

The Euclidean Distortion of Flat Tori

Ishay Haviv*

Oded Regev†

June 20, 2010

Abstract

We show that for every n -dimensional lattice \mathcal{L} the torus \mathbb{R}^n/\mathcal{L} can be embedded with distortion $O(n \cdot \sqrt{\log n})$ into a Hilbert space. This improves the exponential upper bound of $O(n^{3n/2})$ due to Khot and Naor (FOCS 2005, Math. Annal. 2006) and gets close to their lower bound of $\Omega(\sqrt{n})$. We also obtain tight bounds for certain families of lattices.

Our main new ingredient is an embedding that maps any point $u \in \mathbb{R}^n/\mathcal{L}$ to a Gaussian function centered at u in the Hilbert space $L_2(\mathbb{R}^n/\mathcal{L})$. The proofs involve Gaussian measures on lattices, the smoothing parameter of lattices and Korkine-Zolotarev bases.

1 Introduction

An n -dimensional full-rank lattice $\mathcal{L} \subseteq \mathbb{R}^n$ is the set of all integer combinations of n linearly independent vectors. Such a lattice defines the *torus* \mathbb{R}^n/\mathcal{L} , i.e., the space \mathbb{R}^n where two points are identified if and only if the difference between them is a lattice vector. For $u, v \in \mathbb{R}^n/\mathcal{L}$ the distance $\text{dist}_{\mathbb{R}^n/\mathcal{L}}(u, v)$ in the torus \mathbb{R}^n/\mathcal{L} is defined as the distance between a representative of $u - v$ in \mathbb{R}^n from the lattice \mathcal{L} .

In this paper we study the ability to embed a torus \mathbb{R}^n/\mathcal{L} into a Hilbert space in a distance-preserving manner. For a lattice \mathcal{L} we are interested in a Hilbert space L_2 , an embedding $H : \mathbb{R}^n/\mathcal{L} \rightarrow L_2$ and a number $c_2 > 0$ such that for any $u, v \in \mathbb{R}^n/\mathcal{L}$,

$$\text{dist}_{\mathbb{R}^n/\mathcal{L}}(u, v) \leq \text{dist}_{L_2}(H(u), H(v)) \leq c_2 \cdot \text{dist}_{\mathbb{R}^n/\mathcal{L}}(u, v).$$

The *distortion* of an embedding H is the least c_2 for which the above holds. The least distortion that one can get over all the embeddings H is known as the *Euclidean distortion* of \mathbb{R}^n/\mathcal{L} and is denoted by $c_2(\mathbb{R}^n/\mathcal{L})$.

For example, consider the n -dimensional lattice \mathbb{Z}^n . The torus $\mathbb{R}^n/\mathbb{Z}^n$ can be embedded into the Euclidean space \mathbb{R}^{2n} by the embedding $H : \mathbb{R}^n/\mathbb{Z}^n \rightarrow \mathbb{R}^{2n}$ defined by

$$H(x_1, \dots, x_n) = (\cos 2\pi x_1, \sin 2\pi x_1, \dots, \cos 2\pi x_n, \sin 2\pi x_n).$$

It is easy to see that H has a constant distortion independent of n . It is not difficult to extend this example and to achieve an embedding with constant distortion for every lattice generated by n orthogonal vectors.

Metric embeddings have been extensively investigated in the last few years by the theoretical computer science community. One of the main motivations for research on embedding metric spaces comes from

*The Blavatnik School of Computer Science, Tel Aviv University, Tel Aviv 69978, Israel. Supported by the Adams Fellowship Program of the Israel Academy of Sciences and Humanities.

†The Blavatnik School of Computer Science, Tel Aviv University, Tel Aviv 69978, Israel. Supported by the Binational Science Foundation, by the Israel Science Foundation, by the European Commission under the Integrated Project QAP funded by the IST directorate as Contract Number 015848, by the Wolfson Family Charitable Trust, and by a European Research Council (ERC) Starting Grant.

applications to designing geometric approximation algorithms. Indeed, in order to approximate the distance between two points in a certain metric space one can apply an efficient low distortion embedding and then compute (or approximate) the distance between the corresponding embedded points. Studying the Euclidean distortion of flat tori might have applications to the complexity of lattice problems, and might also lead to more efficient algorithms for lattice problems through the use of our metric embeddings. For example, consider the Closest Vector Problem with Preprocessing (CVPP). In this problem a (not necessarily efficient) preprocessing step is applied to the lattice. Then, given a target point, we are supposed to efficiently approximate its distance from the lattice. Embedding flat tori suggests a special type of algorithms for CVPP, in which the data performed in the preprocessing step enables to approximate distances in the embedded space efficiently. A recent result by Micciancio and Voulgaris [13] demonstrates how CVPP can lead to breakthroughs for standard lattice problems. For further information on CVPP we refer the reader to [6].

In this work we study the distortion required to embed an n -dimensional torus into a Hilbert space. This question was introduced by Khot and Naor in [8] who provided a partial answer as stated below. The following theorem provides a lower bound on $c_2(\mathbb{R}^n/\mathcal{L})$ in terms of $\lambda_1(\mathcal{L}^*)$ and $\mu(\mathcal{L}^*)$, which are, respectively, the length of a shortest nonzero vector and the covering radius of \mathcal{L}^* , the dual lattice of \mathcal{L} .

Theorem 1.1 ([8]). *For any $n \geq 1$ and an n -dimensional lattice \mathcal{L} , $c_2(\mathbb{R}^n/\mathcal{L}) = \Omega\left(\frac{\lambda_1(\mathcal{L}^*)}{\mu(\mathcal{L}^*)} \cdot \sqrt{n}\right)$.*

It is known that for every large enough n there exists an n -dimensional self-dual lattice \mathcal{L} (i.e., $\mathcal{L} = \mathcal{L}^*$) such that $\lambda_1(\mathcal{L}) = \Theta(\mu(\mathcal{L}))$. This fact is due to Conway and Thompson; see [14, Page 46] for details. Theorem 1.1 and this family of lattices imply that for any large enough n there exists an n -dimensional lattice \mathcal{L} for which $c_2(\mathbb{R}^n/\mathcal{L}) = \Omega(\sqrt{n})$. We note that in [8] it was shown that the bound in Theorem 1.1 holds even for embeddings into the space L_1 . The next theorem shows an upper bound on $c_2(\mathbb{R}^n/\mathcal{L})$ for n -dimensional lattices and in particular implies that the supremum of $c_2(\mathbb{R}^n/\mathcal{L})$ over all n -dimensional lattices \mathcal{L} is finite.

Theorem 1.2 ([8]). *For any $n \geq 1$ and an n -dimensional lattice \mathcal{L} , $c_2(\mathbb{R}^n/\mathcal{L}) = O(n^{3n/2})$.*

We note that the true performance of the embedding of Khot and Naor used in the proof of Theorem 1.2 is not clear. Yet, it can be shown that there are lattices for which the distortion achieved by their embedding is super-polynomial. We discuss this issue in Section 7.

1.1 Our Results

The gap between the above lower and upper bounds on $c_2(\mathbb{R}^n/\mathcal{L})$ is huge. In this work we significantly reduce this gap. Our main result is that for every lattice the torus \mathbb{R}^n/\mathcal{L} can be embedded into a Hilbert space with distortion slightly higher than linear in n .

Theorem 1.3. *For any $n \geq 1$ and an n -dimensional lattice \mathcal{L} , $c_2(\mathbb{R}^n/\mathcal{L}) = O(n \cdot \sqrt{\log n})$.*

For n -dimensional lattices \mathcal{L} with ratio $\frac{\mu(\mathcal{L})}{\lambda_1(\mathcal{L})} \leq n^{o(n)}$ we provide the following better bound.

Theorem 1.4. *For any $n \geq 1$ and an n -dimensional lattice \mathcal{L} , $c_2(\mathbb{R}^n/\mathcal{L}) = O\left(\sqrt{n \cdot \log\left(\frac{4\mu(\mathcal{L})}{\lambda_1(\mathcal{L})}\right)}\right)$.*

Notice that Theorem 1.1 yields that the bound in Theorem 1.4 is tight up to a multiplicative constant for the self-dual lattices that were mentioned above (see Corollary 5.3).

Finally, we observe that Theorem 1.1 can be slightly improved to the following.

Theorem 1.5. *For any $n \geq 1$ and an n -dimensional lattice \mathcal{L} , $c_2(\mathbb{R}^n/\mathcal{L}) \geq \frac{\lambda_1(\mathcal{L}^*) \cdot \mu(\mathcal{L})}{4\sqrt{n}}$.*

It can be shown that $\mu(\mathcal{L}) \cdot \mu(\mathcal{L}^*) \geq \Omega(n)$ holds for any n -dimensional lattice and hence Theorem 1.5 improves Theorem 1.1 (see Remark 6.2 in Section 6).

1.2 Intuitive Overview of Proofs and Techniques

Our goal is to construct, given a lattice \mathcal{L} , a function H from the torus \mathbb{R}^n/\mathcal{L} to a Hilbert space such that H preserves distances up to a multiplicative factor that is as small as possible. Our basic idea is to map any $u \in \mathbb{R}^n$ to the Gaussian function defined on \mathbb{R}^n centered at u with parameter s , i.e., the function mapping $x \in \mathbb{R}^n$ to $e^{-\pi\|(x-u)/s\|^2}$. It is not difficult to see that the L_2 distance between $H(u)$ and $H(v)$ depends more or less linearly on the distance between u and v as long as the latter is at most s , beyond which the distance between $H(u)$ and $H(v)$ is saturated and no longer increases linearly. This is illustrated in the left side of Figure 1.

However, the embedding defined above is not an embedding of \mathbb{R}^n/\mathcal{L} because it is not \mathcal{L} -periodic. We therefore replace the Gaussian function centered at u with the sum of all Gaussian functions centered at points in $u + \mathcal{L}$, i.e., all the shifts of u by vectors of \mathcal{L} . See the right side of Figure 1.

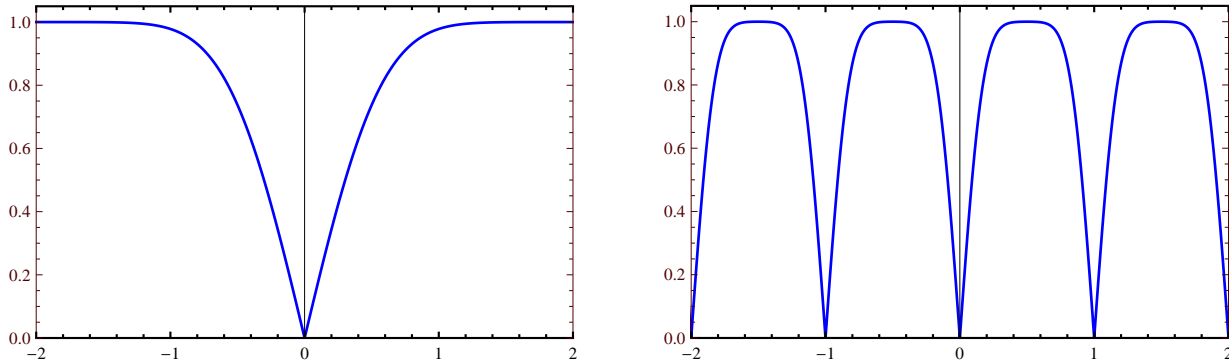


Figure 1: The left plot shows the L_2 distance between the (one-dimensional) Gaussian function centered at 0 and the Gaussian function centered at $u \in \mathbb{R}$ (as a function of u ; $s = 1$). The right plot shows the L_2 distance between the sum of all Gaussian functions centered at points in \mathbb{Z} and the sum of all Gaussian functions centered at points in $u + \mathbb{Z}$ (as a function of u ; $s = 0.3$).

An important role in the performance of our basic embedding is played by the choice of the parameter s . Notice that we cannot take s to be significantly smaller than the covering radius of \mathcal{L} (the maximum distance between two elements in \mathbb{R}^n/\mathcal{L}). Indeed, as mentioned above, the distance between the embedded functions is saturated beyond distance s , thereby leading to a distortion of at least $\mu(\mathcal{L})/s$. On the other hand, s cannot be larger than $\lambda_1(\mathcal{L})$: for such s , small shifts in the direction of a shortest vector of \mathcal{L} are much less noticeable than shifts in directions orthogonal to it, and this creates a huge distortion. By choosing s to be slightly smaller than $\lambda_1(\mathcal{L})$ our basic embedding achieves distortion proportional to $\frac{\mu(\mathcal{L})}{\lambda_1(\mathcal{L})}$ (see Theorem 5.2).

In order to improve the distortion we need two more ideas. First, we combine several basic embeddings for various choices of the parameter s in the range $[\lambda_1(\mathcal{L}), \mu(\mathcal{L})]$. The idea is that every distance in \mathbb{R}^n/\mathcal{L} is handled by at least one of these choices. This proves Theorem 1.4. The second idea which is used in the proof of Theorem 1.3 is to use our basic embedding on projected lattices using Korkine-Zolotarev bases.

In our analysis of the basic embedding we employ and extend techniques originating in a paper by Banaszczyk [4] that were found useful in several recent papers on the complexity of lattice problems (see, e.g., [1]).

1.3 Open Question

As mentioned before, we show in this paper that any n -dimensional lattice \mathcal{L} satisfies $c_2(\mathbb{R}^n/\mathcal{L}) = O(n \cdot \sqrt{\log n})$, and it was shown in [8] that there are lattices for which $c_2(\mathbb{R}^n/\mathcal{L}) = \Omega(\sqrt{n})$. The main open question raised by our work is the following.

Question 1.6. *Is it true that for any n -dimensional lattice \mathcal{L} , $c_2(\mathbb{R}^n/\mathcal{L}) = O(\sqrt{n})$?*

We observe that a positive answer to this question using Theorem 1.5 immediately implies that any n -dimensional lattice \mathcal{L} satisfies $\lambda_1(\mathcal{L}^*) \cdot \mu(\mathcal{L}) \leq O(n)$. The only proof we are aware of for this tight bound is the one of Banaszczyk [4] whose tools and techniques are the heart of the current paper. This might hint that our approach to the embedding question is natural and that it has not been pushed to its limit yet.

A more ambiguous open question is to obtain tight bounds on $c_2(\mathbb{R}^n/\mathcal{L})$ for every lattice \mathcal{L} in terms of geometrical parameters of \mathcal{L} .

1.4 Outline

The paper is organized as follows. In Section 2 we gather all the definitions on embeddings, lattices, Gaussian measures and Korkine-Zolotarev bases that we need in this paper. In Section 3 we prove properties of Gaussian distributions on lattices and in Section 4 we prove properties of Korkine-Zolotarev bases. In Section 5 we prove Theorems 1.4 and 1.3. We note that the lemmas proven in Section 4 are used in the proof of Theorem 1.3 but not in the proof of Theorem 1.4. Then, in Section 6 we prove Theorem 1.5. Finally, in Section 7 we discuss the performance of the embedding of Khot and Naor used in the proof of Theorem 1.2.

2 Preliminaries

2.1 General

For a real x , $\lceil x \rceil$ stands for the integer that satisfies $-0.5 < x - \lceil x \rceil \leq 0.5$. The ℓ_2 norm of $u \in \mathbb{C}^n$ is defined as $\|u\| = (\sum_{i=1}^n |u_i|^2)^{1/2}$ where u_i is the i th coordinate of u . The inner product of $u, v \in \mathbb{C}^n$ is defined as $\langle u, v \rangle = \sum_{i=1}^n u_i \bar{v}_i$. For a point $u \in \mathbb{C}^n$ and a set $S \subseteq \mathbb{C}^n$, denote $u + S = \{u + x \mid x \in S\}$ and $\text{dist}(u, S) = \inf_{x \in S} \|u - x\|$. The open unit ball is defined as $\mathcal{B} = \{w \in \mathbb{R}^n \mid \|w\| < 1\}$. For a scalar function f and a subset A of its domain, we use the notation $f(A) = \sum_{x \in A} f(x)$.

We will need the following simple fact, in which we do not make any attempt to optimize the constants.

Fact 2.1. *For any $a \geq 0$ and $0 \leq b < \frac{1}{\sqrt{2}}$,*

$$\cosh(2\pi ab) - 1 \leq 230 \cdot b^2 e^{\frac{3\pi}{4} a^2}.$$

Proof: We separate the proof into two cases as follows. If $\pi ab \leq 1$ then use the fact that any $\alpha \in [-2, 2]$ satisfies $\cosh(\alpha) - 1 \leq \alpha^2$ and $\alpha \leq e^\alpha$ to obtain $\cosh(2\pi ab) - 1 \leq 4\pi^2 \cdot b^2 e^{a^2}$. Otherwise, use the fact that any $\alpha \geq 0$ satisfies $\cosh(\alpha) \leq e^\alpha$ and $\alpha^2 \leq e^\alpha$ and the assumption $b \leq \frac{1}{\sqrt{2}}$ to obtain

$$\cosh(2\pi ab) - 1 \leq e^{2\pi ab} \leq (\pi ab)^2 \cdot e^{\sqrt{2}\pi a} \leq \pi^2 \cdot b^2 e^{(\sqrt{2}\pi+1)a} \leq 230 \cdot b^2 e^{\frac{3\pi}{4} a^2},$$

where the last inequality is easy to prove by taking the logarithm on both sides. ■

2.2 Embeddings

For two metric spaces (X, dist_X) and (Y, dist_Y) and a function $f : X \rightarrow Y$ we define the *Lipschitz constant* of f as

$$\|f\|_{\text{Lip}} = \sup_{x \neq y \in X} \frac{\text{dist}_Y(f(x), f(y))}{\text{dist}_X(x, y)}.$$

If f is injective we define its *distortion* as $\text{distortion}(f) = \|f\|_{\text{Lip}} \cdot \|f^{-1}\|_{\text{Lip}}$, and otherwise $\text{distortion}(f) = \infty$. By $c_Y(X)$ we denote the least distortion with which X can be embedded into Y , i.e.,

$$c_Y(X) = \inf \{ \text{distortion}(f) \mid f : X \rightarrow Y \}.$$

We use $c_p(X)$ to denote $c_{L_p}(X)$. Of special interest are embeddings into Hilbert spaces and in this case the parameter $c_2(X)$ is called the *Euclidean distortion* of X .

2.3 Lattices

An n -dimensional *lattice* $\mathcal{L} \subseteq \mathbb{R}^n$ is the set of all integer combinations of a set of linearly independent vectors $\{b_1, \dots, b_m\} \subseteq \mathbb{R}^n$, i.e., $\mathcal{L} = \{\sum_{i=1}^m a_i b_i \mid \forall i. a_i \in \mathbb{Z}\}$. The set $\{b_1, \dots, b_m\}$ is called a *basis* of \mathcal{L} and m , the number of vectors in it, is the *rank* of \mathcal{L} . Let B be the n by m matrix whose i th column is b_i . We identify the matrix and the basis that it represents and denote by $\mathcal{L}(B)$ the lattice that B generates. The determinant of \mathcal{L} is defined by $\det(\mathcal{L}) = \sqrt{\det(B^T B)}$. It is not difficult to verify that $\det(\mathcal{L})$ is independent of the choice of the basis. The *dual* lattice, denoted by \mathcal{L}^* , is defined as the set of all vectors in \mathbb{R}^n that have integer inner product with all the lattice vectors of \mathcal{L} , that is $\mathcal{L}^* = \{u \in \mathbb{R}^n \mid \forall v \in \mathcal{L}. \langle u, v \rangle \in \mathbb{Z}\}$, and a *self-dual* lattice is one that satisfies $\mathcal{L} = \mathcal{L}^*$. The length of a shortest nonzero vector in \mathcal{L} is denoted by $\lambda_1(\mathcal{L}) = \min\{\|u\| \mid u \in \mathcal{L} \setminus \{0\}\}$. This definition is naturally extended to the *successive minima* $\lambda_1, \dots, \lambda_m$ defined as follows:

$$\lambda_i(\mathcal{L}) = \inf\{r > 0 \mid \text{rank}(\text{span}(\mathcal{L} \cap r \cdot \mathcal{B})) \geq i\}.$$

It will be convenient to define also $\lambda_0(\mathcal{L}) = 0$. For a full-rank lattice \mathcal{L} (that is, $m = n$) the *covering radius* $\mu(\mathcal{L})$ is defined as the smallest r such that balls of radius r centered at all lattice points cover the entire space, or equivalently $\mu(\mathcal{L}) = \max\{\text{dist}(x, \mathcal{L}) \mid x \in \mathbb{R}^n\}$. It is well known that $\frac{1}{2} \cdot \lambda_n(\mathcal{L}) \leq \mu(\mathcal{L}) \leq \frac{\sqrt{n}}{2} \cdot \lambda_n(\mathcal{L})$ (see, e.g., [11, Page 138]). In [4] Banaszczyk proves relations between parameters of lattices, such as λ_1 and μ , and parameters of their dual. Such results are known as *transference theorems*. One of his results which is known to be tight up to a multiplicative constant is the following.

Theorem 2.2. *For any full-rank n -dimensional lattice \mathcal{L} , $\frac{1}{2} \leq \lambda_1(\mathcal{L}^*) \cdot \mu(\mathcal{L}) \leq \frac{n}{2}$.*

The space \mathbb{R}^n/\mathcal{L} is the quotient space defined by a lattice \mathcal{L} . Let $u, v \in \mathbb{R}^n/\mathcal{L}$ be two points. By abuse of notation we sometimes identify between points in \mathbb{R}^n/\mathcal{L} and their representatives in \mathbb{R}^n . For example, $\text{dist}_{\mathbb{R}^n/\mathcal{L}}(u, v)$ is defined as $\text{dist}(u, \mathcal{L} + v)$, i.e., the distance between representatives of u and v modulo the lattice. A function $f : \mathbb{R}^n \rightarrow \mathbb{C}$ is \mathcal{L} -*periodic* if $f(x) = f(x + y)$ for all $x \in \mathbb{R}^n$ and $y \in \mathcal{L}$. The Hilbert space $L_2(\mathbb{R}^n/\mathcal{L})$ is a space of scalar functions with domain \mathbb{R}^n/\mathcal{L} . We sometimes identify a function in $L_2(\mathbb{R}^n/\mathcal{L})$ with its corresponding \mathcal{L} -periodic function with domain \mathbb{R}^n . For $f, g \in L_2(\mathbb{R}^n/\mathcal{L})$, the distance between them is defined as

$$\text{dist}_{L_2(\mathbb{R}^n/\mathcal{L})}(f, g) = \left(\int_{\mathbb{R}^n/\mathcal{L}} |f(x) - g(x)|^2 dx \right)^{1/2}.$$

2.4 Gaussian Measures and the Smoothing Parameter

For $n \in \mathbb{N}$ and $s > 0$ let $\rho_s : \mathbb{R}^n \rightarrow (0, 1]$ be the Gaussian function centered at the origin scaled by a factor of s defined by

$$\forall x \in \mathbb{R}^n. \rho_s(x) = e^{-\pi\|x/s\|^2}.$$

We omit the subscript when $s = 1$. We define the *discrete Gaussian distribution* with parameter s on a lattice \mathcal{L} by its probability function

$$\forall x \in \mathcal{L}. D_{\mathcal{L},s}(x) = \frac{\rho_s(x)}{\rho_s(\mathcal{L})}.$$

Notice that the sum $\rho_s(\mathcal{L})$ over all lattice vectors is finite, as follows from the fact that $\int_{\mathbb{R}^n} \rho_s(x) dx = s^n$. It can be shown that a vector sampled from $D_{\mathcal{L},s}$ has the zeros vector as expectation and has expected squared norm close to $s^2n/2\pi$ if s is large enough. Micciancio and Regev [12] defined a lattice parameter that measures how big s should be for the distribution $D_{\mathcal{L},s}$ to “behave like” a continuous Gaussian distribution in \mathbb{R}^n (and in particular to have expected squared norm close to $s^2n/2\pi$). This parameter is called the *smoothing parameter* and is defined as follows.

Definition 2.3. For a lattice \mathcal{L} and a positive $\varepsilon > 0$ the smoothing parameter $\eta_\varepsilon(\mathcal{L})$ is defined as the smallest $s > 0$ such that $\rho_{1/s}(\mathcal{L}^* \setminus \{0\}) \leq \varepsilon$.

A main property of the smoothing parameter is that, roughly speaking, the distribution of a uniformly chosen random lattice point from \mathcal{L} perturbed by a Gaussian with $s = \eta_\varepsilon(\mathcal{L})$ is $\varepsilon/2$ -close to a uniform distribution on the entire space. For more details on the smoothing parameter the reader is referred to [12].

We state below a lemma due to Banaszczyk [4] and a simple bound on the smoothing parameter that it yields.

Lemma 2.4 ([4]). For any $n \geq 1$, an n -dimensional lattice \mathcal{L} and a vector $u \in \mathbb{R}^n$,

$$\rho((\mathcal{L} - u) \setminus 2\sqrt{n}\mathcal{B}) \leq 2^{-11n} \cdot \rho(\mathcal{L}).$$

Lemma 2.5. For any $n \geq 1$ and an n -dimensional lattice \mathcal{L} , $\eta_\varepsilon(\mathcal{L}) \leq \frac{2\sqrt{n}}{\lambda_1(\mathcal{L}^*)}$ where $\varepsilon = 2^{-10n}$.

Proof: The proof is nearly identical to a proof of a similar lemma in [12]. For any n -dimensional lattice \mathcal{L} , Lemma 2.4 and the fact that $\rho(\mathcal{L}) = \rho(\mathcal{L} \setminus 2\sqrt{n}\mathcal{B}) + \rho(\mathcal{L} \cap 2\sqrt{n}\mathcal{B})$ imply that

$$\rho(\mathcal{L} \setminus 2\sqrt{n}\mathcal{B}) \leq \frac{2^{-11n}}{1 - 2^{-11n}} \cdot \rho(\mathcal{L} \cap 2\sqrt{n}\mathcal{B}) < 2^{-10n} \cdot \rho(\mathcal{L} \cap 2\sqrt{n}\mathcal{B}).$$

Take $s > \frac{2\sqrt{n}}{\lambda_1(\mathcal{L}^*)}$ and observe that

$$\rho_{1/s}(\mathcal{L}^* \setminus \{0\}) = \rho(s\mathcal{L}^* \setminus \{0\}) = \rho(s\mathcal{L}^* \setminus 2\sqrt{n}\mathcal{B}) < 2^{-10n} \cdot \rho(s\mathcal{L}^* \cap 2\sqrt{n}\mathcal{B}) = 2^{-10n}.$$

■

2.5 Korkine-Zolotarev Bases

The question of specifying a basis of a lattice with valuable properties is known as *reduction theory*. In 1873, Korkine and Zolotarev [9] defined and studied a notion of a reduced basis whose vectors are in some sense close to orthogonal. These bases are known as Korkine-Zolotarev bases.

Before defining Korkine-Zolotarev bases we need to define the *Gram-Schmidt orthogonalization process*. For a sequence of vectors b_1, \dots, b_n define the corresponding Gram-Schmidt orthogonalized vectors $\tilde{b}_1, \dots, \tilde{b}_n$ by

$$\tilde{b}_i = b_i - \sum_{j=1}^{i-1} \mu_{i,j} \tilde{b}_j, \quad \mu_{i,j} = \frac{\langle b_i, \tilde{b}_j \rangle}{\langle \tilde{b}_j, \tilde{b}_j \rangle}.$$

In words, \tilde{b}_i is the component of b_i orthogonal to b_1, \dots, b_{i-1} . A Korkine-Zolotarev basis is defined as follows.

Definition 2.6. Let B be a basis of an n -dimensional lattice \mathcal{L} and let \tilde{B} be the corresponding Gram-Schmidt orthogonalized basis. For $1 \leq i \leq n$ define the projection function $\pi_i^{(B)}(x) = \sum_{j=i}^n \langle x, \tilde{b}_j \rangle \cdot \tilde{b}_j / \|\tilde{b}_j\|^2$ that maps x to its projection on $\text{span}(\tilde{b}_i, \dots, \tilde{b}_n)$. A basis B is a Korkine-Zolotarev basis if for all $1 \leq i \leq n$,

- \tilde{b}_i is a shortest nonzero vector in $\pi_i^{(B)}(\mathcal{L}) = \{\pi_i^{(B)}(u) \mid u \in \mathcal{L}\}$,
- and for all $j < i$, the Gram-Schmidt coefficients $\mu_{i,j}$ of B satisfy $|\mu_{i,j}| \leq \frac{1}{2}$.

Lagarias, Lenstra and Schnorr [10] proved that the norms of the vectors in a Korkine-Zolotarev basis are not far from the successive minima of the lattice, as stated below.

Theorem 2.7 ([10]). If B is a Korkine-Zolotarev basis of an n -dimensional lattice \mathcal{L} , then for all $1 \leq i \leq n$,

$$\frac{4}{i+3} \cdot \lambda_i(\mathcal{L})^2 \leq \|b_i\|^2 \leq \frac{i+3}{4} \cdot \lambda_i(\mathcal{L})^2.$$

3 Properties of Gaussian Distributions

For an n -dimensional lattice $\mathcal{L} \subseteq \mathbb{R}^n$ and a positive number $s > 0$ we define the function $h_{\mathcal{L},s} : \mathbb{R}^n \rightarrow [0, 1)$ by

$$\forall u \in \mathbb{R}^n. \quad h_{\mathcal{L},s}(u) = 1 - \frac{\rho_s(\mathcal{L} - u)}{\rho_s(\mathcal{L})}.$$

It can be shown that the function $h_{\mathcal{L},s}$ is nonnegative.¹ Notice that if $u \in \mathcal{L}$ then $h_{\mathcal{L},s}(u) = 0$.

In this section we gather and prove several results on $h_{\mathcal{L},s}$ that, roughly speaking, show that for certain choices of s , $h_{\mathcal{L},s}(u)$ is closely related to the distance of u from \mathcal{L} . The following lemma provides upper and lower bounds on $h_{\mathcal{L},s}(u)$. Its first item is due to [4] and we include its proof for completeness. We remark that the lemma can also be proven using Fourier transform.

Lemma 3.1. For any $n \geq 1$, an n -dimensional lattice \mathcal{L} , a vector $u \in \mathbb{R}^n$ and $s > 0$,

1. $h_{\mathcal{L},s}(u) \leq \frac{\pi}{s^2} \cdot \text{dist}(u, \mathcal{L})^2$.
2. If $0 < \varepsilon \leq \frac{1}{1000}$, $s \leq \frac{1}{2\eta_\varepsilon(\mathcal{L}^*)}$ and $\text{dist}(u, \mathcal{L}) \leq \frac{s}{\sqrt{2}}$ then $h_{\mathcal{L},s}(u) \geq \frac{c}{s^2} \cdot \text{dist}(u, \mathcal{L})^2$, where c is an absolute constant.

¹For example, this follows from Proposition 5.1.

Proof: Assume without loss of generality that $\text{dist}(u, \mathcal{L}) = \|u\|$ and observe that

$$\begin{aligned} h_{\mathcal{L},s}(u) &= 1 - \frac{1}{\rho_s(\mathcal{L})} \cdot \sum_{x \in \mathcal{L}} e^{-\frac{\pi\|x-u\|^2}{s^2}} = 1 - \frac{1}{2\rho_s(\mathcal{L})} \cdot \sum_{x \in \mathcal{L}} \left(e^{-\frac{\pi\|x-u\|^2}{s^2}} + e^{-\frac{\pi\|x+u\|^2}{s^2}} \right) \\ &= 1 - \frac{e^{-\frac{\pi\|u\|^2}{s^2}}}{\rho_s(\mathcal{L})} \cdot \sum_{x \in \mathcal{L}} \left(e^{-\frac{\pi\|x\|^2}{s^2}} \cdot \cosh\left(\frac{2\pi\langle x, u \rangle}{s^2}\right) \right) \\ &= 1 - e^{-\frac{\pi\|u\|^2}{s^2}} - \frac{e^{-\frac{\pi\|u\|^2}{s^2}}}{\rho_s(\mathcal{L})} \cdot \sum_{x \in \mathcal{L} \setminus \{0\}} \left(e^{-\frac{\pi\|x\|^2}{s^2}} \cdot \left(\cosh\left(\frac{2\pi\langle x, u \rangle}{s^2}\right) - 1 \right) \right). \end{aligned}$$

For Item 1, use the fact that for all $\alpha \in \mathbb{R}$, $\cosh(\alpha) \geq 1$ and $1 - e^{-\alpha} \leq \alpha$ to get that

$$h_{\mathcal{L},s}(u) \leq 1 - e^{-\frac{\pi\|u\|^2}{s^2}} \leq \frac{\pi\|u\|^2}{s^2} = \frac{\pi}{s^2} \cdot \text{dist}(u, \mathcal{L})^2.$$

For Item 2, use the Cauchy-Schwarz inequality and Fact 2.1 to get that any $x \in \mathcal{L} \setminus \{0\}$ satisfies

$$\cosh\left(\frac{2\pi\langle x, u \rangle}{s^2}\right) - 1 \leq \cosh\left(\frac{2\pi\|x\| \cdot \|u\|}{s^2}\right) - 1 \leq 230 \cdot \frac{\|u\|^2}{s^2} \cdot e^{\frac{3\pi\|x\|^2}{4s^2}}.$$

This implies that

$$\begin{aligned} h_{\mathcal{L},s}(u) &\geq 1 - e^{-\frac{\pi\|u\|^2}{s^2}} - \frac{230\|u\|^2}{s^2} \cdot \sum_{x \in \mathcal{L} \setminus \{0\}} \left(e^{-\frac{\pi\|x\|^2}{s^2}} \cdot e^{\frac{3\pi\|x\|^2}{4s^2}} \right) \\ &= 1 - e^{-\frac{\pi\|u\|^2}{s^2}} - \frac{230\|u\|^2}{s^2} \cdot \rho_{2s}(\mathcal{L} \setminus \{0\}) \geq \frac{\|u\|^2}{s^2} \left(\frac{\pi}{4} - 230\varepsilon \right), \end{aligned}$$

where the last inequality follows from the inequality $1 - e^{-\alpha} \geq \frac{\alpha}{4}$ that holds for any $\alpha \leq 2$ and the assumptions $\|u\| \leq \frac{s}{\sqrt{2}}$ and $\eta_\varepsilon(\mathcal{L}^*) \leq \frac{1}{2s}$. This completes the proof by our assumption on ε . \blacksquare

We turn to deal with lower bounds on $h_{\mathcal{L},s}(u)$ for vectors u that are far from the lattice.

Lemma 3.2. *For any $n \geq 1$, an n -dimensional lattice \mathcal{L} , $s > 0$ and $u \in \mathbb{R}^n$,*

1. *If $\text{dist}(u, \mathcal{L}) > 2s \cdot \sqrt{n}$ then $h_{\mathcal{L},s}(u) \geq 1 - 2^{-11n}$.*
2. *If $\lambda_1(\mathcal{L}) \geq 4s\sqrt{n}$ then $h_{\mathcal{L},s}(u) \geq 1 - e^{-\pi \text{dist}(u, \mathcal{L})^2/s^2} - 2^{-11n}$.*

Proof: First, apply Lemma 2.4 to $\frac{1}{s} \cdot \mathcal{L}$ to get that

$$h_{\mathcal{L},s}(u) \geq 1 - 2^{-11n} - \frac{\rho_s((\mathcal{L} - u) \cap 2s \cdot \sqrt{n}\mathcal{B})}{\rho_s(\mathcal{L})}.$$

If $\text{dist}(u, \mathcal{L}) > 2s \cdot \sqrt{n}$ then the intersection $(\mathcal{L} - u) \cap (2s \cdot \sqrt{n}\mathcal{B})$ is empty and we are done. For Item 2, notice that there is at most one point of $\mathcal{L} - u$ inside the (open) ball of radius $2s \cdot \sqrt{n}$. \blacksquare

4 Properties of Korkine-Zolotarev Bases

In this section we prove two simple lemmas on Korkine-Zolotarev bases (see Definition 2.6). For an n -dimensional lattice \mathcal{L} and a Korkine-Zolotarev basis B that generates it, let $\mathcal{L}_i = \pi_i^{(B)}(\mathcal{L})$ be the projection of \mathcal{L} on $\text{span}(\tilde{b}_i, \dots, \tilde{b}_n)$. Notice that \mathcal{L}_i is a lattice for every $1 \leq i \leq n$. Intuitively speaking, since the vectors of B are close to being orthogonal, we expect a shortest nonzero vector in \mathcal{L}_i to have length similar to $\lambda_i(\mathcal{L})$. This is stated formally in the following lemma. Notice that the lower bound is meaningful only when there is a gap between $\lambda_{i-1}(\mathcal{L})$ and $\lambda_i(\mathcal{L})$.

Lemma 4.1. *Let B be a Korkine-Zolotarev basis of an n -dimensional lattice \mathcal{L} and denote $\mathcal{L}_i = \pi_i^{(B)}(\mathcal{L})$. Then for all $1 \leq i \leq n$,*

$$\frac{4}{i+3} \cdot \lambda_i(\mathcal{L})^2 - \frac{i-1}{4} \cdot \lambda_{i-1}(\mathcal{L})^2 \leq \lambda_1(\mathcal{L}_i)^2 \leq \lambda_i(\mathcal{L})^2.$$

Proof: For an n -dimensional lattice \mathcal{L} and $i \leq n$ there exist i linearly independent vectors in \mathcal{L} of length at most $\lambda_i(\mathcal{L})$. At least one of these vectors does not belong to $\text{span}(b_1, \dots, b_{i-1})$. Hence, a nonzero vector of length at most $\lambda_i(\mathcal{L})$ belongs to \mathcal{L}_i , so $\lambda_1(\mathcal{L}_i) \leq \lambda_i(\mathcal{L})$. For the left inequality, use Theorem 2.7 and the right inequality that we just proved to observe that

$$\begin{aligned} \lambda_1(\mathcal{L}_i)^2 &= \|\tilde{b}_i\|^2 = \|b_i\|^2 - \sum_{j=1}^{i-1} \mu_{i,j}^2 \|\tilde{b}_j\|^2 \geq \frac{4}{i+3} \cdot \lambda_i(\mathcal{L})^2 - \frac{1}{4} \cdot \sum_{j=1}^{i-1} \lambda_j(\mathcal{L})^2 \\ &\geq \frac{4}{i+3} \cdot \lambda_i(\mathcal{L})^2 - \frac{i-1}{4} \cdot \lambda_{i-1}(\mathcal{L})^2. \end{aligned}$$

■

The next lemma says that if the distance of a vector $u \in \mathbb{R}^n$ from \mathcal{L} is somewhat higher than $\lambda_{i-1}(\mathcal{L})$, then it is close to the distance between \mathcal{L}_i and the projected vector $\pi_i(u)$.

Lemma 4.2. *Let B be a Korkine-Zolotarev basis of an n -dimensional lattice \mathcal{L} and denote $\mathcal{L}_i = \pi_i^{(B)}(\mathcal{L})$. Then for any $u \in \mathbb{R}^n$ and $1 \leq i \leq n$,*

$$\text{dist}(u, \mathcal{L})^2 - \frac{i-1}{4} \cdot \lambda_{i-1}(\mathcal{L})^2 \leq \text{dist}(\pi_i(u), \mathcal{L}_i)^2 \leq \text{dist}(u, \mathcal{L})^2.$$

Proof: For the right inequality, let $w \in \mathcal{L}$ be a lattice vector that satisfies $\text{dist}(u, \mathcal{L}) = \text{dist}(u, w)$. Since π_i is an orthogonal projection

$$\text{dist}(u, \mathcal{L}) = \text{dist}(u, w) \geq \text{dist}(\pi_i(u), \pi_i(w)) \geq \text{dist}(\pi_i(u), \mathcal{L}_i).$$

For the left inequality, let $v \in \mathcal{L}$ be a lattice vector that satisfies $\text{dist}(\pi_i(u), \mathcal{L}_i) = \text{dist}(\pi_i(u), \pi_i(v))$ and $|\langle u - v - \pi_i(u - v), \tilde{b}_j \rangle| \leq \frac{1}{2} \|\tilde{b}_j\|^2$ for every $1 \leq j \leq i-1$. Such a vector can be easily constructed from $u - v$ by subtracting appropriate integer multiples of $\tilde{b}_{i-1}, \dots, \tilde{b}_1$. We obtain that

$$\begin{aligned} \text{dist}(u, \mathcal{L})^2 &\leq \text{dist}(u, v)^2 = \text{dist}(\pi_i(u), \pi_i(v))^2 + \text{dist}(u - \pi_i(u), v - \pi_i(v))^2 \\ &\leq \text{dist}(\pi_i(u), \mathcal{L}_i)^2 + \frac{1}{4} \cdot \sum_{j=1}^{i-1} \|\tilde{b}_j\|^2 \leq \text{dist}(\pi_i(u), \mathcal{L}_i)^2 + \frac{i-1}{4} \cdot \lambda_{i-1}(\mathcal{L})^2, \end{aligned}$$

as desired. ■

5 The Embedding

In this section we prove the main results of the paper. We define an embedding from a torus \mathbb{R}^n/\mathcal{L} into the Hilbert space $L_2(\mathbb{R}^n/\mathcal{L})$ and relate the distortion that it achieves to the function $h_{\mathcal{L},s}$ defined in Section 3.

For an n -dimensional lattice \mathcal{L} and $s > 0$ we define the embedding $H_{\mathcal{L},s} : \mathbb{R}^n/\mathcal{L} \rightarrow L_2(\mathbb{R}^n/\mathcal{L})$ that maps any vector $u \in \mathbb{R}^n/\mathcal{L}$ to the function that maps any $x \in \mathbb{R}^n$ to

$$\frac{s}{\sqrt{2\rho_s(\mathcal{L})}} \cdot \left(\frac{2}{s}\right)^{n/2} \cdot \rho_{\frac{s}{\sqrt{2}}}(\mathcal{L} + x - u).$$

In words, $H_{\mathcal{L},s}(u)$ is the function that maps any $x \in \mathbb{R}^n$ to the mass of the Gaussian function centered at u with parameter $\frac{s}{\sqrt{2}}$ on all the shifts of x by lattice vectors (up to some normalization factor).

The following proposition relates the distance between two embedded points and the function $h_{\mathcal{L},s}$ from Section 3. This enables us to use the lemmas from Section 3 to bound the distortion achieved by our embedding.

Proposition 5.1. *For any $n \geq 1$, an n -dimensional lattice \mathcal{L} , a real $s > 0$ and $u, v \in \mathbb{R}^n/\mathcal{L}$,*

$$\text{dist}_{L_2(\mathbb{R}^n/\mathcal{L})}(H_{\mathcal{L},s}(u), H_{\mathcal{L},s}(v))^2 = s^2 \cdot h_{\mathcal{L},s}(u - v).$$

Proof: We start by calculating the following integral for general $u, v \in \mathbb{R}^n$.

$$\begin{aligned} \int_{\mathbb{R}^n/\mathcal{L}} \rho_{\frac{s}{\sqrt{2}}}(\mathcal{L} + z - u) \rho_{\frac{s}{\sqrt{2}}}(\mathcal{L} + z - v) dz &= \sum_{x \in \mathcal{L}} \int_{\mathbb{R}^n/\mathcal{L}} \rho_{\frac{s}{\sqrt{2}}}(x + z - u) \rho_{\frac{s}{\sqrt{2}}}(\mathcal{L} + x + z - v) dz \\ &= \int_{\mathbb{R}^n} \rho_{\frac{s}{\sqrt{2}}}(w) \rho_{\frac{s}{\sqrt{2}}}(\mathcal{L} + w + u - v) dw \\ &= \sum_{y \in \mathcal{L}} \int_{\mathbb{R}^n} \rho_s(2w + y + u - v) \rho_s(y + u - v) dw \\ &= \left(\frac{s}{2}\right)^n \cdot \rho_s(\mathcal{L} + v - u), \end{aligned}$$

where for the first equality notice that $\mathcal{L} = x + \mathcal{L}$ for every $x \in \mathcal{L}$ and for the third use the parallelogram law. Now we prove the lemma using the integral from above.

$$\begin{aligned} \text{dist}_{L_2(\mathbb{R}^n/\mathcal{L})}(H_{\mathcal{L},s}(u), H_{\mathcal{L},s}(v))^2 &= \frac{s^2}{2\rho_s(\mathcal{L})} \cdot \left(\frac{2}{s}\right)^n \cdot \int_{\mathbb{R}^n/\mathcal{L}} (\rho_{\frac{s}{\sqrt{2}}}(\mathcal{L} + z - u) - \rho_{\frac{s}{\sqrt{2}}}(\mathcal{L} + z - v))^2 dz \\ &= \frac{s^2}{2\rho_s(\mathcal{L})} \cdot \left(\frac{2}{s}\right)^n \cdot \left(2 \cdot \left(\frac{s}{2}\right)^n \cdot \rho_s(\mathcal{L}) - 2 \cdot \left(\frac{s}{2}\right)^n \cdot \rho_s(\mathcal{L} + v - u)\right) \\ &= s^2 \cdot \left(1 - \frac{\rho_s(\mathcal{L} + v - u)}{\rho_s(\mathcal{L})}\right) = s^2 \cdot h_{\mathcal{L},s}(u - v). \end{aligned}$$

■

5.1 Upper Bounds in Terms of Lattice Parameters

In this section we prove an upper bound on $c_2(\mathbb{R}^n/\mathcal{L})$ in terms of $\lambda_1(\mathcal{L})$ and $\mu(\mathcal{L})$. We start with the following theorem for didactical reasons and then prove its strengthening Theorem 1.4.

Theorem 5.2. *For any $n \geq 1$ and an n -dimensional lattice \mathcal{L} , $c_2(\mathbb{R}^n/\mathcal{L}) = O\left(\frac{\mu(\mathcal{L})}{\lambda_1(\mathcal{L})} \cdot \sqrt{n}\right)$.*

Proof: Let \mathcal{L} be an n -dimensional lattice, consider the embedding $H_{\mathcal{L},s}$ for $s = \frac{\lambda_1(\mathcal{L})}{4\sqrt{n}}$, and fix distinct $u, v \in \mathbb{R}^n/\mathcal{L}$. By Proposition 5.1 our goal is to bound

$$A := \frac{\text{dist}_{L_2(\mathbb{R}^n/\mathcal{L})}(H_{\mathcal{L},s}(u), H_{\mathcal{L},s}(v))^2}{\text{dist}_{\mathbb{R}^n/\mathcal{L}}(u, v)^2} = \frac{s^2 \cdot h_{\mathcal{L},s}(u - v)}{\text{dist}_{\mathbb{R}^n/\mathcal{L}}(u, v)^2}$$

from above and from below. For the upper bound use Item 1 of Lemma 3.1 to obtain $A \leq s^2 \cdot \frac{\pi}{s^2} = \pi$. For the lower bound consider the following two cases. If $\text{dist}_{\mathbb{R}^n/\mathcal{L}}(u, v) \leq \frac{s}{\sqrt{2}}$ then by Item 2 of Lemma 3.1 applied to $u - v$ we get $A \geq s^2 \cdot \frac{c}{s^2} = c$, using Lemma 2.5 that yields $2\eta_\varepsilon(\mathcal{L}^*) \leq \frac{4\sqrt{n}}{\lambda_1(\mathcal{L})} = \frac{1}{s}$ for $\varepsilon = 2^{-10n} \leq \frac{1}{1000}$. Otherwise, if $\text{dist}_{\mathbb{R}^n/\mathcal{L}}(u, v) > \frac{s}{\sqrt{2}}$, by Item 2 of Lemma 3.2 applied to $u - v$ we have $A \geq s^2 \cdot \frac{1 - e^{-\pi/2} - 2^{-11n}}{\mu(\mathcal{L})^2}$, using the fact that $\lambda_1(\mathcal{L}) = 4s \cdot \sqrt{n}$. Hence, our embedding achieves distortion $O\left(\frac{\mu(\mathcal{L})}{s}\right) = O\left(\frac{\mu(\mathcal{L})}{\lambda_1(\mathcal{L})} \cdot \sqrt{n}\right)$.

■

For the proof of Theorem 1.4 we extend the embedding $H_{\mathcal{L},s}$ as follows. For an n -dimensional lattice \mathcal{L} , $s > 0$ and $k \geq 1$, we define the embedding $H_{\mathcal{L},s}^{(k)} : \mathbb{R}^n/\mathcal{L} \rightarrow L_2(\mathbb{R}^n/\mathcal{L})^k$ by

$$H_{\mathcal{L},s}^{(k)} = (H_{\mathcal{L},s_1}, H_{\mathcal{L},s_2}, \dots, H_{\mathcal{L},s_k}),$$

where $s_i = 2^{i-1} \cdot s$.

Theorem 1.4. For any $n \geq 1$ and an n -dimensional lattice \mathcal{L} , $c_2(\mathbb{R}^n/\mathcal{L}) = O\left(\sqrt{n \cdot \log\left(\frac{4\mu(\mathcal{L})}{\lambda_1(\mathcal{L})}\right)}\right)$.

Proof: Let \mathcal{L} be an n -dimensional lattice and consider the embedding $H_{\mathcal{L},s}^{(k)}$ for $s = \frac{\lambda_1(\mathcal{L})}{4\sqrt{n}}$ and $k = \left\lceil \log\left(\frac{4\mu(\mathcal{L})}{\lambda_1(\mathcal{L})}\right) \right\rceil$. This embedding maps any point $u \in \mathbb{R}^n/\mathcal{L}$ to a vector of Gaussian functions with various radii in the interval between the length of a shortest nonzero vector in \mathcal{L} and its covering radius. Intuitively, in this way for every possible distance between two points in \mathbb{R}^n/\mathcal{L} we have a Gaussian function sensitive to it.

Fix distinct $u, v \in \mathbb{R}^n/\mathcal{L}$ and use Proposition 5.1 to observe that

$$\frac{\text{dist}_{L_2(\mathbb{R}^n/\mathcal{L})^k}(H_{\mathcal{L},s}^{(k)}(u), H_{\mathcal{L},s}^{(k)}(v))^2}{\text{dist}_{\mathbb{R}^n/\mathcal{L}}(u, v)^2} = \sum_{i=1}^k \frac{\text{dist}_{L_2(\mathbb{R}^n/\mathcal{L})}(H_{\mathcal{L},s_i}(u), H_{\mathcal{L},s_i}(v))^2}{\text{dist}_{\mathbb{R}^n/\mathcal{L}}(u, v)^2} = \sum_{i=1}^k A_i(u, v),$$

where $s_i = 2^{i-1} \cdot s$ and $A_i(u, v) = \frac{s_i^2 \cdot h_{\mathcal{L},s_i}(u-v)}{\text{dist}_{\mathbb{R}^n/\mathcal{L}}(u,v)^2}$ for $1 \leq i \leq k$. We will show that

$$\Omega\left(\frac{1}{n}\right) \leq \sum_{i=1}^k A_i(u, v) \leq O(k), \quad (1)$$

which implies that our embedding has distortion $O(\sqrt{nk})$, as required.

By Item 1 of Lemma 3.1 we have $A_i(u, v) \leq s_i^2 \cdot \frac{\pi}{s_i^2} = \pi$ for every $1 \leq i \leq k$, which proves the upper bound in (1). In order to prove the lower bound in (1) we now show that there exists an i such that $A_i(u, v) \geq \Omega(\frac{1}{n})$. Consider the following three cases:

- Case 1: $\text{dist}_{\mathbb{R}^n/\mathcal{L}}(u, v) \leq \frac{1}{4\sqrt{2n}} \cdot \lambda_1(\mathcal{L})$.

Notice that by Lemma 2.5 we have $2\eta_\varepsilon(\mathcal{L}^*) \leq \frac{4\sqrt{n}}{\lambda_1(\mathcal{L})} = \frac{1}{s_1}$ for $\varepsilon = 2^{-10n} \leq \frac{1}{1000}$. Hence, by Item 2 of Lemma 3.1, $A_1(u, v) \geq s_1^2 \cdot \frac{c}{s_1^2} = c$.

- Case 2: $\frac{1}{4\sqrt{2n}} \cdot \lambda_1(\mathcal{L}) < \text{dist}_{\mathbb{R}^n/\mathcal{L}}(u, v) \leq \lambda_1(\mathcal{L})$.

Since $\lambda_1(\mathcal{L}) = 4s_1\sqrt{n}$, by Item 2 of Lemma 3.2 we get $h_{\mathcal{L},s_1}(u-v) \geq 1 - e^{-\pi/2} - 2^{-11n}$ and hence

$$A_1(u, v) \geq (1 - e^{-\pi/2} - 2^{-11n}) \cdot \frac{s_1^2}{\text{dist}_{\mathbb{R}^n/\mathcal{L}}^2(u, v)} \geq \frac{1 - e^{-\pi/2} - 2^{-11n}}{16n}.$$

- Case 3: $\lambda_1(\mathcal{L}) < \text{dist}_{\mathbb{R}^n/\mathcal{L}}(u, v) \leq \mu(\mathcal{L})$.

Let $1 \leq i \leq k$ be the index that satisfies $s_i < \frac{\text{dist}_{\mathbb{R}^n/\mathcal{L}}(u,v)}{2\sqrt{n}} \leq 2 \cdot s_i = s_{i+1}$. This index exists due to our choice of k . So $\text{dist}_{\mathbb{R}^n/\mathcal{L}}(u, v) = \text{dist}(u-v, \mathcal{L}) > 2s_i \cdot \sqrt{n}$. Hence, by Item 1 of Lemma 3.2, we have $h_{\mathcal{L},s_i}(u-v) \geq 1 - 2^{-11n}$ and we get that

$$A_i(u, v) \geq (1 - 2^{-11n}) \cdot \frac{s_i^2}{\text{dist}_{\mathbb{R}^n/\mathcal{L}}^2(u, v)} \geq \frac{1 - 2^{-11n}}{16n}.$$

■

In the following two corollaries we observe that our bounds are nearly tight for certain families of lattices. The first follows immediately by combining Theorems 1.5 and 5.2.

Corollary 5.3. *Let \mathcal{L} be an n -dimensional lattice such that $\lambda_1(\mathcal{L}), \mu(\mathcal{L})$ are equal up to a multiplicative constant and $\lambda_1(\mathcal{L}^*) \cdot \mu(\mathcal{L}) \geq \Omega(n)$. Then, $c_2(\mathbb{R}^n/\mathcal{L}) = \Theta(\sqrt{n})$.*

Corollary 5.4. *Let \mathcal{L} be an n -dimensional lattice such that $\lambda_1(\mathcal{L}^*)$ and $\mu(\mathcal{L}^*)$ are equal up to a multiplicative constant. Then, $\Omega(\sqrt{n}) \leq c_2(\mathbb{R}^n/\mathcal{L}) \leq O(\sqrt{n \log n})$.*

Proof: By Theorem 1.1, $c_2(\mathbb{R}^n/\mathcal{L}) \geq \Omega(\sqrt{n})$. For the upper bound notice that Theorem 2.2 implies that

$$\frac{\mu(\mathcal{L})}{\lambda_1(\mathcal{L})} \leq \frac{n \cdot \mu(\mathcal{L}^*)}{\lambda_1(\mathcal{L}^*)} \leq O(n),$$

and apply Theorem 1.4 to get $c_2(\mathbb{R}^n/\mathcal{L}) \leq O(\sqrt{n \log n})$. ■

5.2 General Upper Bound

In this section we prove an upper bound on $c_2(\mathbb{R}^n/\mathcal{L})$ that depends only on n and is almost linear. Before presenting the proof let us start with some intuition. Notice that using the tools presented in Section 3 we have an embedding that works well for distances at most $\lambda_1(\mathcal{L})$ (Item 2 of Lemma 3.1) and an embedding that works for specific distances (Lemma 3.2). Consider a Korkine-Zolotarev basis and the projections that it defines: the lattice $\mathcal{L}_i = \pi_i(\mathcal{L})$ is the lattice \mathcal{L} projected to $\text{span}(\tilde{b}_i, \dots, \tilde{b}_n)$. We think of \mathcal{L}_i as a full-rank lattice inside an $(n - i + 1)$ -dimensional space. Our embedding consists of n Gaussian functions where the i th function corresponds to the lattice \mathcal{L}_i . Due to the use of a Korkine-Zolotarev basis using Item 2 of Lemma 3.1 we can show that the i th Gaussian function handles distances that are both somewhat larger than $\lambda_{i-1}(\mathcal{L})$ and somewhat smaller than $\lambda_i(\mathcal{L})$. In order to treat distances around the $\lambda_i(\mathcal{L})$'s we add additional $O(\log n)$ Gaussian functions for every i and use Lemma 3.2 to prove correctness.

We restate and prove Theorem 1.3.

Theorem 1.3. *For any $n \geq 1$ and an n -dimensional lattice \mathcal{L} , $c_2(\mathbb{R}^n/\mathcal{L}) = O(n \cdot \sqrt{\log n})$.*

Proof: Let \mathcal{L} be an n -dimensional lattice generated by a Korkine-Zolotarev basis B . For $1 \leq i \leq n$ let $\pi_i = \pi_i^{(B)}$ be the corresponding orthogonal projection function that maps vectors to the orthogonal complement of $\text{span}(b_1, \dots, b_{i-1})$. Denote $\mathcal{L}_i = \pi_i(\mathcal{L})$, $n_i = n - i + 1$, $s_i = \frac{\lambda_i(\mathcal{L})}{4n}$, $k = \lceil \frac{1}{2} \cdot (5 + 3 \log n) \rceil$ and $r_{i,j} = 2^{j-1} \cdot \frac{\lambda_i(\mathcal{L})}{8n\sqrt{2n}}$ for $1 \leq j \leq k$. Consider the embedding $H_{\mathcal{L}}$ that maps $u \in \mathbb{R}^n/\mathcal{L}$ to the vector of $n + nk = O(n \log n)$ functions

$$(H_{\mathcal{L}_1, s_1}(\pi_1(u)), H_{\mathcal{L}_2, s_2}(\pi_2(u)), \dots, H_{\mathcal{L}_n, s_n}(\pi_n(u)), H_{\mathcal{L}, r_{1,1}}^{(k)}(u), H_{\mathcal{L}, r_{2,1}}^{(k)}(u), \dots, H_{\mathcal{L}, r_{n,1}}^{(k)}(u)).$$

This is an element in the space $L_2 = L_2(\mathbb{R}^{n_1}/\mathcal{L}_1) \oplus \dots \oplus L_2(\mathbb{R}^{n_n}/\mathcal{L}_n) \oplus L_2(\mathbb{R}^n/\mathcal{L})^{nk}$.

Fix distinct $u, v \in \mathbb{R}^n/\mathcal{L}$. By Proposition 5.1,

$$\frac{\text{dist}_{L_2}(H_{\mathcal{L}}(u), H_{\mathcal{L}}(v))^2}{\text{dist}_{\mathbb{R}^n/\mathcal{L}}(u, v)^2} = \sum_{i=1}^n A_i(u, v) + \sum_{1 \leq i \leq n, 1 \leq j \leq k} B_{i,j}(u, v),$$

where

$$A_i(u, v) = \frac{s_i^2 \cdot h_{\mathcal{L}_i, s_i}(\pi_i(u) - \pi_i(v))}{\text{dist}_{\mathbb{R}^n/\mathcal{L}}(u, v)^2},$$

$$B_{i,j}(u, v) = \frac{r_{i,j}^2 \cdot h_{\mathcal{L}, r_{i,j}}(u - v)}{\text{dist}_{\mathbb{R}^n/\mathcal{L}}(u, v)^2}.$$

We will show that

$$\Omega\left(\frac{1}{n}\right) \leq \sum_{i=1}^n A_i(u, v) + \sum_{1 \leq i \leq n, 1 \leq j \leq k} B_{i,j}(u, v) \leq O(n \log n), \quad (2)$$

which implies that our embedding has distortion $O(n \cdot \sqrt{\log n})$, as required.

By Item 1 of Lemma 3.1, for every $1 \leq i \leq n$ and $1 \leq j \leq k$ we have

$$\begin{aligned} A_i(u, v) &\leq \frac{\text{dist}_{\mathbb{R}^{n_i}/\mathcal{L}_i}(\pi_i(u), \pi_i(v))^2}{\text{dist}_{\mathbb{R}^n/\mathcal{L}}(u, v)^2} \cdot s_i^2 \cdot \frac{\pi}{s_i^2} \leq \pi, \\ B_{i,j}(u, v) &\leq r_{i,j}^2 \cdot \frac{\pi}{r_{i,j}^2} = \pi, \end{aligned}$$

where for the bound on $A_i(u, v)$ we use the upper bound from Lemma 4.2 applied to $u - v$. This yields the upper bound in (2). In order to prove the lower bound in (2) we now show that there exists an i such that $A_i(u, v) \geq \Omega(\frac{1}{n})$ or there exist i, j such that $B_{i,j}(u, v) \geq \Omega(\frac{1}{n})$. Since $\text{dist}_{\mathbb{R}^n/\mathcal{L}}(u, v) = \text{dist}(u - v, \mathcal{L}) \leq \mu(\mathcal{L}) \leq \frac{\sqrt{n}}{2} \cdot \lambda_n(\mathcal{L})$ the vectors u and v correspond to one of the following two cases:

- Case 1: There exists an i such that $\frac{\sqrt{n}}{2} \cdot \lambda_{i-1}(\mathcal{L}) < \text{dist}_{\mathbb{R}^n/\mathcal{L}}(u, v) \leq \frac{1}{4\sqrt{2} \cdot n} \cdot \lambda_i(\mathcal{L})$.

Think of \mathcal{L}_i as a full-rank n_i -dimensional lattice, and use Lemma 2.5 to obtain for $\varepsilon_i = 2^{-10n_i} \leq \frac{1}{1000}$ that

$$\eta_{\varepsilon_i}(\mathcal{L}_i^*)^2 \leq \frac{4n_i}{\lambda_1(\mathcal{L}_i)^2} \leq \frac{4n_i}{\frac{4}{i+3} \cdot \lambda_i(\mathcal{L})^2 - \frac{i-1}{4} \cdot \lambda_{i-1}(\mathcal{L})^2} \leq \frac{4n^2}{\lambda_i(\mathcal{L})^2},$$

where the second inequality follows from Lemma 4.1 and the third from a straightforward calculation. This yields that $2 \cdot \eta_{\varepsilon_i}(\mathcal{L}_i^*) \leq \frac{4n}{\lambda_i(\mathcal{L})} = \frac{1}{s_i}$, so we get that

$$A_i(u, v) \geq s_i^2 \cdot \frac{\text{dist}_{\mathbb{R}^{n_i}/\mathcal{L}_i}(\pi_i(u), \pi_i(v))^2}{\text{dist}_{\mathbb{R}^n/\mathcal{L}}(u, v)^2} \cdot \frac{c}{s_i^2} \geq c \cdot \left(1 - \frac{i-1}{4} \cdot \frac{\lambda_{i-1}(\mathcal{L})^2}{\text{dist}_{\mathbb{R}^n/\mathcal{L}}(u, v)^2}\right) \geq \frac{c}{n},$$

where the first inequality follows from Item 2 of Lemma 3.1, the second follows from Lemma 4.2 applied to $u - v$, and the third from the assumption that $\frac{\sqrt{n}}{2} \cdot \lambda_{i-1}(\mathcal{L}) < \text{dist}_{\mathbb{R}^n/\mathcal{L}}(u, v)$.

- Case 2: There exists an i such that $\frac{1}{4\sqrt{2} \cdot n} \cdot \lambda_i(\mathcal{L}) < \text{dist}_{\mathbb{R}^n/\mathcal{L}}(u, v) \leq \frac{\sqrt{n}}{2} \cdot \lambda_i(\mathcal{L})$.

Let $1 \leq j \leq k$ be the index that satisfies $r_{i,j} < \frac{\text{dist}_{\mathbb{R}^n/\mathcal{L}}(u, v)}{2\sqrt{n}} \leq 2 \cdot r_{i,j} = r_{i,j+1}$. This index exists due to our choice of k . So $\text{dist}_{\mathbb{R}^n/\mathcal{L}}(u, v) = \text{dist}(u - v, \mathcal{L}) > 2r_{i,j} \cdot \sqrt{n}$. Hence, by Item 1 of Lemma 3.2, we have $h_{\mathcal{L}, r_{i,j}}(u - v) \geq 1 - 2^{-11n}$ and we get that

$$B_{i,j}(u, v) \geq (1 - 2^{-11n}) \cdot \frac{r_{i,j}^2}{\text{dist}_{\mathbb{R}^n/\mathcal{L}}^2(u, v)} \geq \frac{1 - 2^{-11n}}{16n}.$$

■

6 Lower Bound

In this section we slightly improve the lower bound on the Euclidean distortion of a torus \mathbb{R}^n/\mathcal{L} in terms of lattice parameters of \mathcal{L} . The following claim lower bounds the expected squared distance between two uniformly chosen points in \mathbb{R}^n/\mathcal{L} . Note that all the integrals below are with respect to the *normalized* Riemannian volume measure on the torus.

Claim 6.1. For any $n \geq 1$ and an n -dimensional lattice \mathcal{L} ,

$$\int_{\mathbb{R}^n/\mathcal{L} \times \mathbb{R}^n/\mathcal{L}} \text{dist}_{\mathbb{R}^n/\mathcal{L}}(x, y)^2 dx dy \geq \frac{\mu(\mathcal{L})^2}{8}.$$

Proof: It is known (see e.g., [7]) that for any fixed $x \in \mathbb{R}^n/\mathcal{L}$, the probability that a uniformly chosen $y \in \mathbb{R}^n/\mathcal{L}$ satisfies $\text{dist}_{\mathbb{R}^n/\mathcal{L}}(x, y) \geq \frac{\mu(\mathcal{L})}{2}$ is at least $\frac{1}{2}$. To see this, let $u \in \mathbb{R}^n/\mathcal{L}$ be a point such that $\text{dist}_{\mathbb{R}^n/\mathcal{L}}(u, 0) = \mu(\mathcal{L})$, and observe that for any $x, y \in \mathbb{R}^n/\mathcal{L}$ at least one of y and $y + u$ is $\frac{\mu(\mathcal{L})}{2}$ -far from x . This gives us a bound of $\frac{1}{2} \cdot \left(\frac{\mu(\mathcal{L})}{2}\right)^2$ on the integral above, as required. ■

Note that the bound in the claim is tight up to a multiplicative constant since for all $x, y \in \mathbb{R}^n/\mathcal{L}$, $\text{dist}_{\mathbb{R}^n/\mathcal{L}}(x, y)$ is bounded from above by $\mu(\mathcal{L})$.

Now we restate and prove Theorem 1.5. The proof is identical to that in [8] except for the use of Claim 6.1, and is included for completeness.

Theorem 1.5. For any $n \geq 1$ and an n -dimensional lattice \mathcal{L} , $c_2(\mathbb{R}^n/\mathcal{L}) \geq \frac{\lambda_1(\mathcal{L}^*) \cdot \mu(\mathcal{L})}{4\sqrt{n}}$.

Proof: Let $f : \mathbb{R}^n/\mathcal{L} \rightarrow L_2$ be an embedding of \mathbb{R}^n/\mathcal{L} into a Hilbert space. This implies that f is differentiable almost everywhere (see [5]). By Parseval's Theorem we get

$$\|f\|_{\text{Lip}}^2 \geq \frac{1}{n} \sum_{j=1}^n \int_{\mathbb{R}^n/\mathcal{L}} \left\| \frac{\partial f}{\partial x_j}(x) \right\|_{L_2}^2 dx = \frac{1}{n} \sum_{x \in \mathcal{L}^*} \|\hat{f}(x)\|_{L_2}^2 \cdot \|x\|^2 \geq \frac{\lambda_1(\mathcal{L}^*)^2}{n} \cdot \sum_{x \in \mathcal{L}^* \setminus \{0\}} \|\hat{f}(x)\|_{L_2}^2.$$

Use Parseval's Theorem again to observe that

$$\begin{aligned} \sum_{x \in \mathcal{L}^* \setminus \{0\}} \|\hat{f}(x)\|_{L_2}^2 &= \int_{\mathbb{R}^n/\mathcal{L}} \|f(x)\|_{L_2}^2 dx - \|\hat{f}(0)\|_{L_2}^2 \\ &= \int_{\mathbb{R}^n/\mathcal{L}} \|f(x)\|_{L_2}^2 dx - \int_{\mathbb{R}^n/\mathcal{L} \times \mathbb{R}^n/\mathcal{L}} \langle f(x), f(y) \rangle_{L_2} dx dy \\ &= \frac{1}{2} \cdot \int_{\mathbb{R}^n/\mathcal{L} \times \mathbb{R}^n/\mathcal{L}} \|f(x) - f(y)\|_{L_2}^2 dx dy. \end{aligned}$$

By Claim 6.1,

$$\|f^{-1}\|_{\text{Lip}}^2 \geq \frac{\int_{\mathbb{R}^n/\mathcal{L} \times \mathbb{R}^n/\mathcal{L}} \text{dist}_{\mathbb{R}^n/\mathcal{L}}(x, y)^2 dx dy}{\int_{\mathbb{R}^n/\mathcal{L} \times \mathbb{R}^n/\mathcal{L}} \|f(x) - f(y)\|_{L_2}^2 dx dy} \geq \frac{\mu(\mathcal{L})^2}{8 \int_{\mathbb{R}^n/\mathcal{L} \times \mathbb{R}^n/\mathcal{L}} \|f(x) - f(y)\|_{L_2}^2 dx dy}.$$

It follows that $\text{distortion}(f)^2 = \|f\|_{\text{Lip}}^2 \cdot \|f^{-1}\|_{\text{Lip}}^2 \geq \frac{\lambda_1(\mathcal{L}^*)^2 \cdot \mu(\mathcal{L})^2}{16n}$, and we are done. ■

Remark 6.2. For any lattice \mathcal{L} , $\mu(\mathcal{L}) = \Omega(\sqrt{n} \cdot \det(\mathcal{L})^{1/n})$, as follows from the fact that a Voronoi cell of \mathcal{L} has volume $\det(\mathcal{L})$ and is contained in a ball with radius $\mu(\mathcal{L})$. This implies that for any lattice \mathcal{L} , $\mu(\mathcal{L}) \cdot \mu(\mathcal{L}^*) \geq \Omega(n)$, and hence Theorem 1.5 is a strengthening of Theorem 1.1.

Remark 6.3. It is not difficult to use the techniques of [8] and a variant of Claim 6.1 to derive the stronger statement $c_1(\mathbb{R}^n/\mathcal{L}) = \Omega\left(\frac{\lambda_1(\mathcal{L}^*) \cdot \mu(\mathcal{L})}{\sqrt{n}}\right)$ for any n -dimensional lattice \mathcal{L} .

7 On the Embedding of Khot and Naor

In this section we collect some observations regarding the exact performance achieved by the embedding of Khot and Naor [8] from the proof of Theorem 1.2. Details follow. For a full-rank lattice $\mathcal{L} \subseteq \mathbb{R}^n$ let $\{b_1, \dots, b_n\}$ be a Korkine-Zolotarev basis that generates \mathcal{L} . The embedding from [8] maps every point $x = \sum_{i=1}^n x_i b_i$ to the point

$$(\|b_1\| \cos 2\pi x_1, \|b_1\| \sin 2\pi x_1, \dots, \|b_n\| \cos 2\pi x_n, \|b_n\| \sin 2\pi x_n) \in \mathbb{R}^{2n}.$$

Khot and Naor show that up to a multiplicative constant the squared distortion of this embedding is the maximum of

$$\frac{\sum_{i=1}^n |x_i - \lceil x_i \rceil|^2 \|b_i\|^2}{\text{dist}(x, \mathcal{L})^2} \quad (3)$$

taken over all vectors $x = \sum_{i=1}^n x_i b_i$. They showed an upper bound of $O(n^{3n/2})$ and we ask here if a smaller upper bound can be shown.

Recently, Ajtai showed that for every large enough n there exists an n -dimensional lattice \mathcal{L} and a Korkine-Zolotarev basis $\{b_1, \dots, b_n\}$ of \mathcal{L} such that $\frac{\|b_1\|^2}{\|b_n\|^2} \geq n^{\Omega(\log n)}$ [2, Theorem 1.9, Definition 3.3]. For $x = \frac{1}{2}\tilde{b}_n = \sum_{i=1}^n x_i b_i$, it follows that $x_n = \frac{1}{2}$ and therefore (3) is at least

$$\frac{\|b_n\|^2}{4 \text{dist}(x, \mathcal{L})^2} \geq \frac{\|b_1\|^2}{\|\tilde{b}_n\|^2} \geq n^{\Omega(\log n)}.$$

This shows that for these lattices the embedding of Khot and Naor has distortion at least $n^{\Omega(\log n)}$. It would be interesting to see whether this is tight or not. It would also be interesting to see whether there are lattices for which for *any* basis that generates it (not necessarily a Korkine-Zolotarev one) the embedding from above has distortion at least, say, super-polynomial.

The maximum of (3) seems relevant to understanding the approximation factor achieved by the “round-off” algorithm of Babai [3] for the Closest Vector Problem where a Korkine-Zolotarev basis is used. This algorithm simply expresses the target vector as a linear combination of the vectors in the Korkine-Zolotarev basis and rounds each coefficient to an integer closest to it. An improved upper bound on the maximum of (3) can be useful for an algorithm for the *search* version of the Closest Vector Problem with Preprocessing (see [6]).

References

- [1] D. Aharonov and O. Regev. Lattice problems in NP intersect coNP. *Journal of the ACM*, 52(5):749–765, 2005. Preliminary version in FOCS’04.
- [2] M. Ajtai. Optimal lower bounds for the Korkine-Zolotareff parameters of a lattice and for Schnorr’s algorithm for the shortest vector problem. *Theory of Computing*, 4(1):21–51, 2008.
- [3] L. Babai. On Lovász lattice reduction and the nearest lattice point problem. *Combinatorica*, 6(1):1–13, 1986.
- [4] W. Banaszczyk. New bounds in some transference theorems in the geometry of numbers. *Mathematische Annalen*, 296(4):625–635, 1993.

- [5] Y. Benyamini and J. Lindenstrauss. *Geometric nonlinear functional analysis. Vol. 1*, volume 48 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2000.
- [6] U. Feige and D. Micciancio. The inapproximability of lattice and coding problems with preprocessing. *J. Comput. System Sci.*, 69(1):45–67, 2004.
- [7] V. Guruswami, D. Micciancio, and O. Regev. The complexity of the covering radius problem on lattices and codes. *Computational Complexity*, 14(2):90–121, 2005. Preliminary version in CCC’04.
- [8] S. Khot and A. Naor. Nonembeddability theorems via Fourier analysis. *Mathematische Annalen*, 334(4):821–852, 2006. Preliminary version in FOCS’05.
- [9] A. Korkine and G. Zolotareff. Sur les formes quadratiques. *Mathematische Annalen*, 6:366–389, 1873.
- [10] J. C. Lagarias, H. W. Lenstra, Jr., and C.-P. Schnorr. Korkin-Zolotarev bases and successive minima of a lattice and its reciprocal lattice. *Combinatorica*, 10(4):333–348, 1990.
- [11] D. Micciancio and S. Goldwasser. *Complexity of Lattice Problems: A Cryptographic Perspective*, volume 671 of *The Kluwer International Series in Engineering and Computer Science*. Kluwer Academic Publishers, Boston, MA, 2002.
- [12] D. Micciancio and O. Regev. Worst-case to average-case reductions based on Gaussian measures. *SIAM Journal on Computing*, 37(1):267–302, 2007.
- [13] D. Micciancio and P. Voulgaris. A deterministic single exponential time algorithm for most lattice problems based on voronoi cell computations. In STOC 2010.
- [14] J. Milnor and D. Husemoller. *Symmetric bilinear forms*. Springer-Verlag, Berlin, 1973.