GAUSSIAN LEFTOVER HASH LEMMA OVER LATTICES

Thanh Huyen NGUYEN

Supervisors 1. Prof. Damien STEHLÉ
2. Elena KIRSHANOVA
3. Alexandre WALLET

École normale supérieure de Lyon

June 2018

1 Introduction

Lattice-based cryptography. Lattice-based cryptography began with the seminal work of Ajtai in [Ajt96]. There have been a number of proposals of cryptographic schemes with security provably relying on hard computational problems over high-dimensional Euclidean lattices. Indeed, these problems are expected to be exponentially hard to solve (in the dimension of the lattice), even with quantum computers. For example, The Shortest Vector Problem in l_2 is NP-hard for randomized reduction [Ajt98].

Many lattice-based schemes require sampling from discrete Gaussian distribution. It has been used extensively in all aspects of lattice-based cryptography, for example: hardness results [Reg09], constructive aspects [GPV08], etc. Moreover, D. Micciancio and O. Regev show in [MR07] that Gaussian distributions shares many of the nice properties with its continuous counterpart, and demonstrate their usefulness for lattice-based cryptography.

Leftover Hash Lemma. Whenever one deals with randomness, the Leftover Hash Lemma (LHL) is a very powerful tool. Its most simple application is the following: consider n uniform random a_i's from $\mathbb{Z}_q$, then take a short random linear combination of these elements mod q. Then the LHL states that the resulting $(n+1)$-tuple is "essentially" a uniform random $(n+1)$-tuple in $\mathbb{Z}_q$ even given $a_1, a_2, \ldots, a_n$. Such a result enables us to argue about indistinguishability of public keys from uniform elements. In [Reg05], Regev uses LHL over $\mathbb{Z}_q$, to show that $\sum s_i a_i$ gives a uniform public key, where s_i's $\in \mathbb{Z}_q$ are the secret key.

More general, LHL leads to simple and efficient randomness extractors, and can be used in many applications requiring good randomness. It therefore finds numerous applications in cryptography: key derivation, random number generators. More formally, the LHL guarantees similarities between two distributions. This is formalized by the notion of statistical distance: $\Delta(D_1; D_2) = \frac{1}{2} \sum_{\mathbf{x} \in \Omega} |D_1[\mathbf{x}] - D_2[\mathbf{x}]|$, where Ω is the common support of D_1 and D_2. When $\Delta(D_1; D_2)$ is small, the two distributions D_1, D_2 are essentially the same.

The classical statement of the LHL relates a fixed uniform distribution (say, D_1) over a **finite** support to another distribution that comes from a specific cryptographic construction. However, for some lattice-based primitives, we cannot use the LHL directly. Indeed, for lattice-based constructions, the application of the LHL is limited for two reasons. The main reason is that we care about distributions whose support is an Euclidean lattice, which is an **infinite** domain. More to that, a popular choice of a distribution to consider is a Discrete Gaussian distribution, instead of uniform one (which does not exist over infinite domain). Hence, it is needed to extend the LHL to such a setting. This is the purpose of this work. We would like to emphasise that having a tight bound on minima of a random lattice is an interesting mathematical question on its own.

Another application of LHL is an extremely simple discrete Gaussian sampler. Specifically, consider the following sampler. In an offline phase, for $m > n$, we sample a set of short vectors $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_m$ from a lattice L. Then, in the online phase, the sample generates $\mathbf{z} \in \mathbb{Z}^m$ according to a discrete Gaussian and simply outputs $\sum_{i=1}^{m} z_i \mathbf{x}_i$. With a variant of the LHL presented in this work, we can argue that the output is statistically close to Gaussian.

Now, we begin by defining some notations necessary to present previous works and our main result.

Lattices and Gaussian Distributions over Lattices.

Lattices. A lattice is a discrete additive subgroup of $\mathbb{R}^m$. A set of linearly independent vectors that generates a lattice is called a basis. It is denoted by $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \subset \mathbb{R}^m$ for integers $m \geq n \geq 1$. The lattice generated by the basis $\mathbf{B}$ (meaning the columns of $\mathbf{B}$), is

$$L = L(\mathbf{B}) := \{\mathbf{Bz} = \sum_{i=1}^{n} z_i \mathbf{b}_i : \mathbf{z} \in \mathbb{Z}^n\}.$$

We say that the rank of this lattice is n and its dimension is m. If $n = m$, the lattice is called a full-rank lattice. For $i = 1, \ldots, n$, the successive minimum $\lambda_i(L)$ is defined as the smallest value such that a ball of radius $\lambda_i(L)$ centered around the origin contains at least i linearly independent lattice vectors.

Dual Lattices. For a lattice $L \subset \mathbb{R}^n$, its dual lattice consists of all the points in $\text{span}(L)$ that are orthogonal to L modulo 1, namely:

$$L^* := \{\mathbf{y} \in \text{ span}(L) : \forall \mathbf{x} \in L, \langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}\}.$$

Gaussian function. For any real $s > 0$, and vector $\mathbf{c} \in \mathbb{R}^n$, the (spherical) Gaussian function on $\mathbb{R}^n$ centered at $\mathbf{c}$ with parameter s is defined as $\rho_{s,\mathbf{c}}(\mathbf{x}) = \exp(-\pi||\mathbf{x}-\mathbf{c}||^2/s^2)$ for all $x \in \mathbb{R}^n$. If $s = 1$, the subscript is omitted. For a rank-n matrix $S \in \mathbb{R}^{m \times n}$, the ellipsoidal Gaussian function on $\mathbb{R}^n$ centered at $\mathbf{c}$ with covariance matrix $\Sigma = S^T S$ is defined as:

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

When $S = sI_n, \rho_S$ is denoted ρ_s.

Discrete Gaussian distributions. For a rank-n lattice $L, S \in \mathbb{R}^{m \times n}$, and $\mathbf{c} \in \mathbb{R}^n$, the ellipsoidal Gaussian distribution with parameter S and support L 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 $\rho_{S,\mathbf{c}}(L) = \sum_{\mathbf{x} \in L} \rho_{S,\mathbf{c}}(\mathbf{x})$.

The same definition applies to the spherical case, which is denoted by $\mathcal{D}_{L,s,\mathbf{c}}(\cdot)$ (with lowercase s). When $\mathbf{c} = \mathbf{0}$ we use the shorthand $\mathcal{D}_{L,S}$ (or $\mathcal{D}_{L,s}$).

Previous work. In [AGHS13], the authors analyze the following distribution. Let $\mathbf{x}_1, ..., \mathbf{x}_m$ be m fixed points in $\mathbb{Z}^n$ for some $m > n$. Let X be the $n \times m$ matrix formed by the vectors $\mathbf{x}_1, ..., \mathbf{x}_m$ as the column vectors. For $s' > 0$, define the distribution

$$\mathcal{E}_{X,s'} = \{X \cdot \mathbf{z} : \mathbf{z} \leftarrow D_{\mathbb{Z}^m,s'}\}.$$

The main result of [AGHS13] is the following: If X satisfies a certain constraint and if s' is large enough, then the distribution $\mathcal{E}_{X,s'}$ is statistically close to the discrete Gaussian distribution with appropriate covariance.

Lemma 1 ([AGHS13], Theorem 2)**.** *For integer $n \geq 1$, let $X \leftarrow (D_{\mathbb{Z}^n,s})^m$ with the parameters m, s chosen appropriately. If $s' \geq 4mn \ln(\frac{1}{\varepsilon})$, then $\Delta(\mathcal{E}_{X,s'}, D_{\mathbb{Z}^m,s'X^T}) \leq 2\varepsilon$.*

This result shows that for the appropriate choice of m, s, s', one can obtain a discrete Gaussian version of the LHL over lattices.

In [AR16], D. Aggarwal and O. Regev improve over the main result of [AGHS13] for some parameter sets. In both of the results, the bound on s' comes from the so-called smoothing parameter of $\Lambda^{\perp}(X)$ (the smoothing parameter is the smallest t such that a Gaussian measure on the dual lattice with parameter $\frac{1}{t}$ gives all but a negligible amount of its weight to the origin, for some negligible function of the lattice dimension, see Definition 5). Here $\Lambda^{\perp}(X)$ is a rank-$(m-n)$ lattice in $\mathbb{Z}^m$, orthogonal to all the rows of X. The main theorem says that if s' bigger than the smoothing parameter of $\Lambda^{\perp}(X)$, then the distance of the two distributions $\mathcal{E}_{X,s'}$ and Gaussian over $\mathbb{Z}^m$ is very close. In order to find a lower bound on s', we need to find an upper bound on the smoothing parameter of $\Lambda^{\perp}(X)$. In [AGHS13], the authors proceed by first embedding $\Lambda^{\perp}(X)$ into a full-rank lattice $\Lambda_q^{\perp}(X)$, where q is an integer whose size will be discussed later, and then move to study $\Lambda_q(X)$, the (scaled) dual of $\Lambda_q^{\perp}(X)$. The above can be depicted by the following graph:

$$\Lambda^{\perp}(X) \subseteq \Lambda_q^{\perp}(X) \xrightarrow{\text{dual}} \frac{1}{q}\Lambda_q(X)$$

$$\lambda_{m-n}\Lambda^{\perp}(X)) \leq \lambda_{m-n}(\Lambda_q^{\perp}(X)) \overset{\text{transference}}{\sim} \lambda_{n+1}(\Lambda_q(X)).$$

The main technical challenge of the proof is obtaining a lower bound on $\lambda_{n+1}(\Lambda_q(X))$. Once this is done, we can deduce an upper bound on $\eta_{\varepsilon}(\Lambda^{\perp}(X))$ by combining 1) Banasczcyk's transference theorem, and 2) a known relationship between $\lambda_{m-n}(\Lambda^{\perp}(X))$ and the smoothing parameter of $\Lambda^{\perp}(X)$ using a lemma by D. Micciancio and O. Regev in [MR07].

In [AR16], a more direct method to bound $\lambda_{m-n}(\Lambda^{\perp}(X))$ is used. The approach the authors take is using a simple, yet powerful, idea from a result by Kuperberg, Lovett, and Peled in [KLP12]. Using this idea, Aggarwal and Regev get that in order to prove a bound on the successive minimum of the orthogonal lattice, it suffices to bound the two quantities: 1) entries of X, and 2) length of vectors $\mathbf{u}_1, ..., \mathbf{u}_n$ such that $X \cdot \mathbf{u}_i = \mathbf{e}_i$ where $\mathbf{e}_i$ are unit vectors of dimension n.

Lemma 2 ([AR16], Theorem 5.1)**.** *For integer $n \geq 1$, let $X \leftarrow (D_{\mathbb{Z}^n,s})^m$ with the parameters m, s appropriately. If $s' \geq 10ns \log m \sqrt{\log(\frac{1}{\varepsilon}) \log(ns)}$, then $\Delta(\mathcal{E}_{X,s'}, D_{\mathbb{Z}^m,s'X^T}) \leq$*

2ε.

Now, we compare the parameter sets from the reference articles.

[AGHS13]	[AR16]
$s = \Omega(\log(n/\varepsilon)))$	$s = \Omega(\log(n/\varepsilon)))$
$m = \Omega(n \log(ns))$	$m = \Omega(n \log(ns))$
$s' = \Omega(mn \ln(\frac{1}{\varepsilon}))$	$s' = \Omega(sn\sqrt{(\log m)(\log ns)(\log \frac{m-n}{\varepsilon})})$

The main difference between two results is in the bound on s'. Namely, the bound on s' obtained by [AGHS13] depends linearly on m. Improving this dependence is an open question, which D.Aggarwal and O. Regev addressed in [AR16]. Their bound on s' is $\Omega(ns\sqrt{\log(\frac{1}{\varepsilon})})$. It depends linearly on s. Therefore the result of [AGHS13] is worse than that of [AR16] for large values of m. However, when s is sufficiently large, the bound on s' obtained by [AGHS13] is better than the bound in [AR16].

Our result. In this note, we improve on the main result of [AGHS13] and [AR16]. Specifically, we remove the dependency on m and s from the bound on s'. Informally, our result is the following:

Theorem 3. (Informal) *Let $n \geq 1, m = poly(n), s = \Omega(\log(n/\varepsilon))$. Then except with probability $2^{-n(1-O(1))}$, we have*

$$\eta_\varepsilon(\Lambda^\perp(X)) \leq s' = \Omega\left(n \log(ns)\sqrt{\ln\left(\frac{1}{\varepsilon}\right)}\right).$$

The formal statement and proof appear as Corollary 24 in Section 3. Using this result, we can state a LHL over lattices with tighter parameters.

Theorem 4. (Informal) *Let $n \geq 1, m = poly(n), s = \Omega(\log(n/\varepsilon))$, and $X \leftarrow (D_{\mathbb{Z}^n,s})^m$. Then except with probability $2^{-n(1-O(1))}$, with $s' = \Omega(n \log(ns)\sqrt{\ln(1/\varepsilon)})$, we have*

$$\Delta(\mathcal{E}_{X,s'}, D_{\mathbb{Z}^m,s'X^T}) \leq 2\varepsilon.$$

The formal statement and proof appear as Theorem 25 in Section 3.

Our Techniques. The goal of our work is to bound the smoothing parameter of $\Lambda^{\perp}(X)$. We use the same idea as in [AGHS13]. First, we give a lower bound on the $(n+1)$-th minimum of the lattice $\Lambda_q(X)$. Our result in Theorem 20 Then, using the so-called Banasczcyk's transference theorem (Theorem 9), we give an upper bound on $\lambda_{m-n}(\Lambda^{\perp}(X))$, which again improves over the bound in [AGHS13] by a factor of n. More precisely, in Corollary 23, the bound on $\lambda_{m-n}(\Lambda^{\perp}(X))$ we obtain is roughly $\Omega(m)$. We can improve it further. In particular, we remove the dependency on m from the upper bound on $\lambda_{m-n}(\Lambda^{\perp}(X))$ in Corollary 24 by combining 1) our new bound from Corollary 23, and 2) Lemma 16 in [AR16]. Once this is done, we can deduce an upper bound on $\eta_{\varepsilon}(\Lambda^{\perp}(X))$ form $\lambda_{m-n}(\Lambda^{\perp}(X))$ by using a lemma from [MR07].

2 Preliminaries

All logarithms, unless otherwise stated, are to the base 2. Natural logarithms, i.e., to the base e, are denoted by ln. The norm $||\cdot||$ considered in this paper is the l_2 norm, unless otherwise stated. We use bold letters to denote vectors, capital letters to denote matrix. The transpose and inverse of a matrix X are denoted as X^T and X^{-1}, respectively.

First, we give all the necessary definitions and lemmas.

Definition 5. *Given $\varepsilon > 0$, the smoothing parameter $\eta_{\varepsilon}(L)$ is smallest real $s > 0$ such that*

$$\min\{s : \rho_{1/s}(L^* \setminus \{0\}) < \varepsilon\},$$

where $\rho_{\frac{1}{s}}(A)$ for a set A is $\sum_{\mathbf{x}\in A} \rho_{\frac{1}{s}}(\mathbf{x})$.

Definition 6. *Let $\Lambda^{\perp}(X)$ be a rank-$(m-n)$ lattice in $\mathbb{Z}^m$ orthogonal to all the rows of X, namely*

$$\Lambda^{\perp}(X) := \{\boldsymbol{v} \in \mathbb{Z}^m : X\boldsymbol{v} = \mathbf{0}\}.$$

Definition 7. *For $q \geq 2$, we let $\Lambda_q(X)$ be the full-rank lattice spanned by the rows of X and the vectors $q\mathbf{e}_i$, i.e.,*

$$\Lambda_q(X) := \{X^T\mathbf{z} + q\mathbf{y} : \mathbf{z} \in \mathbb{Z}^n, \mathbf{y} \in \mathbb{Z}^m\}.$$

Definition 8. *For $q \geq 2$, we let $\Lambda_q^{\perp}(X)$ be the dual of $\Lambda_q(X)$, scaled up by a factor of q, i.e.,*

$$\Lambda_q^{\perp}(X) := \{\mathbf{v} \in \mathbb{R}^m : \forall\, \mathbf{u} \in \Lambda_q(X), \langle \mathbf{v}, \mathbf{u} \rangle \in q\mathbb{Z}\}.$$

Here, we recall some theorems and lemmas needed throughout the note.

Theorem 9 ([Ban93])**.** *For any rank-n lattice $L \subseteq \mathbb{R}^m$, and for all $i \in [n]$,*

$$1 \leq \lambda_i(L) \cdot \lambda_{n+1-i}(L^*) \leq n,$$

where L^* is the dual lattice of L.

Lemma 10 ([MR07], Lemma 3.3)**.** *For any rank-n lattice L, and positive real $\varepsilon > 0$,*

$$\eta_\varepsilon(L) \leq \lambda_n(L) \cdot \sqrt{\frac{\ln(2n(1+\frac{1}{\varepsilon}))}{\pi}}.$$

We also need the following results related to Gaussian distributions.

Lemma 11 ([DRS14], Lemma 2.13)**.** *For any rank-n lattice L, $\varepsilon \in (0,1)$, $s \geq \eta_\varepsilon(L)$, and any $t \geq 1$, we have*

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

Lemma 12 ([AGHS13], Lemma 4)**.** *For any rank-n lattice L, any $\varepsilon \in (0,1)$, $\mathbf{c} \in \mathbb{R}^n$. If $s \geq \eta_\varepsilon(L)$, we have*

$$\rho_{s,\mathbf{c}}(L) \in [\frac{1+\varepsilon}{1-\varepsilon}, 1] \cdot \rho_s(L).$$

Lemma 13 ([Lyu12], Lemma 4.4.3)**.** *For any $k > 1$, we have*

$$\Pr\left[||\mathbf{v}|| > ks\sqrt{n}, \mathbf{v} \leftarrow D_{\mathbb{Z}^n,s}\right] < k^n \cdot \exp\left(\frac{n}{2}(1-k^2)\right).$$

Lemma 14 ([Lyu12], Lemma 4.3)**.** *For any $\mathbf{z} \in \mathbb{Z}^n$ and any $s, r > 0$, we have*

$$\Pr\left[|\langle \mathbf{v}, \mathbf{z} \rangle| > r : \mathbf{v} \leftarrow D_{\mathbb{Z}^n,s}\right] \leq 2\exp\left(-\frac{r^2}{2||\mathbf{z}||^2 s^2}\right).$$

Lemma 15 ([AGHS13], Lemma 6)**.** *Fix a lattice $L \subseteq \mathbb{R}^n$, $\varepsilon \in (0,1)$, $c > 2$, $s \geq (1+c)\eta_\varepsilon(L)$. Then for any subset $T \subseteq L$ and for all $\mathbf{v} \in L$, 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.

Lemma 16 ([AR16], Adapted from Lemma 4.2)**.** *Let $n \geq 100$ be an integer, and let $\varepsilon = \varepsilon(n) \in (0, 1/1000)$. Let s, m be parameters such that $s \geq 9\eta_\varepsilon(\mathbb{Z}^n)$, $m > 30n\log(sn)$, we have*

$$\Pr_{X \leftarrow (D_{\mathbb{Z}^n,s})^m}\left[\exists\ U \in \mathbb{Z}^{m\times n} : XU = I_n \text{ and } \max||\mathbf{u}_i|| \leq 2\sqrt{30n\log(sn)}\right] \geq 1 - 2^{-n},$$

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

Lemma 17 (Hoeffding's inequality)**.** *Let $X_1, ..., X_m$ 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*

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

The next lemma is due to Agrawal et al [AGHS13]. In particular, it gives lower-bounds on the parameters s and m. It shows that the columns of $X \in \mathbb{Z}^{m\times n}$ chosen from Gaussian distribution span all of $\mathbb{Z}^n$ with overwhelming probability. This means also that the support of $\mathcal{E}_{X,s'}$ includes all of $\mathbb{Z}^n$. The proof considers choosing the columns one by one. One shows that a) as long as the current columns only $\mathbb{R}$-span a subspace of $\mathbb{R}^n$, then it is likely that the next row falls outside that subspace, and b) once the current matrix has full rank, as long as the current columns only $\mathbb{Z}$-span a sub-lattice of $\mathbb{Z}^n$, it is likely that the next one falls outside that sub-lattice. The formal proof can be found in [AGHS13].

Lemma 18 ([AGHS13], Lemma 9)**.** *For $\varepsilon \in (0, 1/1000)$, $s \geq 10\eta_\varepsilon(\mathbb{Z}^n)$, $m \geq 10n\log(s\sqrt{n})$, we have*

$$\Pr_{X \leftarrow (D_{\mathbb{Z}^n,s})^m}[X \cdot \mathbb{Z}^m = \mathbb{Z}^n] \geq 1 - 2^{-\Theta(m)}.$$

The next lemma is also due to [AGHS13]. It shows that when we have an estimate on the smoothing parameter $\eta_\varepsilon(\Lambda^\perp(X))$, we can choose a standard deviation s' such that the statistical distribution between $\mathcal{E}_{X,s'} = \{X \cdot \mathbf{z} : \mathbf{z} \leftarrow D_{\mathbb{Z}^m,s'}\}$ and the Gaussian over $\mathbb{Z}^m$ is small.

Lemma 19 ([AGHS13], Lemma 10)**.** *For any $m > n \geq 1$ and $0 < \varepsilon < \frac{1}{3}$. 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*

$$\Delta(\mathcal{E}_{X,s'}, D_{\mathbb{Z}^m,s'X^T}) \leq 2\varepsilon.$$

3 Main Theorem

In this work, the next theorem gives a probabilistic lower bound on the $(n+1)$-th minimum of the lattice $\Lambda_q(X)$. Our result improves the bound of [AGHS13] by the factor of n. The improvement stems from a tighter analysis, in particular 1) we avoid relying on Euclidean/ infinity norm equivalence, and 2) we refine the counting argument for $\mathbf{z}$ by using Hoeffding's inequality. We warn the reader that the original proof in [AGHS13] contained two minor errors. We highlight the exact place of the flaws later in the proof.

The proof works as follows. First, we show that all the rows of X belong to $\Lambda_q(X)$, and that w.h.p. they are linearly independent and relatively short. This already gives us an estimation on the first n minima of $\Lambda_q(X)$. It remains to prove that w.h.p over the choice of X, every vector in $\Lambda_q(X)$, which is not in the linear span of the rows of X, is of size essentially q. This means, we draw our attention to the vectors of the form $[X^T\mathbf{z}]_q \in \Lambda_q(X) \setminus X^T\mathbb{Z}^n$. To upper bound the norm of such vector, we divided the proof into two cases depending on the length of $\mathbf{z}$. This part in our proof is more subtle that in [AGHS13], as we bypass the norm equivalence. For"small" $\mathbf{z}$, we get that with all but probability $2^{-\Omega(n)}$, the vectors $[X^T\mathbf{z}]_q$ belong to the row space of X. For the other ranges of $\mathbf{z}$, we obtain a probabilistic upper bound on the entries of $[X^T\mathbf{z}]_q$.

Theorem 20. *For $\varepsilon \in (0, 1/1000)$, $s \geq 101\eta_\varepsilon(\mathbb{Z}^n)$, $n > 100$, $m \geq 100n \log q$, and $q > 24s\sqrt{3m}$, we have*

$$\Pr_{X \leftarrow (D_{\mathbb{Z}^n,s})^m}\left[\lambda_{n+1}(\Lambda_q(X)) < \frac{q}{24}\right] < 2^{-\Omega(n)}.$$

Proof. We see that all the rows of X belong to $\Lambda_q(X)$. From Lemma 18 they are linearly independent with all but probability $2^{-\Theta(m)}$. Moreover, Lemma 13 with $k = \sqrt{3}$, implies that with all but probability $\sqrt{3}^m \cdot \exp(-m) < 2^{-\frac{m}{2}}$ the rows of X are smaller than $s\sqrt{3m} < \frac{q}{24}$. It follows that $\Lambda_q(X)$ has n linearly independent short non-zero vectors with probability greater than $1 - 2^{-\Theta(m)}$.

Below, we show that if $\mathbf{v} \in \Lambda_q(X) \setminus X^T\mathbb{Z}^n$, then $||\mathbf{v}|| \geq \frac{q}{24}$ with overwhelming probability. Recall that every vector in $\Lambda_q(X)$ is of the form $X^T\mathbf{z} + q\mathbf{y}$ for some $\mathbf{z} \in \mathbb{Z}^n$ such that $||\mathbf{z}||_\infty \leq \frac{q}{2}$ (i.e., an integer vector with entries in $[\frac{-q}{2}, \frac{q}{2})$) and $\mathbf{y} \in \mathbb{Z}^m$. Thus

it suffices to show that every vector of the form $[X^T\mathbf{z}]_q \in \Lambda_q(X) \setminus X^T\mathbb{Z}^n$ has Euclidean norm at least $\frac{q}{24}$. Let us fix such a $\mathbf{z} \in \mathbb{Z}^n$ with $||\mathbf{z}||_\infty \leq \frac{q}{2}$. We consider two cases depending on the l_2 norm of $\mathbf{z}$.

Case 1: "Small" $\mathbf{z}$, i.e., $||\mathbf{z}|| < \frac{q}{2s\sqrt{n \log q}}$.

In this case, the following claim shows that the vectors $[X^T\mathbf{z}]_q$ belong to the row space of X with hight probability.

Claim 21. *Let $\mathbf{z} \in \mathbb{Z}^n$ with $||\mathbf{z}||_\infty \leq \frac{q}{2}$ and $||\mathbf{z}|| < \frac{q}{2s\sqrt{n \log q}}$, then we have*

$$\Pr_{X \leftarrow (D_{\mathbb{Z}^n,s})^m} \left[\exists\, \mathbf{z} \in \mathbb{Z}_q^n : [X^T\mathbf{z}]_q \in \Lambda_q(X) \setminus X^T\mathbb{Z}^n\right] \leq 2^{-\Omega(n)}.$$

Proof. We have that $\mathbf{x}_i$ is distributed as $D_{\mathbb{Z}^n,s}$ with $s > \eta_\varepsilon(\mathbb{Z}^n)$ for all $i \in [n]$. By Lemma 11 with $t = \sqrt{2\pi \log q}$, we have $||\mathbf{x}_i|| \leq s\sqrt{n \log q}$ except with probability q^{-n}.[1] When this happens, we have

$$|\langle \mathbf{z}, \mathbf{x}_i \rangle| \leq ||\mathbf{z}|| \cdot ||\mathbf{x}_i|| < \frac{q}{2s\sqrt{n \log q}} \cdot s\sqrt{n \log q} = \frac{q}{2}.$$

The union bound implies that $\Pr_X \left[||X^T\mathbf{z}||_\infty < \frac{q}{2}\right] > 1 - mq^{-n}$, so $[X^T\mathbf{z}]_q = X^T\mathbf{z}$ belongs to the row space of X with probability at least $1 - mq^{-n}$. Using the union bound, we get

$$\Pr_X \left[\exists\, \mathbf{z} \in \mathbb{Z}_q^n : ||\mathbf{z}|| < \frac{q}{2s\sqrt{n \log q}} \text{ and } [X^T\mathbf{z}]_q \in \Lambda_q(X) \setminus X^T\mathbb{Z}^n\right] \leq 2^{-\Omega(n)}.$$

□

Case 2: The other ranges of $\mathbf{z}$, i.e., $||\mathbf{z}|| \leq \frac{q}{2s\sqrt{n \log q}}$.

This case is handled by the next claim.

Claim 22. *Let $\mathbf{z} \in \mathbb{Z}^n$ with $||\mathbf{z}||_\infty \leq \frac{q}{2}$ and $||\mathbf{z}|| \leq \frac{q}{2s\sqrt{n \log q}}$, then we have*

$$\Pr_{\mathbf{x} \leftarrow D_{\mathbb{Z}^n,s}} \left[|[\langle \mathbf{x}, \mathbf{z} \rangle]_q| < \frac{q}{24\sqrt{n \log q}}\right] \leq 0.91.$$

[1] We note that this step was incorrect in [AGHS13],the suggested s could not enable a small enough probability vie Gaussian Tail Bound.

Proof. We have two subcases.

Subcase 2.1: "Medium" $\mathbf{z}$, i.e., $\frac{q}{2s\sqrt{n\log q}} \leq ||\mathbf{z}|| < \frac{q}{2s}$.

Define the set of "Bad" vectors as

$$\text{Bad} := \left\{ \mathbf{x} \in \mathbb{Z}^n : |[\langle \mathbf{z}, \mathbf{x} \rangle]_q| < \frac{q}{24\sqrt{n\log q}} \right\}.$$

Vectors outside this set will be called "Good" vectors. We let $\mu = \left\lceil \frac{s}{6\sqrt{n}} \right\rceil$. If $\mathbf{x} \in \text{Bad}$, then we can obtain a "Good" vector using the injective map

$$\begin{aligned} \text{Bad} &\to \text{Good} \\ \mathbf{x} &\mapsto \mathbf{x} + \mu \left\lceil \frac{2\mathbf{z}\sqrt{n}}{||\mathbf{z}||} \right\rceil. \end{aligned}$$

By the choice of μ and the fact that $0 \leq \left\langle \mathbf{z}_i, \left\lceil \frac{2\mathbf{z}_i\sqrt{n}}{||\mathbf{z}||} \right\rceil \right\rangle$, we have

$$\begin{aligned} 0 \leq \mu \left\langle \mathbf{z}, \left\lceil \frac{2\mathbf{z}\sqrt{n}}{||\mathbf{z}||} \right\rceil \right\rangle &\leq \mu \cdot \left(\sum_{i=1}^{n} \left(|\mathbf{z}_i| \cdot \frac{2|\mathbf{z}_i|\sqrt{n}}{||\mathbf{z}||} + |\mathbf{z}_i| \right) \right) \\ &\leq 2\frac{s}{6\sqrt{n}}(2||\mathbf{z}||\sqrt{n} + ||\mathbf{z}||\sqrt{n}) \\ &\leq \frac{q}{2}. \end{aligned}$$

To obtain the last inequality, we used that $||\mathbf{z}|| < \frac{q}{2s}$ and $6\sqrt{n} \leq s$. Combining the general fact that $|[a+b]_q| \geq |[a]_q| - |[b]_q|$ with the above inequality, we obtain

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

Now, we show that the map indeed sends a "Bad" vector to a "Good" vector. Since $||\mathbf{z}|| \geq \frac{q}{2s\sqrt{n\log q}}$ and $|[\langle \mathbf{z}, \mathbf{x} \rangle]_q| \leq \frac{q}{24\sqrt{n\log q}}$, we have

$$\begin{aligned} \mu \left\langle \mathbf{z}, \left\lceil \frac{2\mathbf{z}\sqrt{n}}{||\mathbf{z}||} \right\rceil \right\rangle - |[\langle \mathbf{z}, \mathbf{x} \rangle]_q| &\geq \mu \left(\sum \left(|\mathbf{z}_i| \cdot \frac{2|\mathbf{z}_i|\sqrt{n}}{||\mathbf{z}||} - |\mathbf{z}_i| \right) \right) - \frac{q}{24\sqrt{n\log q}} \\ &\geq \frac{s}{6\sqrt{n}}(2||\mathbf{z}||\sqrt{n} - ||\mathbf{z}||\sqrt{n}) - \frac{q}{24\sqrt{n\log q}} \\ &\geq \frac{q}{12\sqrt{n\log q}} - \frac{q}{24\sqrt{n\log q}} = \frac{q}{24\sqrt{n\log q}}. \end{aligned}$$

This implies that $\mathbf{x} + \mu \left\lceil \frac{2\mathbf{z}\sqrt{n}}{||\mathbf{z}||} \right\rceil$ is a Good vector. We apply Lemma 15 with parameters $L = \mathbb{Z}^n$, $\varepsilon \in (0, 1/1000)$, $s > 101\eta_\varepsilon(\mathbb{Z}^n)$, $||\mathbf{v}|| = \left|\left| \mu \left\lceil \frac{2\mathbf{z}\sqrt{n}}{||\mathbf{z}||} \right\rceil \right|\right| \leq s$ and $p = \frac{||\mathbf{v}||\sqrt{\pi}}{s} \leq \sqrt{\pi}$. We obtain

$$\Pr_{\mathbf{x}}[\mathbf{x} \in \text{Bad}] - \Pr_{\mathbf{x}}[\mathbf{x} \in \text{Good}] \leq \frac{\text{erf}(p(1+\frac{4}{c})/2)}{\text{erf}(2p)} \cdot \frac{1+\varepsilon}{1-\varepsilon} \leq 0.81.$$

As we also have $\Pr_{\mathbf{x}}[\mathbf{x} \in \text{Bad}] + \Pr_{\mathbf{x}}[\mathbf{x} \in \text{Good}] \leq 1$, we obtain $\Pr_{\mathbf{x}}[\mathbf{x} \in \text{Bad}] \leq \frac{1+0.81}{2}$. We conclude that $\Pr_{\mathbf{x}}\left[|[\langle \mathbf{x}, \mathbf{z} \rangle]_q| < \frac{q}{24\sqrt{n \log q}}\right] \leq 0.91$.

Subcase 2.2: "Large" $\mathbf{z}$, i.e., $||\mathbf{z}|| \geq \frac{q}{2s}$, which implies $||\mathbf{z}||_\infty \geq \frac{q}{2s\sqrt{n}}$.

We modify the mapping[2] from Bad to Good vectors by defining $\mu := \min\left\{ \lceil s \rceil , \left\lfloor \frac{q}{2||\mathbf{z}||_\infty} \right\rfloor \right\}$, and consider

$$\text{Bad} \rightarrow \text{Good}$$

$$\mathbf{x} \mapsto \mathbf{x} + \mu \mathbf{e}_{i_{max}},$$

where i_{max} is the index of a largest entry in $\mathbf{z}$ (in absolute value). We have $\mu||\mathbf{z}||_\infty \leq \frac{q}{2||\mathbf{z}||_\infty}||\mathbf{z}||_\infty = \frac{q}{2}$. Therefore, it holds that $|[\langle \mathbf{z}, \mathbf{x} + \mu \mathbf{e}_{i_{max}} \rangle]_q| = |[\langle \mathbf{z}, \mathbf{x} \rangle + \mu||\mathbf{z}||_\infty]_q| \geq \mu||\mathbf{z}||_\infty - |[\langle \mathbf{z}, \mathbf{x} \rangle]_q|$.

Assume, $\mu = \lceil s \rceil$. Using that $||\mathbf{z}||_\infty > \frac{q}{2s\sqrt{n}}$ and $|[\langle \mathbf{z}, \mathbf{x} \rangle]_q| < \frac{q}{24\sqrt{n \log q}}$, we obtain

$$\mu||\mathbf{z}||_\infty - |[\langle \mathbf{z}, \mathbf{x} \rangle]_q| > s\frac{q}{2s\sqrt{n}} - \frac{q}{24\sqrt{n \log q}} > \frac{q}{24\sqrt{n \log q}}.$$

Assume now, $\mu = \left\lfloor \frac{q}{2||\mathbf{z}||_\infty} \right\rfloor$. This implies

$$\mu||\mathbf{z}||_\infty - |[\langle \mathbf{z}, \mathbf{x} \rangle]_q| > \frac{q}{3||\mathbf{z}||_\infty} \cdot ||\mathbf{z}||_\infty - \frac{q}{24\sqrt{n \log q}} > \frac{q}{24\sqrt{n \log q}}.$$

In both cases, we have $|[\langle \mathbf{z}, \mathbf{x} + \mu \mathbf{e}_{i_{max}} \rangle]_q| > \frac{q}{24\sqrt{n \log q}}$. We apply Lemma 15 with parameters $||\mathbf{v}|| = ||\mu \mathbf{e}_{i_{max}}|| = \mu < s + 1, p = \frac{||\mathbf{v}||\sqrt{\pi}}{s} < 1.0001\sqrt{\pi}$. It follows similarly as in the previous case that $\Pr_{\mathbf{x}}[\mathbf{x} \in \text{Bad}] \leq 0.91$. Overall, all the cases give

$$\Pr_{\mathbf{x}}\left[|[\langle \mathbf{x}, \mathbf{z} \rangle]_q| < \frac{q}{24\sqrt{n \log q}}\right] \leq 0.91.$$

□

Next, we show that with overwhelming probability over the choice of X, there are more than $n \log q$ entries of $[X^T \mathbf{z}]_q$ that have magnitude larger than $\frac{q}{24\sqrt{n \log q}}$. Consider independent binary random variables Y_i for $i = 1, 2, \ldots, m$, defined as follows over the choice of the columns $\mathbf{x}_i$ of X:

$$\begin{cases} Y_i = 1, \text{ if } |[\langle \mathbf{x}_i, \mathbf{z} \rangle]_q| \geq \frac{q}{24\sqrt{n \log q}} \\ Y_i = 0 \text{ otherwise.} \end{cases}$$

[2]Here, we apply the same map as in [AGHS13].

From Claim 13, we see that $\Pr_X[Y_i = 1] \geq 0.09$, which implies $\mathbb{E}\left[\sum_i Y_i\right] \geq 0.09m$. Using Lemma 17 with $t = 0.09m - n\log q$, it follows that $\Pr_X\left[\left|\sum_i Y_i - \mathbb{E}\left[\sum_i Y_i\right]\right| \geq 0.09m - n\log q\right] \leq 2\exp\left(-2\frac{(0.09m - n\log q)^2}{m}\right)$. Hence,

$$\begin{aligned}\Pr_X\left[\sum_i Y_i < n\log q\right] &\leq \Pr_X\left[0.09m - \sum_i Y_i \geq 0.09m - n\log q\right] \\ &\leq 2\exp\left(-2\frac{(0.09m - n\log q)^2}{m}\right) \\ &\leq 2\exp(-0.012m).\end{aligned}$$

The latter holds, for any $\mathbf{z} \in \mathbb{Z}^n$ with $||\mathbf{z}||_\infty \leq \frac{q}{2}$, and $||\mathbf{z}|| \geq \frac{q}{2s\sqrt{n\log q}}$. We conclude that

$$\Pr_X\left[\exists\, \mathbf{z} \in \mathbb{Z}^n : ||\mathbf{z}||_\infty \leq \frac{q}{2}, ||\mathbf{z}|| \leq \frac{q}{2s\sqrt{n}} \text{ and } \sum_i Y_i < n\log q\right] < q^n \cdot 2^{-0.012m} < 2^{-\Omega(n)}.$$

Summing up the two cases, with all but probability $2^{-\Omega(n)}$ over the choice of X, there does not exist any vector $\mathbf{z} \in \mathbb{Z}_q^n$ for which $[X^T\mathbf{z}]_q \setminus X^T\mathbb{Z}^n$ and $||[X^T\mathbf{z}]_q|| < \frac{q}{24}$. □

The next corollary, our result is a quantitative improvement over the result of [AGHS13] on the bound on the smoothing parameter of $\Lambda^\perp(X)$, by a factor of n.

Corollary 23. *With the parameters as in Theorem 20, except with probability $2^{-\Omega(n)}$ over the random choice of X, we have*

$$\eta_\varepsilon(\Lambda^\perp(X)) = O\left(m\sqrt{\log\left(\frac{m}{\varepsilon}\right)}\right).$$

Proof. By Theorem 20 we have that $\lambda_{n+1}(\Lambda_q(X)) \geq \frac{q}{24}$ with probability greater than $1 - 2^{-\Omega(n)}$. From Theorem 9 with $i = n+1$, we have that $\lambda_{m-n}(\Lambda_q^\perp(X)) \leq 24m$, implying that $\Lambda_q^\perp(X)$ has $m-n$ linearly independent vectors $||\mathbf{v}_1|| \leq ||\mathbf{v}_2|| \leq ... \leq ||\mathbf{v}_{m-n}|| \leq 24m$. Now, with any $q \geq 72ms\sqrt{n}$, we show that $\mathbf{v}_j \in \Lambda^\perp(X)$ for all $1 \leq j \leq m - n$.

First, we show that $\mathbf{v}_j$'s must be integer vectors. By definition of $\Lambda_q^\perp(X)$ and since $q\mathbf{e}_i \in \Lambda_q(X)$, for every $\mathbf{v} \in \Lambda_q^\perp(X)$, it holds that $qI_m \cdot \mathbf{v} \in q\mathbb{Z}^m$ and therefore $\mathbf{v} = I_m \cdot \mathbf{v} \in \mathbb{Z}^m$. By definition $X \cdot \mathbf{v}_j \in q\mathbb{Z}^n$ for all j. Now, by Lemma 13 with $r = 36ms\sqrt{n}$, we have $||X \cdot \mathbf{v}_j||_\infty \leq 36ms\sqrt{n} \leq \frac{q}{2}$ with all but probability at most $n \cdot 2\exp(-\frac{36^2m^2s^2n}{2\cdot 24^2m^2s^2}) < 2^{-\Omega(n)}$.[3]

[3]We note that this step was incorrect in [AGHS13]. This probability in [AGHS13] was $2^{-O(m)}$.

The above together with $X \cdot \mathbf{v}_j \in q\mathbb{Z}^n$ implies that $X \cdot \mathbf{v}_j = \mathbf{0}$ (over $\mathbb{R}$, without modular reduction). We conclude that the $\mathbf{v}_j$'s are in $\Lambda^\perp(X)$.

Finally, Lemma 10 gives us

$$\begin{aligned}\eta_\varepsilon(\Lambda^\perp(X)) &\leq 24m\sqrt{\frac{\ln\left(2(m-n)(1+\frac{1}{\varepsilon})\right)}{\pi}} \\ &\leq 24m\sqrt{\ln\left((m-n)(1+\frac{1}{\varepsilon})\right)} \\ &= O\left(m\sqrt{\log\left(\frac{m}{\varepsilon}\right)}\right).\end{aligned}$$

□

Now, we show how to remove the dependency on m in the leading order from the bound on the smoothing parameter of $\Lambda^\perp(X)$, which implies an improved upper bound on $\lambda_{m-n}(\Lambda^\perp(X))$. The main technique here is to divide our wide matrix X into $\frac{m}{m'}$ matrices of smaller size $n \times m'$, where m' is independent of m and is large enough to satisfy the conditions of Theorem 18. We show that every orthogonal lattice defined by such small matrices has $m' - n$ linearly independent vectors of norm at most $24m'$. By padding these vectors with zeros appropriately, we thus find $(m' - n)\frac{m}{m'}$ short and linearly independent vectors in $\Lambda^\perp(X)$. Finally, using Lemma 16 we obtain $m-n$ linearly independent vectors whose lengths are independent of m.

Corollary 24. *With the parameters m, n, s as in Theorem 20, except with probability $2^{-n(1-O(1))}$ over the random choice of X, we have*

$$\eta_\varepsilon(\Lambda^\perp(X)) = O\left(n\log(ns)\sqrt{\log\left(\frac{m}{\varepsilon}\right)}\right).$$

Proof. Having a "wide" matrix X, we start by splitting it up into $\frac{m}{m'}$ smaller matrices X_i, where m' is the smallest integer such that $m' \geq 100n\log(n^3s^2)$ and $\frac{m}{m'} \in \mathbb{Z}$. In particular, we have $X = [X_1|X_2|\ldots|X_{\frac{m}{m'}}]$ with $X_i \leftarrow (D_{\mathbb{Z}^n,s})^{m'}$ for all $i = 1, 2, \ldots, \frac{m}{m'}$. We use the same arguments as in the proof of Corollary 23 instantiated with $X_i \leftarrow (D_{\mathbb{Z}^n,s})^{m'}$ and parameters $s \geq 101\eta_\varepsilon(\mathbb{Z}^n)$, $n > 100$, $m' = 100n\log q$, $q = n^3s^2 > 72m's\sqrt{n}$. We find that $\Lambda^\perp(X_i)$ has $m' - n$ linearly independent vectors such that $||\mathbf{v}_1^i|| \leq ||\mathbf{v}_2^i|| \leq \ldots \leq ||\mathbf{v}_{m'-n}^i|| \leq 24m'$ with probability $1-2^{-\Omega(n)}$. It follows that we have $(m'-n)\frac{m}{m'} = m-n\frac{m}{m'}$

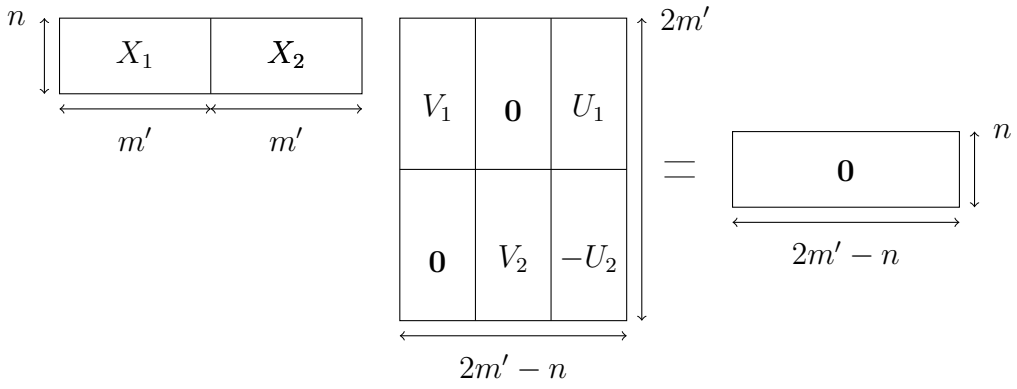

Figure 1: $2m' - n$ linearly independent short vectors in $\Lambda^{\perp}[X_1|X_2]$.

linearly independent vectors in $\Lambda^{\perp}(X)$ of the form:

$$\mathbf{u}_j^i = [\mathbf{0}_{(i-1)m'}||\mathbf{v}_j^i||\mathbf{0}_{(\frac{m}{m'}-i)m'}],$$

for $j = 1, 2, \ldots, m' - n$, and $i = 1, 2, \ldots, \frac{m}{m'}$. These vectors have norm at most $24m' = O(n \log(ns))$. Our goal is to have $(m - n)$ linearly independent short vectors in $\Lambda^{\perp}(X)$.

For simplicity, we consider only two blocks X_1, X_2 with the parameters as above. Our arguments can be readily generalized to more than two blocks. We show that with overwhelming probability, the lattice $\Lambda^{\perp}([X_1|X_2])$ has $2m' - n$ linearly independent vectors of norms $O(n \log(ns))$.

For $i = 1, 2$, let $U_i \in \mathbb{Z}^{m' \times n}$ be the matrices such that $X_i U_i = I_n$. Now, by Lemma 16 with parameters above, we have with probability greater than $1 - 2^{-n}$ the columns of U_i have norms smaller than $2\sqrt{30n \log(ns)}$. Hence, with all but probability $2^{-n(1-O(1))}$ over the choice of X_i, we get $X_i \cdot [V_i|U_i] = [\mathbf{0}_{n \times (m'-n)}|I_n]$ where V_i are the $m' \times (m' - n)$ matrices whose columns are $\mathbf{v}_1^i, \mathbf{v}_2^i \cdots, \mathbf{v}_{m'-n}^i$. It follows that $\Lambda^{\perp}([X_1|X_2])$ has $2m' - n$ short vectors (see Figure 1) with norms in $O(n \log(ns))$. We see that they are linearly independent because all of the column vectors of V_i, U_i are linearly independent.

Using the union bound, we get that $\Lambda^{\perp}(X)$ has $m - n$ short vectors with norms in $O(n \log(ns))$ with all but probability $\frac{m}{m'} \cdot 2^{-n(1-O(1))} = 2^{-n(1-O(1))}$.

Finally, we conclude that

$$\eta_\varepsilon(\Lambda^\perp(X)) = O(n\log(ns))\sqrt{\frac{\ln(2(m-n)(1+\frac{1}{\varepsilon}))}{\pi}} = O\left(n\log(ns)\sqrt{\log\left(\frac{m}{\varepsilon}\right)}\right).$$

□

Now as an important consequence of our main result, we obtain a tighter statement of the Leftover Hash Lemma over Lattices.

Theorem 25. *Let* $\varepsilon \in (0, 1/1000)$, $s \geq 101\eta_\varepsilon(\mathbb{Z}^n)$, $n > 100$, $m \geq 100n\log(72ms\sqrt{n})$, *and* $s' = \Omega(n\log(ns)\sqrt{\ln(1/\varepsilon)})$. *Then, with all but probability* $2^{-n(1-O(1))}$ *over the random choice of* X, *we have that*

$$\Delta(\mathcal{E}_{X,s'}, D_{\mathbb{Z}^m, s'X^T}) \leq 2\varepsilon.$$

Proof. By Lemma 18 with the parameters $\varepsilon \in (0, 1/1000)$, $s \geq 101\eta_\varepsilon(\mathbb{Z}^n) \geq 10\eta_\varepsilon(\mathbb{Z}^n)$, $n > 100$, and $m \geq 100n\log(72ms\sqrt{n}) \geq 10n\log(sn)$, the columns of X span all the $\mathbb{Z}^n$ with probability $1 - 2^{-\Theta(m)}$. Now, from Corollary 24, these parameters also ensure that with probability at least $1 - 2^{-n(1-O(1))}$, we have $\eta_\varepsilon(\Lambda^\perp(X)) \leq s'$. Finally, Lemma 19 says that when columns of X span all the $\mathbb{Z}^n$ and $\eta_\varepsilon(\Lambda^\perp(X)) \leq s'$, we have $\Delta(\mathcal{E}_{X,s'}, D_{\mathbb{Z}^m, s'X^T}) \leq 2\varepsilon$. This means that with the parameters as above, with all but probability $2^{-n(1-O(1))}$ over the random choice of X, the statistical distance between $\mathcal{E}_{X,s'}$ and $D_{\mathbb{Z}^m, s'X^T}$ is at most 2ε. □

References

[AGHS13] S. Agrawal, C. Gentry, S. Halevi, and A. Sahai. Discrete Gaussian leftover hash lemma over infinite domains. In ASIACRYPT, pages 97-116. 2013.

[AR16] D. Aggarwal, O. Regev. A Note on Discrete Gaussian Combinations of Lattice Vectors. 2013. Available at https://arxiv.org/abs/1308.2405

[MR07] D. Micciancio and O. Regev. Worst-case to average-case reductions based on gaussian measures. SIAM J. Computing, 37(1):267-302, 2007.

[DRS14] D. Dadush, O. Regev, and N. Stephens-Davidowitz. On the closest vector problem with a distance guarantee. In IEEE 29th Conference on Computational Complexity, pages 98-109, 2014. Full version available at http://arxiv.org/abs/1409.8063.

[Ban93] W. Banaszczyk. New bounds in some transference theorems in the geometry of numbers. Mathematische Annalen, 296(4):625-635, 1993.

[Lyu12] V. Lyubashevsky. Lattice signatures without trapdoors. In Proceedings of the 31st Annual international conference on Theory and Applications of Cryptographic Techniques, EUROCRYPT'12, Berlin, Heidelberg, 2012. SpringerVerlag.

[Ajt96] M. Ajitai. Generating hard instances of lattice problems, Electronic Colloquium on Computational Complexity (ECCC) 3 (1996), 29 p.

[Reg09] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. J. ACM,56(6), 2009.

[LPR10] V. Lyubashevsky, C. Peikert, and O. Regev. On ideal lattices and learning with errors over rings. In EUROCRYPT, pages 1-23, 2010.

[MR09] D. Micciancio and O. Regev. Lattice-based cryptography. In Post Quantum Cryptography, pages 147-191. Springer, February 2009.

[BBR88] C. H. Bennett, G. Brassard, and J.M. Robert. Privacy amplification by public discussion. SIAM Journal on Computing, 17(2):210-229, 1988.

[GKR04] R. Gennaro, H. Krawczyk, and T. Rabin. Secure Hashed Diffie-Hellman over Non-DDH Groups. In Eurocrypt '04, 2004. LNCS No.

[BH05] B. Barak and S. Halevi. A model and architecture for pseudo-random generation with applications to /dev/random. In Vijay Atluri, Catherine Meadows, and Ari Juels, editors, ACM Conference on Computer and Communications Security, pages 203-212. ACM, 2005.

[vDGHV10] M. van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan. Fully homomorphic encryption over the integers. In EUROCRYPT, pages 24-43, 2010.

[GGH12] S. Garg, C. Gentry, and S. Halevi. Candidate multilinear maps from ideal lattices and applications. Cryptology ePrint Archive, Report 2012/610, 2012. http://eprint.iacr.org/.

[GPV08] C. Gentry, C. Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In Cynthia Dwork, editor, STOC, pages 197-206. ACM, 2008.

[KLP12] G. Kuperberg, S. Lovett, and R. Peled. Probabilistic existence of rigid combinatorial structures. In 44th Symposium on Theory of Computing-STOC, pages 1091-1106. ACM, 2012.

[Reg05] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM, 56(6):34, 2009. Preliminary version in STOC'05.

[Ajt98] M. Ajtai. The shortest vector problem in L2 is NP-hard for randomized reductions. Proc. 30th ACM Symposium on Theory of Computing, pp. 10-19, 1998.