto \langle \mathbf{z}, \mathbf{a} \rangle \bmod q$. With a motivation stemming from a cryptographic multilinear map construction [11], Agrawal, Gentry, Halevi and Sahai considered the following variation: instead of starting from the finite set $\mathbb{Z}/q\mathbb{Z}$, they consider a matrix $X \in \mathbb{Z}^{n\times m}$ with entries sampled from an integer Gaussian distribution and focus on the closeness between the distribution of the vector $X\mathbf{z}$ and a discrete Gaussian distribution, for an appropriately chosen Gaussian multiplier $\mathbf{z}$ and conditioned over X. The main novelty was to replace the finite support $\mathbb{Z}/q\mathbb{Z}$ by the infinite support $\mathbb{Z}$. This question can be answered by considering the smoothing parameter of the lattice $\Lambda^{\perp}(X)$. Let us denote by $D_{\mathbb{Z}^n,S}$ the n-dimensional zero-centered discrete Gaussian distribution over $\mathbb{Z}^n$ with parameter a full column-rank matrix S with n columns (the probability of a vector $\mathbf{k} \in \mathbb{Z}^n$ is proportional to $\exp(-\pi\|\mathbf{k}^{\mathrm{t}}(S^{\mathrm{t}}S)^{-1}\mathbf{k}\|)$) and by $D_{\mathbb{Z}^n,s}$ the case when $S = sI_n$. The following probabilistic bound is proved in [2]:

$$\eta_{\varepsilon}(\Lambda^{\perp}(X)) \leq \mathcal{O}(mn\sqrt{\ln(m/\varepsilon)}),$$

where $X \leftarrow (D_{\mathbb{Z}^n,s})^m$,[1] $s > \eta_{\varepsilon}(\mathbb{Z}^n)$[2] and $m = \Omega(n\ln(ns))$. This statement holds with probability $\geq 1-2^{-\Omega(n)}$ over the choice of X. They obtain a LHL over lattices as a direct consequence of this result: for parameters satisfying the same conditions

[1] Note that an equivalent description of the distribution for X would be $X \leftarrow (D_{\mathbb{Z},s})^{n\times m}$. Our choice follows prior works.

[2] We recall that $\eta_{\varepsilon}(\mathbb{Z}^n) = \mathcal{O}(\sqrt{\ln(n/\varepsilon)})$ (see Section 2).

and if the above smoothing parameter bound holds, the statistical distance[3] between the distributions $X\mathbf{z}$ (conditioned on X) and $D_{\mathbb{Z}^m,s'X^t}$ is at most ε, when $\mathbf{z}$ is sampled from $D_{\mathbb{Z}^m,s'}$ for $s' \geq \eta_\varepsilon(\Lambda^\perp(X))$.

Our objective here is to obtain a sufficient condition on s' which is as mild as possible. Note that improving the upper bound on $\eta_\varepsilon(\Lambda^\perp(X))$ directly leads to a milder condition on s'.

Following [2], Aggarwal and Regev [1] gave another bound on the smoothing parameter of $\Lambda^\perp(X)$. Namely, they showed that

$$\eta_\varepsilon(\Lambda^\perp(X)) \leq \mathcal{O}\left(ns \cdot \sqrt{\ln(ns) \cdot \ln(m) \cdot \ln(m/\varepsilon)}\right),$$

with probability $\geq 1 - 2^{-\Omega(n)}$ over the choice of $X \leftarrow (D_{\mathbb{Z}^n,s})^m$. The bound holds for $s > \eta_\varepsilon(\mathbb{Z}^n)$ and $m = \Omega(n \ln(ns))$. The bound of [1] is lower for large m and small s, while the result of [2] is preferable for large s and small m.

Our results. Our first result is an improved upper bound on $\eta_\varepsilon(\Lambda^\perp(X))$.

Theorem 1 *Let n be an integer growing to infinity, $\varepsilon > 0$, $s \geq \Omega(\sqrt{n})$ and $m = \Omega(n \ln s)$. Then, we have*

$$\Pr_{X \leftarrow (D_{\mathbb{Z}^n,s})^m}\left[\eta_\varepsilon(\Lambda^\perp(X)) \leq \mathcal{O}\left(\sqrt{(n + \ln m) \cdot \ln(m/\varepsilon)}\right)\right] \geq 1 - 2^{-\Omega(n)}.$$

Moreover, for any $\varepsilon \leq e^{-(m-n)}$,

$$\Pr_{X \leftarrow (D_{\mathbb{Z}^n,s})^m}\left[\eta_\varepsilon(\Lambda^\perp(X)) \leq \mathcal{O}\left(\sqrt{\ln(1/\varepsilon)}\right)\right] \geq 1 - 2^{-\Omega(n)}.$$

Note that the second probabilistic upper bound is lower than the first, but is not applicable for every $\varepsilon > 0$. It holds for $\varepsilon \leq e^{-(m-n)}$,and, for larger values of ε, only the first bound applies.The reason why there are two possibilities for the upper bound stems from the two uncomparable relations between the smoothing parameter and the first minimum of the dual lattice $\Lambda^\perp(X)^\star$ for the Euclidean and infinity norms (see Lemmas 5 and 6).

A proof for this theorem can be found in Section 3. Our result improves over both bounds of [2] and [1] when $s = \Omega(\sqrt{n})$ and m is sufficiently large. In particular, the minimum of our two upper bounds is smaller by an $\Omega(\sqrt{n})$ factor for the above ranges of m and s, is independent of s and depends at most logarithmically in m. However, our result requires $s = \Omega(\sqrt{n})$ (which is a consequence of our proof technique, in particular, Lemma 12), so for small values of s, the prior results of [2] and [1] remain the best known upper bounds on $\eta_\varepsilon(\Lambda^\perp(X))$. As an immediate corollary to Theorem 1, we obtain a tighter version the leftover hash lemma over lattices (see Corollary 1). We summarise our results and compare them with previous works in Table 1.

For applications, it is useful to keep in mind the following parameter set with respect to n: $\varepsilon = 2^{-\Theta(n)}$, $s = n^{\Theta(1)}$ and $m = \Theta(n \ln n)$. For these parameters, Theorem 1 yields $\eta_\varepsilon(\Lambda^\perp(X)) \leq \widetilde{\mathcal{O}}(n)$ with probability $\geq 1 - 2^{-\Omega(n)}$. For the same parameters, the probabilistic bounds from [2] and [1] are $\eta_\varepsilon(\Lambda^\perp(X)) \leq \widetilde{\mathcal{O}}(n^3)$ and $\eta_\varepsilon(\Lambda^\perp(X)) \leq \widetilde{\mathcal{O}}(n^{3/2}s)$, respectively.

[3] The statistical distance between two distributions X and Y is half their ℓ_1-distance, i.e., $\Delta(X, Y) := \frac{1}{2}\|X - Y\|_1 = \frac{1}{2}\sum_{\omega \in \Omega} |X(\omega) - Y(\omega)|$.

	Agrawal et al. [2]	Aggarwal-Regev [1]	This work
s	$\Omega(\eta_\varepsilon(\mathbb{Z}^n))$	$\Omega(\eta_\varepsilon(\mathbb{Z}^n))$	$\Omega(\sqrt{n})$
m	$\Omega(n\ln(ns))$	$\Omega(n\ln(ns))$	$\Omega(n\ln s)$
$\eta_\varepsilon(\Lambda^\perp(X))$	$\mathcal{O}\left(mn\sqrt{\ln\frac{m}{\varepsilon}}\right)$	$\mathcal{O}\left(ns\sqrt{\ln(ns)\ln(m)\ln\frac{m}{\varepsilon}}\right)$	$\mathcal{O}\left(\sqrt{(n+\ln m)\cdot\ln\frac{m}{\varepsilon}}\right)$ or $\mathcal{O}\left(\sqrt{\ln\frac{1}{\varepsilon}}\right)$

Table 1: Probabilistic upper bounds on $\eta_\varepsilon(\Lambda^\perp(X))$ for $X \leftarrow (D_{\mathbb{Z}^n,s})^m$ together with requirements on s and m needed for the bounds to hold. The two cases in the last table entry depend on the range of ε, see Theorem 1.

.

Our second main result is an upper bound on the $(m-n)$-th minimum of the orthogonal lattice $\Lambda^\perp(X)$. Note that we could use our result of Theorem 1 to obtain an upper bound on $\lambda_{m-n}(\Lambda^\perp(X))$ via the relation $\lambda_{m-n}(\Lambda) \leq \sqrt{m-n}\cdot\eta_\varepsilon(\Lambda)$, which holds for any rank-$(m-n)$ lattice Λ and any $\varepsilon \in (0, 1/2))$ (see Lemma 7). Below we state the result, which gives a better bound for a large set of parameters. In particular, for many ranges of s and m, it improves over the bound $\lambda_{m-n}(\Lambda^\perp(X)) \leq \mathcal{O}(ns\sqrt{\ln(m)\ln(ns)})$ from [1], and the bound $\lambda_{m-n}(\Lambda^\perp(X)) \leq \mathcal{O}(mn)$ from [2].

Theorem 2 *Let n be an integer growing to infinity, $s \geq \Omega(\sqrt{n})$ and m satisfying $m = \Omega(n\ln s)$ and $m \leq 2^{n/2}$. Then, we have*

$$\Pr_{X\leftarrow(D_{\mathbb{Z}^n,s})^m}\left[\lambda_{m-n}(\Lambda^\perp(X)) \leq \mathcal{O}(n\ln s)\right] \geq 1 - 2^{-\Omega(n)}.$$

This theorem is proven in Section 4. An interesting fact to be noticed from this result is that, with overwhelming probability, the lattice $\Lambda^\perp(X)$ contains $(m-n)$ linearly independent vectors whose norms do not depend on m — a parameter which can be as large as $2^{n/2}$. On the other hand, our statement holds even when taking m as small as $\Theta(n\cdot\ln s)$. We summarise our results and compare them with previous works in Table 2.

	Agrawal et al. [2]	Aggarwal-Regev [1]	This work
s	$\Omega(\eta_\varepsilon(\mathbb{Z}^n))$	$\Omega(\eta_\varepsilon(\mathbb{Z}^n))$	$\Omega(\sqrt{n})$
m	$\Omega(n\ln(ns))$	$\Omega(n\ln(ns))$	$\Omega(n\ln s)$ and $\leq 2^{n/2}$
$\lambda_{m-n}(\Lambda^\perp(X))$	$\mathcal{O}(mn)$	$\mathcal{O}\left(ns\sqrt{\ln(ns)\ln(m)}\right)$	$\mathcal{O}(n\ln s)$

Table 2: Probabilistic upper bounds on $\lambda_{m-n}(\Lambda^\perp(X))$ for $X \leftarrow (D_{\mathbb{Z}^n,s})^m$ together with requirements on s and m needed for the bounds to hold.

.

1.1 Techniques

The bound on the smoothing parameter is obtained via a chain of relations between successive minima of different lattices and the smoothing parameter of $\Lambda^{\perp}(X)$. Well-known transference relations between the smoothing parameter of a lattice and the first minimum of its dual lead us to study $\lambda_1(\Lambda^{\perp}(X)^{\star})$. Namely, in order to obtain our result on $\eta_{\varepsilon}(\Lambda^{\perp}(X))$, we bound $\lambda_1(\Lambda^{\perp}(X)^{\star})$ from below in both Euclidean and infinity norms.

To obtain these lower bounds, we consider the lattice $\Lambda_q(X) \subseteq \mathbb{Z}^m$ – the full-rank lattice spanned by the rows of X and $q\mathbb{Z}^m$ (in other words, we consider the so-called Construction A lattice of X, see [8, Chapter 5]). Following [2], our objective is to obtain a probabilistic lower bound on the norms of vectors from $\Lambda_q(X) \setminus X^{\mathsf{t}}\mathbb{Z}^n$. Note that this implies a probabilistic lower bound on $\lambda_{n+1}(\Lambda_q(X))$, as the vector space $X^{\mathsf{t}}\mathbb{Q}^n$ has dimension at most n.

At the heart of both proofs, ours and the one from [2], is a counting argument that allows to bound the norms of lattice vectors of the form $X^{\mathsf{t}}\mathbf{z} \bmod q \in \Lambda_q(X) \setminus X^{\mathsf{t}} \cdot \mathbb{Z}^n$. The counting argument is divided into several cases depending on the norm of $\mathbf{z}$. One source of improvement in our result is a more fine-grained division of these cases as well as a tighter treatment of interchange between different norms.

Once we have a lower bound on the norms of vectors from $\Lambda_q(X) \setminus X^{\mathsf{t}}\mathbb{Z}^n$, we relate the smallest norm of such vectors to $\lambda_1(\Lambda^{\perp}(X)^{\star})$. This is where our approach differs most from [2]. The intuition behind the relation is the following: observe that for a sufficiently large q, the lattice $\frac{1}{q}\Lambda_q(X)$ can be thought of as an approximation to $\Lambda^{\perp}(X)^{\star}$, in the sense that any $\mathbf{u} \in \Lambda^{\perp}(X)^{\star}$ can be expressed as a vector in $\frac{1}{q}\Lambda_q(X)$ plus a small element in the row-span of X. Our lower bound on norms of vectors in $\Lambda_q(X) \setminus X^{\mathsf{t}} \cdot \mathbb{Z}^n$ and a Gaussian tail bound give a lower bound on $\lambda_1(\Lambda^{\perp}(X)^{\star})$. This is in contrast to [2], which at this step invokes Banaszczyk's transference theorem [5] in order to relate $\lambda_{n+1}(\Lambda_q(X))$ and $\lambda_{m-n}(\Lambda_q(X)^{\star})$. Then, using the inclusion $\Lambda^{\perp}(X) \subseteq \frac{1}{q}\Lambda_q(X)^{\star}$, Agrawal et al. obtain their lower bound on $\lambda_1(\Lambda^{\perp}(X)^{\star})$.

Summing up the above description, we:

1. obtain a (probabilistic) lower bound on $\|\mathbf{b}\|$ for $\mathbf{b} \in \Lambda_q(X) \setminus X^{\mathsf{t}}\mathbb{Z}^n$, improving the result of [2] by an $\Omega(n)$ factor (see Theorem 5);
2. relate the shortest norm of $\mathbf{b} \in \Lambda_q(X) \setminus X^{\mathsf{t}}\mathbb{Z}^n$ with $\lambda_1(\Lambda^{\perp}(X)^{\star})$ (see Lemma 14);
3. apply known relations (Lemma 5 or Lemma 6, depending on the norm) between the first minimum of $\Lambda^{\perp}(X)^{\star}$ and $\eta_{\varepsilon}(\Lambda^{\perp}(X))$.

Our second result, stated in Theorem 2, gives an upper bound on the $(m-n)$-th minimum of $\Lambda^{\perp}(X)$. The main ingredient in the proof is an observation that we can subdivide, column-wise, a 'wide' matrix $X \in \mathbb{Z}^{n \times m}$ (here m is potentially much larger than n) into $\frac{m}{m'}$ smaller matrices $X_i \in \mathbb{Z}^{n \times m'}$, and obtain short vectors in each $\Lambda^{\perp}(X_i)$, which are also short vectors in $\Lambda^{\perp}(X)$. (For the sake of simplicity, we assume here that m' divides m.)

As a first step, we obtain an upper bound on $\lambda_{m'-n}(\Lambda^{\perp}(X_i))$ for all i. Such an upper bound on $\lambda_{m'-n}(\Lambda^{\perp}(X_i))$ is a corollary of our lower bound on $\lambda_{n+1}(\Lambda_q(X))$ and Banaszczyk's transference theorem [5]. Thus, we obtain $\frac{m}{m'}(m'-n)$ relatively short vectors of dimension m'. Note that each such vector can be 'padded' with enough 0's in a way that the resulting m-dimensional vector belongs to $\Lambda^{\perp}(X)$. The

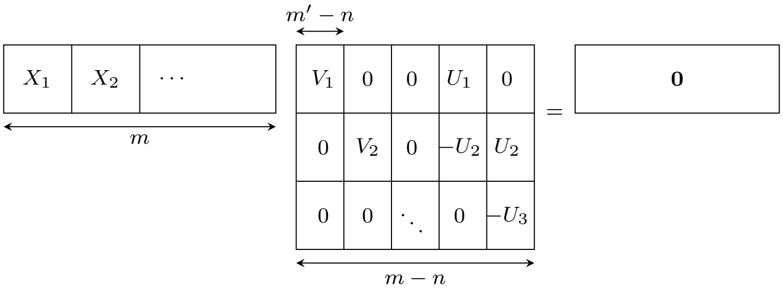

Fig. 1: Technique used in bounding $\lambda_{m-n}(\Lambda^{\perp}(X))$. For each i, the matrix $V_i \in \mathbb{Z}^{m' \times m'-n}$ consists of $m' - n$ short linearly independent vectors orthogonal to X_i, the matrix consisting of the first m' columns of X. The vectors making up V_i are chosen so that they reach the first $(m' - n)$ successive minima of $\Lambda^{\perp}(X_i)$. Another $n\big(\frac{m}{m'} - 1\big)$ short orthogonal to X vectors are obtained using matrices $U_i \in \mathbb{Z}^{m' \times n}$ that satisfy $X_i U_i = I_n$ and whose columns have small norms.

latter is illustrated in Figure 1 as follows: the columns of each matrix V_i are linearly independent vectors reaching the minima of $\Lambda^{\perp}(X_i)$, the columns containing them in the center matrix in Figure 1 are short linearly independent vectors in $\Lambda^{\perp}(X)$.

The second step consists in obtaining $n\big(\frac{m}{m'} - 1\big)$ additional short vectors (linearly independent with the previous ones), by applying a result due Aggarwal and Regev [1], which gives a probabilistic upper bound on the norm of the columns of a matrix $U \in \mathbb{Z}^{m \times n}$ such that $XU = I_n$. Hence, for each X_i, there exist $U_i \in \mathbb{Z}^{m' \times n}$ such that $X_i U_i = I_n$. Stacking the pairs $(U_i, -U_{i+1})$ as illustrated in Figure 1, we obtain the missing short vectors from $\Lambda^{\perp}(X)$.

1.2 Open problems

Our upper bound the last minimum of the lattice $\Lambda^{\perp}(X)$ improves the prior ones, but may not be the tightest possible. In fact, we suspect it is not sharp. The Gaussian matrix $X \leftarrow (D_{\mathbb{Z}^n,s})^m$ has rank n with overwhelming probability (see Lemma 9 below). Using the fact that $\det(\Lambda^{\perp}(X)) \leq \det(X^{\mathsf{t}}\mathbb{Z}^n)$ (see, e.g., [19, p. 30]) and Minkowski's theorem, we have

$$\prod_{i \in [m-n]} \lambda_i(\Lambda^{\perp}(X)) \leq \sqrt{m-n}^{\,m-n} \cdot \det(X^{\mathsf{t}}\mathbb{Z}^n).$$

Then, by applying a Gaussian tail bound, all the columns of X^{t} have norms $\leq s\sqrt{m}$ with overwhelming probability. If we assume that the successive minima are essentially the same, we obtain from Hadamard's inequality that

$$\forall i \leq m-n, \quad \lambda_i(\Lambda^{\perp}(X)) \leq \sqrt{m-n} \cdot (s\sqrt{m})^{\frac{n}{m-n}}.$$

Consider now $m = \Theta(n \ln n)$ and $s \leq \mathrm{poly}(n)$, and assume the above inequality is essentially tight. Then it suggests that the minimum $\lambda_{m-n}(\Lambda^{\perp}(X))$ should be $\widetilde{\Theta}(\sqrt{n})$. However, Theorem 2 only states that $\lambda_{m-n}(\Lambda^{\perp}(X)) \leq \widetilde{\mathcal{O}}(n)$. This gap possibly stems from our counting arguments in Lemma 11 and Lemma 13. Indeed, we impose there that all points in an n-dimensional cube satisfy some property with a success probability that is exponentially close to 1. It could be the case that by weakening our constraints on the probabilities, e.g., by asking for a failure at most $n^{-\omega(1)}$, we could achieve sharper estimations for smaller parameters. However, it does not seem straightforward, because we also rely on union bounds over sets of exponential sizes.

On the other hand, for exponentially small ε, we also expect the smoothing parameter to be essentially the same as the minima. This would heuristically give $\eta_\varepsilon(\Lambda^\perp(X)) = \widetilde{\Theta}(\sqrt{n})$ when $m = \Theta(n \ln n)$ and $s \leq \mathrm{poly}(n)$. Theorem 1 provides a $\widetilde{\mathcal{O}}(\sqrt{n})$ bound for these parameters.

2 Preliminaries

We let ln denote the natural logarithm. We use $\|\cdot\|$ for the Euclidean norm, and $\|\cdot\|_\infty$ for the infinity norm. The set of integers $\{1, \ldots, m\}$ is denoted by $[m]$. Bold letters will be used for vectors and capital letters for matrices. We write $\mathbf{e}_i$ for the canonical unit vectors of $\mathbb{Z}^m$, $\mathbf{0}_{m\times n}$ for the zero matrix of dimensions $m \times n$, $\mathbf{0}_m$ for the zero-vector of dimension m and $\mathbf{1}_m$ for the vector with all m entries equal to 1. For an integer $q > 2$, we use $[\mathbf{v}]_q$ to denote the modular reduction of all the entries of $\mathbf{v}$ into the interval $[-\frac{q}{2}, \frac{q}{2})$. We also write $\llbracket -\frac{q}{2}, \frac{q}{2} \llbracket^n := \mathbb{Z}^n \cap [-\frac{q}{2}, \frac{q}{2})^n$. The transpose and inverse of a matrix X are written as X^{t} and X^{-1}, respectively. The kernel of a matrix $X \in \mathbb{R}^{n\times m}$ seen as linear maps is denoted $\ker(X)$. For a vector subspace $V \subseteq \mathbb{R}^d$ and a vector $\mathbf{x} \in \mathbb{R}^d$, we let $\pi(\mathbf{x}, V)$ denote the orthogonal projection of $\mathbf{x}$ onto V. The orthogonal of a vector space E is denoted $E^\perp$.

For a distribution D, we write $\mathbf{x} \leftarrow D$ to say that $\mathbf{x}$ is sampled from D. For two distributions D, D' over a common support Ω, their statistical distance is defined as $\Delta(D, D') = \frac{1}{2}\sum_{\omega\in\Omega} |D(\omega) - D'(\omega)|$. Lastly, we will need the following version of Hoeffding's inequality.

Lemma 1 (Hoeffding's inequality) *Let $X_1, \ldots, X_m$ be independent random variables such that $0 \leq X_i \leq 1$ for all i. Let $S_m = X_1 + \cdots + X_m$. Then for any $t > 0$, we have*

$$\Pr\left[|S_m - \mathbb{E}[S_m]| \geq t\right] \leq 2\exp\left(-2t^2/m\right).$$

2.1 Lattices

A lattice is a discrete additive subgroup of $\mathbb{R}^m$, for some integer $m \geq 1$. A set of linearly independent vectors $B = \{\mathbf{b}_1, \ldots, \mathbf{b}_d\} \subset \mathbb{R}^m$ that generates a lattice via integer linear combinations is called a basis, and we write the lattice generated by B as

$$L(B) := \Big\{B\mathbf{z} = \sum_{i\in[d]} z_i \mathbf{b}_i : \mathbf{z} \in \mathbb{Z}^d\Big\}.$$

The rank of this lattice is d and its embedding dimension is m. When $d = m$, we say that the lattice has full rank. For $i \in [d]$, the i-th successive minimum $\lambda_i(L)$ is defined as

$$\lambda_i(L) := \inf\{r : \dim(\mathrm{Span}(L \cap \mathcal{B}(r))) \geq i\},$$

where $\mathcal{B}(r)$ denotes the closed zero-centered Euclidean ball of radius r. We use the notation $\lambda_i^\infty(L)$ when we consider the infinity norm.

Any lattice $L \subseteq \mathbb{R}^m$ has a dual lattice $L^\star$. It consists of all the vectors in $\mathrm{Span}(L)$ that are orthogonal to L modulo 1, namely:

$$L^\star := \{\mathbf{y} \in \mathrm{Span}(L) : \forall\, \mathbf{x} \in L, \langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}\}.$$

Note that $L^{\star\star} = L$. The following is a *transference theorem* as it allows to link the minima of a given lattice to those of its dual.

Theorem 3 ([5]) *For any rank-d lattice $L \subseteq \mathbb{R}^m$, and for all $i \in [d]$, we have*

$$1 \leq \lambda_i(L) \cdot \lambda_{d-i+1}(L^\star) \leq d.$$

Several families of lattices are considered in this work.

Definition 1 Let $m > n \geq 1$ and $q \geq 2$ be integers. Let $X \in \mathbb{Z}^{n \times m}$.

1. The **orthogonal lattice** $\Lambda^\perp(X)$ is the integral lattice whose vectors are orthogonal to the rows of X, i.e.,
$$\Lambda^\perp(X) := \{\mathbf{v} \in \mathbb{Z}^m : X\mathbf{v} = \mathbf{0}\}.$$
2. The lattice $\Lambda_q(X) \subseteq \mathbb{Z}^m$ is the full-rank lattice spanned by the rows of X and the vectors $q\mathbf{e}_i$, i.e.,
$$\Lambda_q(X) := \{X^{\mathsf{t}}\mathbf{z} + q\mathbf{y} \ : \ \mathbf{z} \in \mathbb{Z}^n, \mathbf{y} \in \mathbb{Z}^m\}.$$
3. The lattice $\Lambda_q^\perp(X) \subseteq \mathbb{R}^m$ is the dual of $\Lambda_q(X)$ scaled up by a factor of q, i.e.,
$$\Lambda_q^\perp(X) := \{\mathbf{v} \in \mathbb{R}^m : \forall\, \mathbf{u} \in \Lambda_q(X), \langle \mathbf{v}, \mathbf{u} \rangle \in q\mathbb{Z}\}.$$

We note that if X is of full row rank (over the integers), then $\Lambda^\perp(X)$ has rank $m - n$. It is a standard fact that if q is prime, then $\Lambda_q^\perp(X) = \{\mathbf{v} \in \mathbb{Z}^m : X\mathbf{v} = \mathbf{0} \bmod q\}$. Note that it always has rank m. Finally, we want to stress that the dual of $\Lambda^\perp(X)$ is not the lattice $X^{\mathsf{t}}\mathbb{Z}^n$.

Definition 2 (Orthogonal projection) Let L be a lattice and $E \subseteq \mathbb{R}^m$ be a vector subspace. The orthogonal projection of L onto E is:

$$\pi(L, E) = \{\mathbf{v}_1 \in E : \exists\ \mathbf{v}_2 \in E^\perp, \mathbf{v}_1 + \mathbf{v}_2 \in L\}.$$

Note that $\pi(L, E)$ is a finitely generated additive subgroup in $\mathbb{R}^m$, but not necessarily a lattice. The next lemma is standard (see, e.g., [7, Lemma 3.4]).

Lemma 2 *Let $E \subseteq \mathbb{R}^m$ be a vector space. For any lattice $L \in \mathbb{R}^m$ such that $\pi(L^\star, E)$ is a lattice, we have*

$$L \cap E = \big(\pi(L^\star, E)\big)^\star.$$

Lemma 3 *Let $X \in \mathbb{Z}^{n \times m}$ and $\Lambda^\perp(X)^\star$ be the dual lattice of $\Lambda^\perp(X)$. We have*

$$\Lambda^\perp(X)^\star = (\mathbb{Z}^m + X^{\mathsf{t}}\mathbb{R}^n) \cap \ker(X).$$

Proof. Any $\mathbf{r} \in \pi(\mathbb{Z}^m, \ker(X))$ can be written as $\mathbf{r} = \mathbf{k} - X^{\mathsf{t}}(XX^{\mathsf{t}})^{-1}X\mathbf{k}$, for some $\mathbf{k} \in \mathbb{Z}^m$. It follows that $\pi(\mathbb{Z}^m, \ker(X)) \subseteq \frac{1}{\det(XX^{\mathsf{t}})} \cdot \mathbb{Z}^m$, hence $\pi(\mathbb{Z}^m, \ker(X))$ is a lattice. Now, we apply Lemma 2 with $L = \mathbb{Z}^m$ and $E = \ker(X)$ to obtain

$$\Lambda^\perp(X)^\star = (\mathbb{Z}^m \cap \ker(X))^\star = \pi(\mathbb{Z}^m, \ker(X)) = (\mathbb{Z}^m + X^{\mathsf{t}}\mathbb{R}^n) \cap \ker(X).$$

In the last equation, we use the fact that $(\ker(X))^\perp = X^{\mathsf{t}}\mathbb{R}^n$. □

2.2 Lattice Gaussian distributions and the smoothing parameter

For a rank-n matrix $S \in \mathbb{R}^{m\times n}$ and vector $\mathbf{c} \in \mathbb{R}^n$, the Gaussian function on $\mathbb{R}^n$ centered at $\mathbf{c}$ with covariance matrix $S^{\mathrm{t}}S$ is defined as:

$$\forall\, \mathbf{x} \in \mathbb{R}^n,\, \rho_{S,\mathbf{c}}(\mathbf{x}) = \exp(-\pi(\mathbf{x}-\mathbf{c})^{\mathrm{t}}(S^{\mathrm{t}}S)^{-1}(\mathbf{x}-\mathbf{c})).$$

Given a rank-d lattice $L \subset \mathbb{R}^m$, the discrete Gaussian distribution with support L, covariance parameter S and shift $\mathbf{c}$ is defined as:

$$\forall\, \mathbf{x} \in L, \mathcal{D}_{L,S,\mathbf{c}}(\mathbf{x}) = \frac{\rho_{S,\mathbf{c}}(\mathbf{x})}{\rho_{S,\mathbf{c}}(L)},$$

where $\rho_{S,\mathbf{c}}(L) = \sum_{\mathbf{x}\in L} \rho_{S,\mathbf{c}}(\mathbf{x})$. When $S = sI_n$ for some real $s > 0$, we write $\rho_{s,\mathbf{c}}$, resp. $D_{L,s,\mathbf{c}}$, the associated (spherical) function, resp. distribution, and we omit the subscript $\mathbf{c}$ when it is $\mathbf{0}$.

We will make use of the following tail bound for discrete Gaussians [5]. This precise formulation is borrowed from [9, Lemma 2.13].

Lemma 4 *For any rank-d lattice L, $s > 0$ and $t \geq 1$, we have*

$$\Pr_{\mathbf{v}\leftarrow D_{L,s}}\left[\|\mathbf{v}\| > s\cdot t\sqrt{\frac{d}{2\pi}}\right] \leq \exp\left(-\frac{d}{2}(t-1)^2\right).$$

We will use the following consequence of the Poisson summation formula:

$$\rho_S(\Lambda) = \det(\Lambda^\star)\cdot\sqrt{\det(S^{\mathrm{t}}S)}\cdot\rho_{S(S^{\mathrm{t}}S)^{-1}}(\Lambda^\star),$$

for any rank-d lattice Λ and any matrix $S \in \mathbb{R}^{m\times n}$ of rank n. The definition of the smoothing parameter is motivated by the Poisson summation formula. Given $\varepsilon > 0$ and a lattice L, the *smoothing parameter* $\eta_\varepsilon(L)$ is defined as the smallest real $s > 0$ such that $\rho_{1/s}(L^\star \setminus \{\mathbf{0}\}) \leq \varepsilon$. We recall below standard upper bounds on this parameter, involving lattice minima.

Lemma 5 ([23, Lemma 3.5]) *For any rank-d lattice L and $\varepsilon > 0$, we have*

$$\eta_\varepsilon(L) \leq \frac{\sqrt{\ln(2d(1+\frac{1}{\varepsilon}))/\pi}}{\lambda_1^\infty(L^\star)}.$$

Lemma 6 ([24, Lemma 2.6], [5, Lemma 1.5]) *For any rank-d lattice L and $\varepsilon \in (0, e^{-d}]$, we have*

$$\eta_\varepsilon(L) \leq \frac{\sqrt{\ln(\frac{1}{\varepsilon})}}{\lambda_1(L^\star)}.$$

First, Lemma 5 and Lemma 6 differ in terms of the norm considered for the first minimum of the dual lattice. Second, these lemmas give different smoothing parameter bounds for different ε-regimes: depending on the smallness of ε, one of the lemmas may give a tighter statement than the other. In particular, in our results, we will obtain a probabilistic lower bound on $\lambda_1(L^\star)$ for a rank-d orthogonal lattice L that is larger than a lower bound on $\lambda_1^\infty(L^\star)$ by a factor quasi-linear in $\sqrt{d}$. It follows that for small ε (e.g., $\varepsilon = 2^{-o(d)}$), Lemma 6 is preferable to Lemma 5.

When ε is large, Lemma 6 may not be applicable, whereas Lemma 5 still provides a bound.

The smoothing parameter of a lattice can alternatively be bounded using the last minimum of the (primal) lattice.

Lemma 7 ([4, Lemma 2.13] and [18, Lemma 3.3]) *For any rank-d lattice L and $\varepsilon \in (0, 1/2)$, we have*

$$\frac{\lambda_d(L)}{\sqrt{d}} \leq \eta_\varepsilon(L) \leq \lambda_d(L) \cdot \sqrt{\ln\left(2d\left(1+\frac{1}{\varepsilon}\right)\right)/\pi}.$$

2.3 Properties of smoothed Gaussians

The first lemma states that the Gaussian mass of a subset of a lattice L does not differ too much from the Gaussian mass of a small shift of it.

Lemma 8 ([2, Lemma 6]) *Fix a rank-d lattice $L \subseteq \mathbb{R}^d$, $\varepsilon \in (0, 1)$, $c > 2$, and $s \geq (1+c)\eta_\varepsilon(L)$. Then, for any subset $T \subseteq L$ and for any $\mathbf{v} \in L$, we have*

$$D_{L,s}(T) - D_{L,s}(T - \mathbf{v}) \leq \frac{\mathrm{erf}(p(1+4/c)/2)}{\mathrm{erf}(2p)} \cdot \frac{1+\varepsilon}{1-\varepsilon},$$

where $p = \frac{\|\mathbf{v}\|\sqrt{\pi}}{s}$, and $\mathrm{erf}(\cdot)$ is the error function.

The following lemma implies that an integral lattice, generated by the columns sampled from a discrete Gaussian distribution over $\mathbb{Z}^n$, spans all of $\mathbb{Z}^n$ with overwhelming probability, if the standard deviation of this distribution is sufficiently large. It also provides information on the matrix that maps X to the canonical basis of $\mathbb{Z}^n$.

Lemma 9 (Adapted from [1, Lemma 4.2]) *Let $n \geq 100$ and $\varepsilon \in (0, \frac{1}{1000})$. Further, let s, m be such that $s \geq 9\eta_\varepsilon(\mathbb{Z}^n)$, $m \geq 44n\ln(ns)$. Then, we have*

$$\Pr_{X \leftarrow (D_{\mathbb{Z}^n,s})^m}\left[\exists U \in \mathbb{Z}^{m\times n}\colon XU = I_n \textit{ and } \max_i \|\mathbf{u}_i\| \leq 2\sqrt{44n\ln(sn)}\right] \geq 1 - 2^{-n},$$

where the $\mathbf{u}_i$'s are the columns of U.

We now state the leftover hash lemma involving Gaussians over infinite domains, the topic of study of [2].

Lemma 10 ([2, Lemma 10]) *Let $m > n \geq 1$ be integers and $\varepsilon \in (0, 1/3)$. Let $X \in \mathbb{Z}^{n\times m}$ such that the columns of X span all of $\mathbb{Z}^n$. If $s' \geq \eta_\varepsilon(\Lambda^\perp(X))$, then we have*

$$\Delta(X \cdot D_{\mathbb{Z}^m,s'}, D_{\mathbb{Z}^m,s'X^t}) \leq 2\varepsilon.$$

3 Smoothing parameter of the orthogonal lattice

This section is devoted to proving our first main result: a tighter upper bound on the smoothing parameter of $\Lambda^{\perp}(X)$, where the columns of $X \in \mathbb{Z}^{n\times m}$ are chosen from the discrete Gaussian $D_{\mathbb{Z}^n,s}$. In the rest of this article, we view all other parameters as functions of n. We stress that Theorem 4 below differs from Theorem 1 in that the asymptotic notations are made explicit by specifying the constants. In this section and the next, we keep these constants explicit. We do not claim that they are optimal in some sense: we provide them to help the reader follow the proofs.

Theorem 4 *Let $n \geq 60$, $\varepsilon > 0$, $s \geq 20\sqrt{n}$, and $m \geq 1355n\ln s$. Then, we have*

$$\Pr_{X\leftarrow(D_{\mathbb{Z}^n,s})^m}\left[\eta_\varepsilon(\Lambda^{\perp}(X)) \leq 77\sqrt{(n+\ln m)\cdot\ln(2m/\varepsilon)}\right] \geq 1-2^{-\Omega(n)}.$$

For any $\varepsilon \leq e^{-(m-n)}$, we also have

$$\Pr_{X\leftarrow(D_{\mathbb{Z}^n,s})^m}\left[\eta_\varepsilon(\Lambda^{\perp}(X)) \leq 96\sqrt{\ln(1/\varepsilon)}\right] \geq 1-2^{-\Omega(n)}.$$

We now give an informal description of the proof strategy. The first part of the proof is similar to the proof presented in [2]: we first embed the lattice $X^{\mathsf{t}}\mathbb{Z}^n$ into a full rank q-ary lattice $\Lambda_q(X)$ by "adding" all the vectors $q\mathbf{e}_i$ to $X^{\mathsf{t}}\mathbb{Z}^n$ (where the $\mathbf{e}_i$'s are the canonical basis vectors). If q is set sufficiently large, then the short vectors in $\Lambda_q(X)$ should come only from the rows of X (with overwhelming probability) and thus be common to the short vectors of $X^{\mathsf{t}}\mathbb{Z}^n$. Starting from this intuition, the authors of [2] provide a lower bound on the norms of the vectors *not* belonging to the row span of X. We improve their bound by an $\Omega(n)$ factor by using tighter arguments on several estimations during the proof. This lower bound also gives a lower bound on $\lambda_{n+1}(\Lambda_q(X))$ since $X^{\mathsf{t}}\mathbb{Q}^n$ spans an vector space of dimension at most n. We also observe that a lower bound on the infinity norms of vectors in $\Lambda_q(X)\setminus X^{\mathsf{t}}\mathbb{Z}^n$ can be derived from the proof, without relying on a loose norm equivalence.

The second part of the proof differs from the one of [2]: we observe that we can directly relate the $(n+1)$-th minimum of $\Lambda_q(X)$ to the first minimum of $\Lambda^{\perp}(X)^{\star}$. This avoids relying twice on a transference argument, as in [2], which allows us to save another $\Omega(\sqrt{n})$ factor. The final result on the smoothing parameter is then a consequence of Lemmas 5 and 6.

As a direct corollary of Theorem 4, we obtain the following leftover hash lemma over lattices.

Corollary 1 *Let $n \geq 100$, $\varepsilon \in \left(0, \frac{1}{1000}\right)$, $s \geq 20\sqrt{n}$ and $m > 1355n\ln s$. Let $s' \geq 77\sqrt{(n+\ln m)\cdot\ln(2m/\varepsilon)}$. Then, we have*

$$\Pr_{X\leftarrow(D_{\mathbb{Z}^n,s})^m}\left[\Delta(X\cdot D_{\mathbb{Z}^m,s}, D_{\mathbb{Z}^m,s'X^{\mathsf{t}}}) \leq 2\varepsilon\right] \geq 1-2^{-\Omega(n)}.$$

If moreover $\varepsilon \leq e^{-(m-n)}$, then the same result holds with $s' \geq 96\sqrt{\ln(1/\varepsilon)}$.

Proof. Using Lemma 9 with the parameters as in the statement, the columns of X span $\mathbb{Z}^n$ with probability $1-2^{-\Omega(n)}$. Now, from Theorem 4, these parameters also ensure that with probability at least $1-2^{-\Omega(n)}$, we have $\eta_\varepsilon(\Lambda^{\perp}(X)) \leq s'$. Finally, Lemma 10 states that when the columns of X span $\mathbb{Z}^n$ and s' is chosen such that $\eta_\varepsilon(\Lambda^{\perp}(X)) \leq s'$, we have $\Delta(X\cdot D_{\mathbb{Z}^m,s}, D_{\mathbb{Z}^m,s'X^{\mathsf{t}}}) \leq 2\varepsilon$. □

3.1 Short vectors in the Construction A lattice of a Gaussian matrix

This section deals with short vectors in $\varLambda_q(X) \setminus X^{\mathsf{t}}\mathbb{Z}^n$. More precisely, we prove the following theorems.

Theorem 5 *Let $n \geq 60$, $q \geq 2$, $m \geq 335n \ln q$ be integers, and $s \geq 20\sqrt{n}$. Then, we have*

$$\Pr_{X \leftarrow (D_{\mathbb{Z}^n,s})^m} \left[\exists \mathbf{b} \in \varLambda_q(X) \setminus X^{\mathsf{t}}\mathbb{Z}^n : \|\mathbf{b}\| < \frac{q}{48} \right] \leq 2^{-\Omega(n)}.$$

As the vector space $X^{\mathsf{t}}\mathbb{Q}^n$ has dimension at most n, the above also gives a lower bound to $\lambda_{n+1}(\varLambda_q(X))$. We are also able to obtain a similar statement for the infinity norm. This result does not follow from just using the equivalence of norms and Theorem 5.

Theorem 6 *Let $n \geq 7, q \geq 2$, $m \geq 20n \ln q$ be integers, and $s \geq 20\sqrt{n}$. Then, we have*

$$\Pr_{X \leftarrow (D_{\mathbb{Z}^n,s})^m} \left[\exists \mathbf{b} \in \varLambda_q(X) \setminus X^{\mathsf{t}}\mathbb{Z}^n : \|\mathbf{b}\|_\infty < \frac{q}{48\sqrt{n + \ln m}} \right] \leq 2^{-\Omega(n)}.$$

For the sake of readability, we split the proofs into several lemmas. The theorems follow from these lemmas and their proofs are given at the end of this subsection. We now give an overview of the proofs of the lemmas.

Recall that $\varLambda_q(X)$ is a lattice spanned by the rows of X and the vectors $q\mathbf{e}_i$.In particular, it contains the integer span of the rows of X, which is of dimension at most n. The purpose of the following lemmas is to prove that every vector in $\varLambda_q(X)$ that is not in the linear span of the rows of X, is of Euclidean norm $\Omega(q)$. In order to show this, we look at the vectors of the form $[X^{\mathsf{t}}\mathbf{z}]_q \in \varLambda_q(X) \setminus X^{\mathsf{t}}\mathbb{Z}^n$ for $\mathbf{z} \in \mathbb{Z}^n$. This is indeed enough as any vector in $\varLambda_q(X)$ can be written $X^{\mathsf{t}}\mathbf{z} + q\mathbf{y}$ for some $\mathbf{z} \in [\![-\frac{q}{2}, \frac{q}{2}[\![^n$ and $\mathbf{y} \in \mathbb{Z}^m$. To obtain a lower bound on the norms of such vectors, we divide the proof into two cases depending on the norm of $\mathbf{z}$.

In the first lemma, we prove for a "short" $\mathbf{z}$ that, with all but probability $2^{-\Omega(n)}$, the vector $[X^{\mathsf{t}}\mathbf{z}]_q$ belongs to the row-span of X. This part of our proof differs from the one of [2] as we bypass norm equivalence between Euclidean and infinity norms. The second lemma deals with the other ranges of $\mathbf{z}$: we obtain a lower bound on the entries of $[X^{\mathsf{t}}\mathbf{z}]_q$ by first proving a probabilistic lower bound on $[\langle \mathbf{x} \, , \mathbf{z} \rangle]_q$ taken over a Gaussian vector $\mathbf{x}$. For a "large" $\mathbf{z}$, the proof is identical to the proof of [2]. This is detailed in the proof of Lemma 12. Finally, we extend this argument from a vector $\mathbf{x}$ to a matrix X using Hoeffding's inequality. This part of the proof is also new.

Lemma 11 *Let $m, n, q \geq 2$ be integers. Then we have*

$$\Pr \left[\exists \, \mathbf{z} \in \mathbb{Z}^n \text{ with } \|\mathbf{z}\| < \frac{q}{4s\sqrt{n + \ln m}} \; : \; [X^{\mathsf{t}}\mathbf{z}]_q \in \varLambda_q(X) \setminus X^{\mathsf{t}}\mathbb{Z}^n \right] \leq 2^{-n},$$

where the probability is taken over $X \leftarrow (D_{\mathbb{Z}^n,s})^m$.

Proof. Each row $\mathbf{x}_i$ is distributed as $D_{\mathbb{Z}^n,s}$. Let $t = \sqrt{2\pi(1 + (\ln m)/n)}+1$. Lemma 4 gives that $\Pr_X[\|\mathbf{x}_i\| > st\sqrt{n/2\pi}] \leq 2^{-n}/m$. When this does not occur, we have, for any integer vector $\mathbf{z}$ with $\|\mathbf{z}\| \leq \frac{q}{4s\sqrt{n+\ln m}} \leq \frac{q\sqrt{2\pi}}{2st\sqrt{n}}$:

$$|\langle \mathbf{z}, \mathbf{x}_i \rangle| \leq \|\mathbf{z}\| \cdot \|\mathbf{x}_i\| < \frac{q}{2}.$$

The result follows by union bound over $i \in [m]$. □

We now consider longer $\mathbf{z}$'s. We show that the probability that their inner product with a Gaussian vector is quite smaller than q is bounded away from 1 by a constant.

Lemma 12 *Let $m, n \geq 7$ and $q \geq 2$ be integers and $s \geq 20\sqrt{n}$. For any $\mathbf{z} \in [\![-\frac{q}{2}, \frac{q}{2}[\![^n$ such that $\|\mathbf{z}\| \geq \frac{q}{4s\sqrt{n+\ln m}}$, we have*

$$\Pr_{\mathbf{x} \leftarrow D_{\mathbb{Z}^n,s}} \left[|[\langle \mathbf{x}, \mathbf{z} \rangle]_q| < \frac{q}{48\sqrt{n + \ln m}} \right] \leq 0.95.$$

We first outline the main ideas of the proof. For a fixed $\mathbf{z}$, our concern is the vectors $\mathbf{x} \in \mathbb{Z}^n$ whose inner-products with $\mathbf{z}$ are "small" when reduced modulo q: they lead to vectors in the lattice $X^{\mathsf{t}}\mathbb{Z}^n$ that are shorter than what we would expect. Thus, we shall call them "$\mathrm{Bad}_{\mathbf{z}}$" vectors. Then we show that a suitably chosen translation maps any "$\mathrm{Bad}_{\mathbf{z}}$" vector $\mathbf{x}$ to a "$\mathrm{Good}_{\mathbf{z}}$" vector $\mathbf{x}'$, such that the inner-product between $\mathbf{x}'$ and $\mathbf{z}$ is "large". This proof technique is borrowed from [2]; however, we refine it by splitting the ranges of $\|\mathbf{z}\|$ further and finding a better translation map for medium $\|\mathbf{z}\|$. In either case, the translation vectors turn out to be short enough to argue that the probabilities of sampling a "$\mathrm{Bad}_{\mathbf{z}}$" $\mathbf{x}$ and a "$\mathrm{Good}_{\mathbf{z}}$" $\mathbf{x}$ are relatively close. From there, we readily obtain an upper bound on the probability that $\mathbf{x}$ is "$\mathrm{Bad}_{\mathbf{z}}$". Below we quantify the terms "large" and "short", "$\mathrm{Bad}_{\mathbf{z}}$" and "$\mathrm{Good}_{\mathbf{z}}$", and provide formal arguments.

Proof. Fix a $\mathbf{z}$ as in the statement and define the set of "$\mathrm{Bad}_{\mathbf{z}}$" vectors as

$$\mathrm{Bad}_{\mathbf{z}} := \left\{ \mathbf{x} \in \mathbb{Z}^n : |[\langle \mathbf{z}, \mathbf{x} \rangle]_q| < \frac{q}{48\sqrt{n + \ln m}} \right\}.$$

We also define $\mathrm{Good}_{\mathbf{z}} = \mathbb{Z}^n \setminus \mathrm{Bad}_{\mathbf{z}}$, i.e., vectors outside the set $\mathrm{Bad}_{\mathbf{z}}$ will be considered as "good".

Case 1: "Medium" $\mathbf{z}$, i.e., $\frac{q}{4s\sqrt{n+\ln m}} \leq \|\mathbf{z}\| < \frac{q}{2s}$.

We let $\mu = \lceil \frac{s}{6\sqrt{n}} \rceil$. If $\mathbf{x} \in \mathrm{Bad}_{\mathbf{z}}$, then we can obtain a $\mathrm{Good}_{\mathbf{z}}$ vector using the injective map

$$\begin{aligned} \mathrm{Bad}_{\mathbf{z}} &\longrightarrow \mathrm{Good}_{\mathbf{z}} \\ \mathbf{x} &\longmapsto \mathbf{x} + \mu \left\lceil \tfrac{2\mathbf{z}\sqrt{n}}{\|\mathbf{z}\|} \right\rceil, \end{aligned}$$

where the ceiling is taken coordinate-wise. Now, we show that the map indeed sends $\mathrm{Bad}_{\mathbf{z}}$ to $\mathrm{Good}_{\mathbf{z}}$. First, we note that $\langle \mathbf{z}, \lceil 2\mathbf{z}\sqrt{n}/\|\mathbf{z}\| \rceil \rangle \geq 0$, because a and $\lceil a \rceil$ have the same sign for any $a \in \mathbb{R}$. Also, by the choice of μ, we have

$$\begin{aligned} 0 \leq \mu \left\langle \mathbf{z}, \left\lceil \frac{2\mathbf{z}\sqrt{n}}{\|\mathbf{z}\|} \right\rceil \right\rangle &\leq \mu \sum_{i \in [n]} \left(|z_i| \cdot \frac{2|z_i|\sqrt{n}}{\|\mathbf{z}\|} + |z_i| \right) \\ &\leq 2\frac{s}{6\sqrt{n}} (2\|\mathbf{z}\|\sqrt{n} + \|\mathbf{z}\|\sqrt{n}) \\ &< \frac{q}{2}, \end{aligned}$$

where for the second inequality we use the fact that $s > 6\sqrt{n}$, and, for the last inequality, the fact that $\|\mathbf{z}\| < \frac{q}{2s}$. Combining this with the fact that $|[a+b]_q| \geq |[a]_q| - |[b]_q|$ for all $a, b \in \mathbb{R}$, we obtain for $\mathbf{x} \in \mathrm{Bad}_{\mathbf{z}}$ that

$$\left| \left[\left\langle \mathbf{z}, \mathbf{x} + \mu \left\lceil \frac{2\mathbf{z}\sqrt{n}}{\|\mathbf{z}\|} \right\rceil \right\rangle \right]_q \right| \geq \mu \left\langle \mathbf{z}, \left\lceil \frac{2\mathbf{z}\sqrt{n}}{\|\mathbf{z}\|} \right\rceil \right\rangle - |[\langle \mathbf{z}, \mathbf{x} \rangle]_q|.$$

Since $\|\mathbf{z}\| \geq \frac{q}{4s\sqrt{n+\ln m}}$ and $|[\langle \mathbf{z}, \mathbf{x} \rangle]_q| \leq \frac{q}{48\sqrt{n+\ln m}}$, we have

$$\begin{aligned} \mu \left\langle \mathbf{z}, \left\lceil \frac{2\mathbf{z}\sqrt{n}}{\|\mathbf{z}\|} \right\rceil \right\rangle - |[\langle \mathbf{z}, \mathbf{x} \rangle]_q| &\geq \mu \sum_{i \in [n]} \left(|z_i| \cdot \frac{2|z_i|\sqrt{n}}{\|\mathbf{z}\|} - |z_i| \right) - \frac{q}{48\sqrt{n + \ln m}} \\ &\geq \frac{s}{6\sqrt{n}} (2\|\mathbf{z}\|\sqrt{n} - \|\mathbf{z}\|\sqrt{n}) - \frac{q}{48\sqrt{n + \ln m}} \\ &\geq \frac{q}{48\sqrt{n + \ln m}}. \end{aligned}$$

This implies that $\mathbf{x} + \mu \left\lceil \frac{2\mathbf{z}\sqrt{n}}{\|\mathbf{z}\|} \right\rceil \in \mathrm{Good}_{\mathbf{z}}$.

Now, we want to apply Lemma 8 with $\mathbf{v} = \mu \lceil 2\mathbf{z}\sqrt{n}/\|\mathbf{z}\| \rceil$. For this, we bound $\|\mathbf{v}\|$ from above. Using that $\lceil a \rceil^2 \leq (|a|+1)^2$ for any $a \in \mathbb{R}$, we have

$$\left\| \left\lceil \frac{2\mathbf{z}\sqrt{n}}{\|\mathbf{z}\|} \right\rceil \right\|^2 \leq \sum_{i \in [n]} \left(\frac{2\sqrt{n}|z_i|}{\|\mathbf{z}\|} + 1 \right)^2 = \left\| \frac{2\sqrt{n}|\mathbf{z}|}{\|\mathbf{z}\|} + \mathbf{1}_n \right\|^2,$$

where $|\mathbf{z}| = (|z_1|, \ldots, |z_n|)$. This gives us

$$\begin{aligned} \|\mathbf{v}\| = \mu \left\| \left\lceil \frac{2\mathbf{z}\sqrt{n}}{\|\mathbf{z}\|} \right\rceil \right\| &\leq \mu \left(\left\| \frac{2\sqrt{n}|\mathbf{z}|}{\|\mathbf{z}\|} \right\| + \|\mathbf{1}_n\| \right) \\ &\leq \frac{2s}{6\sqrt{n}} \cdot 3\sqrt{n} = s. \end{aligned}$$

Now, we apply Lemma 8 with parameters $L = \mathbb{Z}^n$, $\varepsilon = 1/1000$, $c = 14$, $\mathbf{v} = \mu \lceil 2\mathbf{z}\sqrt{n}/\|\mathbf{z}\| \rceil$ and $p = \|\mathbf{v}\|\sqrt{\pi}/s \leq \sqrt{\pi}$. The assumption of Lemma 8 is indeed satisfied for these parameters. This gives that

$$\Pr_{\mathbf{x}}[\mathbf{x} \in \mathrm{Bad}_{\mathbf{z}}] - \Pr_{\mathbf{x}}[\mathbf{x} \in \mathrm{Good}_{\mathbf{z}}] \leq \frac{\mathrm{erf}(p(1 + \frac{4}{c})/2)}{\mathrm{erf}(2p)} \cdot \frac{1+\varepsilon}{1-\varepsilon} \leq 0.9.$$

Since we always have that $\Pr_{\mathbf{x}}[\mathbf{x} \in \mathrm{Bad}_{\mathbf{z}}] + \Pr_{\mathbf{x}}[\mathbf{x} \in \mathrm{Good}_{\mathbf{z}}] = 1$, it holds that $\Pr_{\mathbf{x}}[\mathbf{x} \in \mathrm{Bad}_{\mathbf{z}}] \leq \frac{1+0.9}{2}$. We conclude that $\Pr_{\mathbf{x}} \left[|[\langle \mathbf{x}, \mathbf{z} \rangle]_q| < \frac{q}{48\sqrt{n+\ln m}} \right] \leq 0.95$.

Case 2: "Long" $\mathbf{z}$, i.e., $\mathbf{z} \in \llbracket -\frac{q}{2}, \frac{q}{2} \llbracket^n$ and $\|\mathbf{z}\| \geq \frac{q}{2s}$.
This part of the proof is the same as in [2, Lemma 11]. We reproduce it for the sake of completeness. Consider a "long" $\mathbf{z}$, i.e., $\|\mathbf{z}\| \geq \frac{q}{2s}$, which implies $\|\mathbf{z}\|_\infty \geq \frac{q}{2s\sqrt{n}}$. We modify the mapping defined in Case 1 from $\mathrm{Bad}_{\mathbf{z}}$ to $\mathrm{Good}_{\mathbf{z}}$ vectors by letting $\mu := \min\{\lceil s \rceil, \lfloor \frac{q}{2\|\mathbf{z}\|_\infty} \rfloor\}$ and defining:

$$\begin{aligned} \mathrm{Bad}_{\mathbf{z}} &\to \mathrm{Good}_{\mathbf{z}} \\ \mathbf{x} &\mapsto \mathbf{x} + \mu \mathbf{e}_{i_{\max}}, \end{aligned}$$

where $i_{\max}$ is the index of a largest entry in $\mathbf{z}$ (in absolute value).

We now prove that the map indeed sends $\mathrm{Bad}_{\mathbf{z}}$ to $\mathrm{Good}_{\mathbf{z}}$. We have $\mu\|\mathbf{z}\|_\infty \leq \frac{q}{2\|\mathbf{z}\|_\infty}\|\mathbf{z}\|_\infty \leq \frac{q}{2}$. Therefore, it holds that

$$|[\langle \mathbf{z}, \mathbf{x} + \mu \mathbf{e}_{i_{\max}}\rangle]_q| = |[\langle \mathbf{z}, \mathbf{x}\rangle \pm \mu\|\mathbf{z}\|_\infty]_q| \geq \mu\|\mathbf{z}\|_\infty - |[\langle \mathbf{z}, \mathbf{x}\rangle]_q|.$$

First, assume that $\mu = \lceil s \rceil$. Using the facts that $\|\mathbf{z}\|_\infty > \frac{q}{2s\sqrt{n}}$ and $|[\langle \mathbf{z}, \mathbf{x}\rangle]_q| < \frac{q}{48\sqrt{n+\ln m}}$ for $\mathbf{x} \in \mathrm{Bad}_{\mathbf{z}}$, we obtain

$$\mu\|\mathbf{z}\|_\infty - |[\langle \mathbf{z}, \mathbf{x}\rangle]_q| > s\frac{q}{2s\sqrt{n}} - \frac{q}{48\sqrt{n+\ln m}} > \frac{q}{48\sqrt{n+\ln m}}.$$

Now, assume that $\mu = \left\lfloor \frac{q}{2\|\mathbf{z}\|_\infty} \right\rfloor$. For $\mathbf{x} \in \mathrm{Bad}_{\mathbf{z}}$, it implies that

$$\mu\|\mathbf{z}\|_\infty - |[\langle \mathbf{z}, \mathbf{x}\rangle]_q| > \frac{q}{6\|\mathbf{z}\|_\infty} \cdot \|\mathbf{z}\|_\infty - \frac{q}{48\sqrt{n+\ln m}} > \frac{q}{48\sqrt{n+\ln m}}.$$

In both cases, we have $|[\langle \mathbf{z}, \mathbf{x} + \mu \mathbf{e}_{i_{\max}}\rangle]_q| > \frac{q}{48\sqrt{n+\ln m}}$.

We apply Lemma 8 with parameters $L = \mathbb{Z}^n$, $\varepsilon = 1/1000, c = 35$, and $\mathbf{v} = \mu \mathbf{e}_{i_{\max}}$. The assumption of Lemma 8 is indeed satisfied for these parameters. Note that $\|\mathbf{v}\| = \mu < s+1$, and $p := \frac{\|\mathbf{v}\|\sqrt{\pi}}{s} < \frac{s+1}{s}\sqrt{\pi} < \frac{20\sqrt{n}+1}{20\sqrt{n}}\sqrt{\pi} < 1.02\sqrt{\pi}$. Similarly to the previous case it follows that $\Pr_{\mathbf{x}}[\mathbf{x} \in \mathrm{Bad}_{\mathbf{z}}] - \Pr_{\mathbf{x}}[\mathbf{x} \in \mathrm{Good}_{\mathbf{z}}] \leq 0.9$. Hence, we obtain $\Pr_{\mathbf{x}}[\mathbf{x} \in \mathrm{Bad}] \leq 0.95$. □

Using Lemma 12 and Hoeffding's bound, we can now show that with overwhelming probability over the choice of X, there are more than $n + \ln m$ entries of $[X^{\mathsf{t}}\mathbf{z}]_q$ that have magnitude larger than $\frac{q}{48\sqrt{n+\ln m}}$ for any not too short $\mathbf{z} \in [\![-\frac{q}{2}, \frac{q}{2}[\![^n$. This implies the following result.

Lemma 13 *Let $n \geq 60$, $q \geq 2$, $m \geq 335n\ln q$ be integers, and $s \geq 20\sqrt{n}$.Then, we have*

$$\Pr\left[\forall \mathbf{z} \in \left[\!\!\left[-\frac{q}{2}, \frac{q}{2}\right[\!\!\right[^n \textit{with}\, \|\mathbf{z}\| \geq \frac{q}{4s\sqrt{n+\ln m}} : \|[X^{\mathsf{t}}\mathbf{z}]_q\| \geq \frac{q}{48}\right] > 1 - 2 \cdot 2^{-0.001m},$$

where the probability is taken over $X \leftarrow (D_{\mathbb{Z}^n,s})^m$.

Proof. Fix $\mathbf{z}$ with $\|\mathbf{z}\| \geq \frac{q}{4s\sqrt{n+\ln m}}$. For $i \in [m]$, consider independent binary random variables Y_i, defined over the choice of the columns $\mathbf{x}_i$ of X:

$$\begin{cases} Y_i = 1 \text{ if } |[\langle \mathbf{x}_i, \mathbf{z}\rangle]_q| \geq \frac{q}{48\sqrt{n+\ln m}}, \\ Y_i = 0 \text{ otherwise.} \end{cases}$$

From Lemma 12, it follows that $\Pr_X[Y_i = 1] \geq 0.05$. Therefore by linearity of expectation, we have $\mathbb{E}\left[\sum_i Y_i\right] \geq 0.05m$. Using Hoeffding's bound (Lemma 1) with $t = 0.05m - (n + \ln m)$, we obtain

$$\Pr\left[|\sum_i Y_i - \mathbb{E}[\sum_i Y_i]| \geq 0.05m - (n+\ln m)\right]$$
$$\leq 2\exp\Big(-2\frac{(0.05m - (n+\ln m))^2}{m}\Big).$$

Hence, for $m \geq 200(n + \ln m)$ (which is implied by the condition $m \geq 335n \ln q$), we have

$$\begin{aligned}\Pr_X\left[\sum_i Y_i < n + \ln m\right] &\leq \Pr_X\left[0.05m - \sum_i Y_i \geq 0.05m - (n + \ln m)\right] \\ &\leq 2\exp\left(-2\frac{(0.05m - (n + \ln m))^2}{m}\right) \\ &\leq 2\exp(-0.004m).\end{aligned}$$

The inequality above holds for any $\mathbf{z} \in [\![-\frac{q}{2}, \frac{q}{2}[\![^n$ with $\|\mathbf{z}\| \geq \frac{q}{4s\sqrt{n+\ln m}}$. Using the lower bound on m, $m \geq 335n \ln q$, we conclude that

$$\begin{aligned}&\Pr\left[\exists \mathbf{z} \in \left[\!\!\left[-\frac{q}{2}, \frac{q}{2}\right[\!\!\right[^n \text{with } \|\mathbf{z}\| \geq \frac{q}{4s\sqrt{n + \ln m}} : \sum_i Y_i < n + \ln m\right] \\ &\quad < 2q^n \cdot e^{-0.004m} \\ &\quad < 2 \cdot e^{-0.001m}.\end{aligned}$$

Since $\sum_i Y_i \geq n + \ln m$ implies that $\|[X^{\mathrm{t}}\mathbf{z}]_q\| \geq \frac{q}{48}$, the result follows. □

We are now in a position to prove our first main results.

Proof of Theorem 5. The choice of parameters allows us to use both Lemma 11 and Lemma 13. Their combination tells us that, with all but probability $2^{-\Omega(n)}$ over the choice of X, there does not exist any vector $\mathbf{z} \in [\![-\frac{q}{2}, \frac{q}{2}[\![^n$ for which $[X^{\mathrm{t}}\mathbf{z}]_q \notin X^{\mathrm{t}}\mathbb{Z}^n$ and $\|[X^{\mathrm{t}}\mathbf{z}]_q\| < \frac{q}{48}$. This gives the first result. □

Proof of Theorem 6. We show that if $\mathbf{v} \in \Lambda_q(X) \setminus X^{\mathrm{t}}\mathbb{Z}^n$, then $\|\mathbf{v}\|_\infty \geq \frac{q}{48\sqrt{n+\ln m}}$ with overwhelming probability. For $\mathbf{z} \in [\![-\frac{q}{2}, \frac{q}{2}[\![^n$ and $\|\mathbf{z}\| \geq \frac{q}{4s\sqrt{n+\ln m}}$, we have from Lemma 12 that $\Pr_{\mathbf{x}}[|[\langle \mathbf{x}, \mathbf{z}\rangle]_q| < \frac{q}{48\sqrt{n+\ln m}}] \leq 0.95$. It follows that

$$\Pr_X\left[\left\|[X^{\mathrm{t}}\mathbf{z}]_q\right\|_\infty < \frac{q}{48\sqrt{n + \ln m}}\right] \leq 0.95^m \leq e^{-0.05m}.$$

By the union bound, we obtain

$$\Pr_X\left[\exists\ \mathbf{z} : \|[X^{\mathrm{t}}\mathbf{z}]_q\|_\infty < \frac{q}{48\sqrt{n + \ln m}}\right] \leq q^n \cdot e^{-0.05m} = 2^{-\Omega(n)}.$$

Combining the above with Lemma 11, we conclude that with all but probability $2^{-\Omega(n)}$ over the choice of X, there does not exist any vector $\mathbf{z} \in [\![-\frac{q}{2}, \frac{q}{2}[\![^n$ for which $[X^{\mathrm{t}}\mathbf{z}]_q \notin X^{\mathrm{t}}\mathbb{Z}^n$ and $\|[X^{\mathrm{t}}\mathbf{z}]_q\|_\infty < \frac{q}{48\sqrt{n+\ln m}}$. This completes the proof. □

3.2 Using the dual of $\Lambda^{\perp}(X)$

We want to find an upper bound on the smoothing parameter of $\Lambda^{\perp}(X)$. Using Lemma 5, such a bound comes from a lower bound on the minimum of the dual lattice of $\Lambda^{\perp}(X)$. We now relate the $(n+1)$-th minimum of the lattice $\Lambda_q(X)$ and the norms of the shortest vectors in $\Lambda^{\perp}(X)^{\star}$. For the proof below, it is useful to recall that $\Lambda^{\perp}(X)^{\star} = (\mathbb{Z}^m + X^{\mathsf{t}}\mathbb{R}^n) \cap \ker(X)$, as showed in Lemma 3.

Lemma 14 *Let $n \geq 60$ and $s \geq 20\sqrt{n}$. Let q and m be integers satisfying $m \geq 335n \ln q$ and that $q \geq 96sn\sqrt{m}$ We have*

$$\Pr_{X \leftarrow (D_{\mathbb{Z}^n,s})^m}\left[\lambda_1^{\infty}(\Lambda^{\perp}(X)^{\star}) \geq \frac{1}{96\sqrt{n+\ln m}}\right] \geq 1 - 2^{-\Omega(n)},$$

$$\Pr_{X \leftarrow (D_{\mathbb{Z}^n,s})^m}\left[\lambda_1(\Lambda^{\perp}(X)^{\star}) \geq \frac{1}{96}\right] \geq 1 - 2^{-\Omega(n)}.$$

Proof. Let $\mathbf{u}$ be any vector in $\Lambda^{\perp}(X)^{\star}$. From Lemma 3, we can write $\mathbf{u} = \mathbf{k} + X^{\mathsf{t}}\mathbf{y}$, for some $\mathbf{k} \in \mathbb{Z}^m$ and $\mathbf{y} \in \mathbb{R}^n$. Let $\mathbf{z} \in \mathbb{R}^n$ with $\|\mathbf{z}\|_{\infty} < \frac{1}{q}$ such that $\mathbf{y} = \mathbf{y}' + \mathbf{z}$ and $\mathbf{y}' \in \frac{1}{q}\mathbb{Z}^n$. Thus, we can write $\mathbf{u} = \mathbf{v} + X^{\mathsf{t}}\mathbf{z}$, where $\mathbf{v} = \mathbf{k} + X^{\mathsf{t}}\mathbf{y}' \in \frac{1}{q}\Lambda_q(X)$.

Assume now that $\mathbf{u}$ is a non-zero vector of $\Lambda^{\perp}(X)^{\star}$. We show by contradiction that $\mathbf{v}$ cannot be in the row-span of X. Assume on the contrary that $\mathbf{v} \in X^{\mathsf{t}}\mathbb{Q}^n$. Then, on the one hand, this implies that $\mathbf{u} \in X^{\mathsf{t}}\mathbb{R}^n = (\ker X)^{\perp}$. On the other hand, we have $\mathbf{u} \in \ker X$ by definition of $\Lambda^{\perp}(X)^{\star}$. Then we must have $\mathbf{u} = \mathbf{0}_m$, which contradicts the choice of $\mathbf{u}$ as a non-zero vector of $\Lambda^{\perp}(X)^{\star}$. In particular, from Theorems 5 and 6,we see that $\|\mathbf{v}\|_{\infty} \geq \frac{1}{48\sqrt{n+\ln m}}$ and $\|\mathbf{v}\| \geq \frac{1}{48}$ with probability at least $1 - 2^{-\Omega(n)}$.

Now, we let $\mathbf{u}$ be such that $\|\mathbf{u}\|_{\infty} = \lambda_1^{\infty}(\Lambda^{\perp}(X)^{\star})$ and we compare it to $\|\mathbf{v}\|_{\infty}$, for $\mathbf{v}$ defined as above. Applying Lemma 4 with $t = \sqrt{2\pi}$, we obtain that with probability greater than $1 - 2^{-n}$, the rows of X^{t} have Euclidean norms smaller than $s\sqrt{n}$. It follows that $\|X^{\mathsf{t}}\mathbf{z}\|_{\infty} \leq \max(\|\mathbf{x}_i\|) \cdot \|\mathbf{z}\| \leq \frac{sn}{q}$. By the triangular inequality, we have $\|\mathbf{v}\|_{\infty} \leq \|\mathbf{u}\|_{\infty} + \|X^{\mathsf{t}}\mathbf{z}\|_{\infty}$, from which we deduce that

$$\|\mathbf{u}\|_{\infty} \geq \|\mathbf{v}\|_{\infty} - \frac{sn}{q}$$

with all but probability at most 2^{-n}. We then deduce using Theorem 6 and the assumptions on m and q that

$$\|\mathbf{v}\|_{\infty} - \frac{sn}{q} \geq \frac{1}{48\sqrt{n+\ln m}} - \frac{sn}{q} \geq \frac{1}{96\sqrt{n+\ln m}},$$

also with probability greater than $1 - 2^{-\Omega(n)}$.

Let now $\mathbf{u}$ be such that $\|\mathbf{u}\| = \lambda_1(\Lambda^{\perp}(X)^{\star})$, and $\mathbf{v}$ be as defined above. By norm equivalence, we have $\|X^{\mathsf{t}}\mathbf{z}\| \leq \sqrt{m}\|X^{\mathsf{t}}\mathbf{z}\|_{\infty} \leq \frac{sn\sqrt{m}}{q}$ except with probability at most 2^{-n}. As above, we deduce that $\|\mathbf{u}\| \geq \|\mathbf{v}\| - \frac{sn\sqrt{m}}{q}$. Using Theorem 5 and the second assumption on q, we obtain

$$\|\mathbf{v}\| - \frac{sn\sqrt{m}}{q} \geq \frac{1}{48} - \frac{sn\sqrt{m}}{q} \geq \frac{1}{96},$$

except with probability at most $2^{-\Omega(n)}$. □

Finally, we complete the proof of our first main result.

Proof (Theorem 4). Let $q = \lceil 96sn\sqrt{m} \rceil$. With this choice, it turns out that any m satisfying $m \geq 1355n \ln s$ also satisfies $m \geq 335n \ln(97sn\sqrt{m})$. By Lemmas 5 and 14,we obtain that, with all but probability $2^{-\Omega(n)}$,

$$\eta_\varepsilon(\Lambda^\perp(X)) \leq \frac{\sqrt{\ln\left(2(m-n)(1+\frac{1}{\varepsilon})\right)/\pi}}{\lambda_1^\infty(\Lambda^\perp(X)^\star)} \leq 96\sqrt{(n+\ln m)\cdot\frac{\ln\left(2(m-n)(1+\frac{1}{\varepsilon})\right)}{\pi}}.$$

Alternatively, for any $\varepsilon \leq 2^{-(m-n)}$, we can use Lemmas 6 and 14 to obtain that (with all but probability $2^{-\Omega(n)}$)

$$\eta_\varepsilon(\Lambda^\perp(X)) \leq \frac{\sqrt{\ln(1/\varepsilon)}}{\lambda_1(\Lambda^\perp(X)^\star)} \leq 96\sqrt{\ln(1/\varepsilon)}.$$

This completes the proof. □

4 Last minimum of $\Lambda^\perp(X)$

In this section we present our second result: an upper bound on the $(m-n)$-th minimum of the orthogonal lattice $\Lambda^\perp(X)$.

The question of finding an upper bound on $\lambda_{m-n}(\Lambda^\perp(X))$ was addressed in [2] and later in [1], with the aim of obtaining an upper bound on the smoothing parameter of $\Lambda^\perp(X)$. In particular, Agrawal et al. in [2] first give a lower bound on $\lambda_{n+1}(\Lambda_q(X))$, then use Banaszczyk's theorem (Theorem 3) to obtain an upper bound on $\lambda_{m-n}(\Lambda_q^\perp(X))$. Finally, they argue that this is also an upper bound on $\lambda_{m-n}(\Lambda^\perp(X))$. Aggarwal and Regev in [1] present a more direct approach to bound $\lambda_{m-n}(\Lambda^\perp(X))$. In all cases, these bounds on the last minimum of $\Lambda^\perp(X)$ were used as a way to bound its smoothing parameter (our approach in Section 3 is in some sense more direct).

We shall need the following lemma, obtained by combining Theorem 5 with Theorem 3.

Lemma 15 *Let $n \geq 60$, $s \geq 20\sqrt{n}$ and $m \geq 1400n \ln s$.Then, we have:*

$$\Pr_{X \leftarrow (D_{\mathbb{Z}^n,s})^m}\left[\lambda_{m-n}(\Lambda^\perp(X)) \leq 48m\right] \geq 1 - 2^{-\Omega(n)}.$$

Proof. Let q be the smallest prime such that $q \geq 96sm^{3/2}$. By [14], there exists a prime in the range $(96sm^{3/2}, 192sm^{3/2})$, hence we have $q < 192sm^{3/2}$.[4] We apply Theorem 5 to conclude that $\lambda_{n+1}(\Lambda_q(X)) \geq \frac{q}{48}$ with overwhelming probability. From Theorem 3 with $i = n+1$, it follows that $\lambda_{m-n}(\Lambda_q^\perp(X)) \leq 48m$. This implies that $\Lambda_q^\perp(X)$ contains $m-n$ linearly independent vectors $\mathbf{v}_1, \ldots, \mathbf{v}_{m-n}$ such that $\|\mathbf{v}_1\| \leq \|\mathbf{v}_2\| \leq \cdots \leq \|\mathbf{v}_{m-n}\| \leq 48m$. As q is prime, we have that $X\mathbf{v}_j = \mathbf{0} \bmod q$ for all $j \in [m-n]$ (see the discussion after Definition 1).

Now, we show that $\mathbf{v}_j \in \Lambda^\perp(X)$ for all $j \in [m-n]$, i.e., that $X\mathbf{v}_j = \mathbf{0}$ over the integers. Thanks to Lemma 4 with $t = \sqrt{2\pi}$, the rows of X have norms bounded

[4] In fact, the following stronger result is proved in [14]: the number of primes in the interval $(x - x^\alpha, x)$ is at least $\frac{x^\alpha}{\log x}$ for $\alpha < 7/12$. To simplify our statements, we use a looser bound.

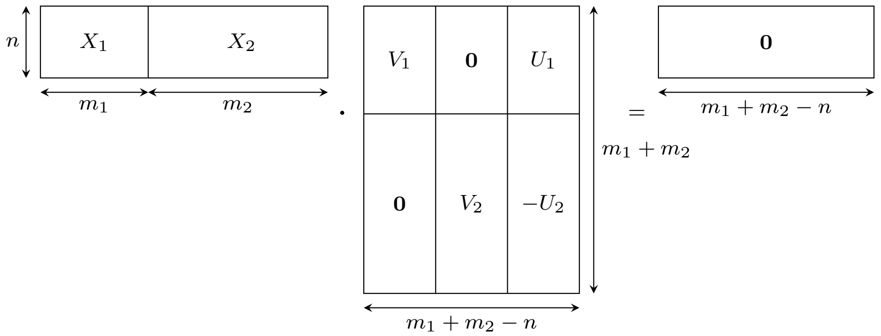

Fig. 2: Given a wide matrix $X = [X_1|X_2] \in \mathbb{Z}^{n\times(m_1+m_2)}$, we first obtain $m_1 + m_2 - n$ linearly independent short vectors in $\Lambda^\perp([X_1|X_2])$. These correspond to the columns $[{V_1}^\mathsf{t}|\mathbf{0}]^\mathsf{t}$ and $[\mathbf{0}|{V_2}^\mathsf{t}]^\mathsf{t}$. The n other missing short vectors are obtained via stacking U_i matrices satisfying $X_iU_i = I_n$, as depicted.

by $s\sqrt{m}$ with probability greater than $1 - 2^{-\Omega(n)}$. Therefore, for any $j \in [m-n]$, we have

$$\|X \cdot \mathbf{v}_j\|_\infty = \max_i |\langle \mathbf{x}_i, \mathbf{v}_j\rangle| \le \max_i \|\mathbf{x}_i\| \cdot \|\mathbf{v}_j\| \le 48sm^{\frac{3}{2}}$$

with overwhelming probability. Our choice of q implies that $\|X \cdot \mathbf{v}_j\|_\infty < q/2$, hence the equality $X \cdot \mathbf{v}_j = \mathbf{0}$ holds over $\mathbb{Z}$. The result follows. □

We now consider the case of a wide matrix X, i.e. with very large m. We split it into t matrices of smaller dimensions $n \times m_i$ for $i \in [t]$, where m_i is independent of m and is large enough to satisfy the conditions of Lemma 15. For simplicity, one could think of m_i's being all equal assuming that m is divisible by m_i. In general, we may not be able to divide m into large enough and equal pieces. This is why our X_i's may have different numbers of columns. Using Lemma 15, we show that every orthogonal lattice defined by such small matrices has $m_i - n$ linearly independent vectors of norm at most $48m_i$. By padding these vectors with zeros appropriately (see Figure 2), we thus find $\sum_{i\in[t]}(m_i - n)$ short and linearly independent vectors in $\Lambda^\perp(X)$. To show that there are, in fact, more short vectors in this lattice, we apply Lemma 9. We can "stack" the U-matrices from this lemma (see Figure 2) to obtain other short vectors orthogonal to X. Thus, in total we obtain $m - n$ short linearly independent vectors in $\Lambda^\perp(X)$ whose norms can be bounded independently from m. In the statement below, we use a Landau notation for the sake of clarity. An explicit constant of 142176 can be used instead.

Theorem 7 *Let $n \ge 100$ and $s \ge 20\sqrt{n}$. Let m such that $2801n\ln s \le m \le 2^{n/2}$. Then, we have*

$$\Pr_{X \leftarrow (D_{\mathbb{Z}^n,s})^m}\left[\lambda_{m-n}(\Lambda^\perp(X)) \le \mathcal{O}\left(n\ln(ns)\right)\right] \ge 1 - 2^{-\Omega(n)}.$$

Proof. We divide our wide matrix X into smaller matrices with appropriate numbers of columns. For $m \ge 2801n\ln s$, we can divide the matrix X into at least two blocks of at least $m' = \lceil 1400n\ln s\rceil$ columns.

We start by splitting X into t smaller matrices $X_i \in \mathbb{Z}^{n \times m_i}$ such that $m_i \in [m', 2m']$ for all $i \in [t]$. We look at X as a block-matrix $X = [X_1|X_2|\ldots|X_t]$, where $X_i \leftarrow (D_{\mathbb{Z}^n,s})^{m_i}$ for all $i \in [t]$. We apply Lemma 15 to each block X_i. The lattice $\Lambda^{\perp}(X_i)$ has $m_i - n$ linearly independent vectors $\mathbf{v}_1^i, \ldots, \mathbf{v}_{m_i-n}^i$ such that

$$\|\mathbf{v}_1^i\| \leq \|\mathbf{v}_2^i\| \leq \ldots \leq \|\mathbf{v}_{m_i-n}^i\| \leq 48m_i \leq 96m',$$

with probability $1 - 2^{-\Omega(n)}$. It follows that we have $\sum_{i\in[t]}(m_i - n) = m - tn$ linearly independent vectors in $\Lambda^{\perp}(X)$ of the form:

$$\bar{\mathbf{v}}_j^i = [\mathbf{0}_{m_1+\cdots+m_{i-1}}\|\mathbf{v}_j^i\|\mathbf{0}_{m_{i+1}+\cdots+m_t}]^{\mathrm{t}},$$

for $j \in [m_i - n]$ and $i \in [t]$. Our goal is to have more ($m - n$, to be precise) short linearly independent vectors in $\Lambda^{\perp}(X)$.

Let $i \in [t]$. By Lemma 9, with probability greater than $1 - 2^{-n}$, there exists a matrix $U_i \in \mathbb{Z}^{m_i \times n}$ such that $X_i U_i = I_n$ with columns of norms $\leq 2\sqrt{44n\ln(ns)}$. When this event occurs, we have Let $i \in [t]$. By Lemma 9, with probability greater than $1 - 2^{-n}$, there exists a matrix $U_i \in \mathbb{Z}^{m_i \times n}$ such that $X_i U_i = I_n$ with columns of norms $\leq 2\sqrt{44n\ln(ns)}$. When this event occurs, we have

$$X_i \cdot [V_i|U_i] = [\mathbf{0}_{n\times(m_i-n)}|I_n],$$

where V_i is the $m_i \times (m_i - n)$ matrix whose columns are $\bar{\mathbf{v}}_1^i, \bar{\mathbf{v}}_2^i \cdots, \bar{\mathbf{v}}_{m_i-n}^i$.

With probability $\geq 1 - t2^{-n}$ (which is $\geq 1 - 2^{-\Omega(n)}$ by assumption on m), we can write:

$$\left[\, X_1 | X_2 | X_3 | \ldots | X_t \,\right] \cdot \left[\begin{array}{c|c|c|c|c|c|c|c|c} V_1 & \mathbf{0} & \mathbf{0} & \ldots & \mathbf{0} & U_1 & \mathbf{0} & \ldots & \mathbf{0} \\ \hline \mathbf{0} & V_2 & \mathbf{0} & \ldots & \mathbf{0} & -U_2 & U_2 & \ldots & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{0} & V_3 & \ldots & \mathbf{0} & \mathbf{0} & -U_3 & \ldots & \mathbf{0} \\ \hline \vdots & & & \ddots & & & & \ddots & \\ \hline \mathbf{0} & \mathbf{0} & \mathbf{0} & \ldots & V_t & \mathbf{0} & \mathbf{0} & \ldots & -U_t \\ \hline \end{array} \right] = \mathbf{0}_{m\times(m-n)}.$$

Now, we argue that the columns of the matrix built from the U_i's and V_i's are linearly independent. First, for each i, the columns of $[V_i|U_i]$ are linearly independent since they satisfy $X_i \cdot [V_i|U_i] = [\mathbf{0}_{m_1-n}|I_{m_1}]$, and since the columns of V_i are linearly independent. This implies that for every i, the "block row" $[\mathbf{0}|\ldots|\mathbf{0}|V_i|\mathbf{0}|\ldots|\mathbf{0}|-U_i|\ldots]$ has rank exactly m_i. If one re-orders the block columns appropriately, the matrix has a "block triangular" shape. Its rank is $m_1 + \ldots + m_{t-1} + m_t - n = m - n$.

Overall, we obtain $m - n$ linearly independent vectors in $\Lambda^{\perp}(X)$, with norms $\leq \mathcal{O}(n\ln(ns))$, with probability $\geq 1 - 2^{-\Omega(n)}$. □

Acknowledgments. This work has been supported by ERC Starting Grant ERC-2013-StG-335086-LATTAC and by the European Union PROMETHEUS project (Horizon 2020 Research and Innovation Program, grant 780701). Most of the work leading to this article was done while the first and last authors were at ENS de Lyon.

References

1. Divesh Aggarwal and Oded Regev. A note on discrete Gaussian combinations of lattice vectors. *Chic. J. Theoret. Comput. Sci.*, (7), June 2016.
2. Shweta Agrawal, Craig Gentry, Shai Halevi, and Amit Sahai. Discrete Gaussian leftover hash lemma over infinite domains. In *Advances in Cryptology - ASIACRYPT 2013*, pages 97–116, 2013.
3. Shweta Agrawal, Benoît Libert, and Damien Stehlé. Fully secure functional encryption for inner products, from standard assumptions. In *Advances in Cryptology - CRYPTO 2016*, pages 333–362, 2016.
4. Navid Alamati, Chris Peikert, and Noah Stephens-Davidowitz. New (and old) proof systems for lattice problems. In *Public-Key Cryptography - PKC 2018*, pages 619–643, 2018.
5. Wojciech Banaszczyk. New bounds in some transference theorems in the geometry of numbers. *Math. Ann.*, pages 625–636, 1993.
6. Jean-Claude Belfiore. Lattice codes for the compute-and-forward protocol: The flatness factor. *2011 IEEE Information Theory Workshop, ITW 2011*, 10 2011.
7. Jingwei Chen, Damien Stehlé, and Gilles Villard. A new view on HJLS and PSLQ: Sums and projections of lattices. In *Proceedings of the 38th International Symposium on Symbolic and Algebraic Computation*, pages 149–156, 2013.
8. John H. Conway and Neil J. A. Sloane. *Sphere packings, lattices, and groups.* Third edition, Springer-Verlag, 1993.
9. Daniel Dadush, Oded Regev, and Noah Stephens-Davidowitz. On the closest vector problem with a distance guarantee. In *Proceedings of the 2014 IEEE 29th Conference on Computational Complexity*, pages 98–109, 2014.
10. Marten van Dijk, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan. Fully homomorphic encryption over the integers. In *Advances in Cryptology — EUROCRYPT 2010*, pages 24–43, 2010.
11. Sanjam Garg, Craig Gentry, and Shai Halevi. Candidate multilinear maps from ideal lattices. In *Advances in Cryptology – EUROCRYPT 2013*, pages 1–17, 2013.
12. Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the 14th Annual ACM Symposium on Theory of Computing*, pages 197–206, 2008.
13. George Havas, Bohdan S. Majewski, and Keith R. Matthews. Extended GCD and Hermite normal form algorithms via lattice basis reduction. *Exp. Math.*, 7(2):125–136, 1998.
14. D.R. Heath-Brown. The number of primes in a short interval. *J. Reine Angew. Math.*, 389:22–63, 1988.
15. Russell Impagliazzo, Leonid A. Levin, and Michael Luby. Pseudo-random generation from one-way functions. In *Proceedings of the 21st Annual ACM Symposium on Theory of Computing*, pages 12–24. ACM, 1989.
16. Arjen K. Lenstra, Hendrik W. Lenstra, and László Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261:515–534, 1982.
17. San Ling, Duong Hieu Phan, Damien Stehlé, and Ron Steinfeld. Hardness of k-LWE and applications in traitor tracing. *Algorithmica*, pages 1318–1352, 2017.
18. Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on Gaussian measures. 37(1):267–302, 2007. Preliminary version in FOCS 2004.
19. Phong Nguyen. *La géométrie des nombres en cryptologie.* PhD thesis, Université Paris 7, 1999.
20. Phong Nguyen and Jacques Stern. Merkle-Hellman revisited: A cryptanalysis of the Qu-Vanstone cryptosystem based on group factorizations. In *Advances in Cryptology – CRYPTO 1997*, pages 198–212, 1997.
21. Phong Nguyen and Jacques Stern. The hardness of the hidden subset sum problem and its cryptographic implications. In *Advances in Cryptology – CRYPTO 1999*, pages 31–46, 1999.
22. Phong Nguyen and Brigitte Vallée. *The LLL Algorithm: Survey and Applications.* Springer, 1st edition, 2009.
23. Chris Peikert. Limits on the hardness of lattice problems in ℓ_p norms. *Computational Complexity*, 17(2):300–351, 2008.
24. Chris Peikert, Oded Regev, and Noah Stephens-Davidowitz. Pseudorandomness of ring-LWE for any ring and modulus. In *Proceedings of the 49th Annual ACM Symposium on Theory of Computing*, pages 461–473. ACM, 2017.