Nearly Optimal Embeddings of Flat Tori

Ishan Agarwal
Courant Institute of Mathematical Sciences, New York University, USA
ia1020@nyu.edu

Oded Regev
Courant Institute of Mathematical Sciences, New York University, USA

Yi Tang
Courant Institute of Mathematical Sciences, New York University, USA
yt1433@nyu.edu

Abstract

We show that for any n-dimensional lattice $\mathcal{L} \subseteq \mathbb{R}^n$, the torus $\mathbb{R}^n/\mathcal{L}$ can be embedded into Hilbert space with $O(\sqrt{n \log n})$ distortion. This improves the previously best known upper bound of $O(n\sqrt{\log n})$ shown by Haviv and Regev (APPROX 2010, J. Topol. Anal. 2013) and approaches the lower bound of $\Omega(\sqrt{n})$ due to Khot and Naor (FOCS 2005, Math. Ann. 2006).

2012 ACM Subject Classification Mathematics of computing → Discrete mathematics

Keywords and phrases Lattices, metric embeddings, flat torus

Digital Object Identifier 10.4230/LIPIcs.APPROX/RANDOM.2020.43

Funding *Ishan Agarwal*: Research supported by National Science Foundation (NSF) under Grant No. CCF-1814524.
Oded Regev: Research supported by the Simons Collaboration on Algorithms and Geometry, a Simons Investigator Award, and by the National Science Foundation (NSF) under Grant No. CCF-1814524.

1 Introduction

Low distortion embeddings play an important role in many approximation algorithms, allowing one to map points in a "difficult" metric space into another simpler metric space (such as Hilbert space), in a way that approximately preserves distances. See the survey by Indyk [2] for many examples of algorithmic applications. One interesting family of difficult metric spaces is given by *flat tori*. These are defined as quotients of Euclidean space by a lattice, and play an important role in lattice problems and algorithms.

In more detail, an n-dimensional lattice $\mathcal{L} \subseteq \mathbb{R}^n$ is defined as the set of all integer linear combinations of some n linearly independent vectors in $\mathbb{R}^n$. The torus $\mathbb{R}^n/\mathcal{L}$ is the quotient space obtained by identifying points in $\mathbb{R}^n$ with each other if their difference is a lattice vector. The torus has a natural metric associated to it; namely, the distance between any two elements of the torus is defined as the minimum distance between any representative of these elements. So for instance, in the one-dimensional case $\mathbb{R}/\mathbb{Z}$, the distance between 0.1 and 0.9 is 0.2.

Khot and Naor [3] considered the question of how well one can embed flat tori $\mathbb{R}^n/\mathcal{L}$ into Hilbert space. They proved that for any $\mathcal{L}$ and any embedding of $\mathbb{R}^n/\mathcal{L}$ into Hilbert space, the distortion must be at least $\Omega(\frac{\lambda_1(\mathcal{L}^*)}{\mu(\mathcal{L}^*)}\sqrt{n})$. Here, $\mathcal{L}^*$ is the dual lattice of $\mathcal{L}$ and $\lambda_1(\mathcal{L})$ and $\mu(\mathcal{L})$ represent the length of the shortest nonzero vector and the covering radius of $\mathcal{L}$ respectively. It is known by a result of Conway and Thompson (see [4, Page 46]) that, for large enough n, there exist lattices $\mathcal{L}$ where $\lambda_1(\mathcal{L}) = \mu(\mathcal{L})$. Thus the lower bound of Khot and Naor shows that there are n-dimensional lattices whose torus requires distortion $\Omega(\sqrt{n})$ in any embedding into Hilbert space. In the same paper, they also present an embedding that achieves a distortion of $O(n^{3n/2})$ for any lattice $\mathcal{L}$. While the distortion of

their embedding might be better than this upper bound, it is known that for some lattices it is super-polynomial [1, Section 7].

In [1] an $O(n\sqrt{\log n})$ distortion metric embedding is constructed, significantly reducing the gap between the upper and lower bounds. They also provide an alternative upper bound of $O(\sqrt{n \log(\mu(\mathcal{L})/\lambda_1(\mathcal{L}))})$. For lattices with good geometric structure (specifically, where the ratio $\mu(\mathcal{L})/\lambda_1(\mathcal{L})$ is only polynomial) this gives an $O(\sqrt{n \log n})$ upper bound. However, in general, the ratio $\mu(\mathcal{L})/\lambda_1(\mathcal{L})$ can be arbitrarily big, in which case this alternative bound is not useful.

Our result is a nearly tight embedding of flat tori, essentially resolving the question of Khot and Naor up to a $\sqrt{\log n}$ factor.

▶ **Theorem 1.1.** *For any lattice $\mathcal{L} \subseteq \mathbb{R}^n$ there exists a metric embedding of $\mathbb{R}^n/\mathcal{L}$ into Hilbert space with distortion $O(\sqrt{n \log n})$.*

1.1 Proof Overview

Our starting point is the embedding by Haviv and Regev [1], which is based on Gaussian measures. Their embedding achieves a distortion of $O(\sqrt{n \log n})$ assuming that the lattice $\mathcal{L}$ has poly(n) "aspect ratio," i.e., the ratio between $\mu(\mathcal{L})$ (the diameter of the torus, or equivalently, the covering radius of the lattice) and $\lambda_1(\mathcal{L})$ (the length of the shortest nonzero vector in the lattice) is polynomial in the dimension n. Their embedding can also be applied to arbitrary lattices; the only issue is that it "saturates" at distance poly$(n)\lambda_1(\mathcal{L})$ — points at greater distance will be contracted by the embedding. See Section 3 for the details.

A natural way to address this issue is to first partition the lattice into scales, and to then embed each scale separately. Specifically, one can define a filtration of sublattices $\{\mathbf{0}\} = \mathcal{L}_0 \subset \mathcal{L}_1 \subset \cdots \subset \mathcal{L}_m = \mathcal{L}$ with each $\mathcal{L}_j$ capturing a different scale of the lattice. Then, for each $j = 1, \ldots, m$, we project the torus on the space orthogonal to $\mathcal{L}_{j-1}$, and embed each projection in Hilbert space separately. Our embedding is then the direct sum of the m individual embeddings.

This approach does work, and is used as part of the construction in [1]. The difficulty is that it introduces an additional $\sqrt{m}$ loss in the distortion, which at worst can be $O(\sqrt{n})$ and is the reason they only achieved an overall distortion of $O(n\sqrt{\log n})$. To see where this loss comes from, consider a short vector inside the span of $\mathcal{L}_1$; this vector only contributes to the first embedding (because it becomes zero in the other $m-1$ projections). On the other hand, a short vector orthogonal to $\mathcal{L}_{m-1}$ gets accounted for in all m projections, leading to an expansion of $\sqrt{m}$ (the square root due to the L_2 norm in the target Hilbert space).

In order to avoid this loss and achieve a $O(\sqrt{n \log n})$ distortion, it is tempting to decompose space into *orthogonal* subspaces (and not nested subspaces as in the above). So instead of projecting on the subspace orthogonal to $\mathcal{L}_{j-1}$, we would like to only project on the subspace of $\mathcal{L}_j$ that is orthogonal to $\mathcal{L}_{j-1}$ (i.e., on the span of $\mathcal{L}_j/\mathcal{L}_{j-1}$). This, however, is impossible; projecting a lattice in such a way in general gives a dense set, and not a lattice.[1]

Our novel contribution is to replace this "harsh" two-sided projection (which is in general impossible) by a more gentle "compressed projection." Namely, we first project orthogonally to $\mathcal{L}_{j-1}$, and then *scale down* the subspace orthogonal to $\mathcal{L}_j$. Returning to the example above, a short vector orthogonal to $\mathcal{L}_{m-1}$ is still accounted for in all m "compressed projections," but the scaling factors are such that its contributions form a geometric series, so the overall

[1] To see why, consider the two-dimensional lattice generated by $(1, 0)$ and $(\pi, 1)$; its projection on the first coordinate is a dense set.

expansion is only a constant instead of $\sqrt{m}$. The technical effort is in showing that these compressions do not distort the geometry by too much; see Section 4 for details. We remark that this "compressed projection" idea might find applications in other cases where decomposing a lattice into scales is desirable.

2 Preliminaries

2.1 Embeddings and Distortion

A metric space is a tuple $(\mathcal{M}, \mathrm{dist}_{\mathcal{M}})$ where $\mathcal{M}$ is a set and $\mathrm{dist}_{\mathcal{M}} : \mathcal{M} \times \mathcal{M} \to \mathbb{R}$ is a function such that the following hold for all $x, y, z \in \mathcal{M}$:

- $\mathrm{dist}_{\mathcal{M}}(x, y) \geq 0$, and the equality holds if and only if $x = y$,
- $\mathrm{dist}_{\mathcal{M}}(x, y) = \mathrm{dist}_{\mathcal{M}}(y, x)$,
- $\mathrm{dist}_{\mathcal{M}}(x, y) + \mathrm{dist}_{\mathcal{M}}(y, z) \geq \mathrm{dist}_{\mathcal{M}}(x, z)$.

For simplicity, we often write metric space $\mathcal{M}$ for $(\mathcal{M}, \mathrm{dist}_{\mathcal{M}})$. We also use dist without the subscript to represent the standard Euclidean metric over $\mathbb{R}^n$ (for some n that is clear from the context). A (metric) embedding is a mapping from one metric space to another.

▶ **Definition 2.1.** *Suppose $F : \mathcal{M}_1 \to \mathcal{M}_2$ is an embedding of metric space $\mathcal{M}_1$ into $\mathcal{M}_2$. The distortion of F is defined by*

$$\inf\left\{ \frac{c_u}{c_l} : \forall x, y \in \mathcal{M}_1,\ c_l \cdot \mathrm{dist}_{\mathcal{M}_1}(x, y) \leq \mathrm{dist}_{\mathcal{M}_2}(F(x), F(y)) \leq c_u \cdot \mathrm{dist}_{\mathcal{M}_1}(x, y) \right\} .$$

2.2 Lattices

We now recall some standard definitions and notations regarding lattices. A (full-rank) *lattice* $\mathcal{L} \subseteq \mathbb{R}^n$ is the set of all integer linear combinations of n linearly independent vectors. This set of vectors is called a *basis* of the lattice. Equivalently, a lattice is a discrete subgroup of the additive group $\mathbb{R}^n$. The *dual lattice* $\mathcal{L}^*$ of $\mathcal{L}$ is defined as the set of all vectors $y \in \mathrm{span}(\mathcal{L})$ such that $\langle x, y \rangle$ is an integer for all vectors $x \in \mathcal{L}$. A *sublattice* $\mathcal{L}' \subseteq \mathcal{L}$ is an additive subgroup of $\mathcal{L}$. We say that a sublattice $\mathcal{L}' \subseteq \mathcal{L}$ is *primitive* if $\mathcal{L}' = \mathcal{L} \cap \mathrm{span}(\mathcal{L}')$. All sublattices in this paper will be primitive. For a lattice $\mathcal{L}$ and a primitive sublattice $\mathcal{L}' \subseteq \mathcal{L}$, the *quotient lattice* $\mathcal{L}/\mathcal{L}'$ is defined as the projection of $\mathcal{L}$ onto the subspace orthogonal to $\mathrm{span}(\mathcal{L}')$. Sublattices and quotient lattices can be thought of as full rank while sitting inside some lower-dimensional space. For lattice $\mathcal{L} \subseteq \mathbb{R}^n$, the *torus* $\mathbb{R}^n/\mathcal{L}$ is naturally associated with the quotient metric, defined as

$$\mathrm{dist}_{\mathbb{R}^n/\mathcal{L}}(\mathbf{x}, \mathbf{y}) = \mathrm{dist}(\mathbf{x} - \mathbf{y}, \mathcal{L}) = \min_{\mathbf{v} \in \mathcal{L}} \mathrm{dist}(\mathbf{x} - \mathbf{y}, \mathbf{v}) .$$

The *length of the shortest vector* of a lattice $\mathcal{L}$, denoted by $\lambda_1(\mathcal{L})$, is defined as the minimum length of a non-zero vector in $\mathcal{L}$. Note that here and elsewhere, length refers to the Euclidean norm. The *covering radius* of a lattice $\mathcal{L}$, denoted by $\mu(\mathcal{L})$, is defined as the maximum (Euclidean) distance from any vector in $\mathrm{span}(\mathcal{L})$ to $\mathcal{L}$. Equivalently, as its name suggests, it is the minimum radius such that balls of that radius centered at all lattice points cover the entire $\mathrm{span}(\mathcal{L})$.

We end with two simple technical lemmas, where we denote by π_V the orthogonal projection onto subspace V.

▶ **Lemma 2.2.** *For any $n \geq 1$, lattice $\mathcal{L} \subseteq \mathbb{R}^n$, vectors $\mathbf{x} \in \mathbb{R}^n$, $\mathbf{v} \in \mathcal{L}$ such that $\|\mathbf{x} - \mathbf{v}\| = \mathrm{dist}(\mathbf{x}, \mathcal{L})$, and sublattice $\mathcal{L}' \subseteq \mathcal{L}$,*

$$\|\pi_{\mathrm{span}(\mathcal{L}')}(\mathbf{x} - \mathbf{v})\| \leq \mu(\mathcal{L}') .$$

Proof. Suppose towards contradiction that $\|\pi_{\mathrm{span}(\mathcal{L}')}(\mathbf{x}-\mathbf{v})\| > \mu(\mathcal{L}')$. Then consider the lattice point $\mathbf{u} \in \mathcal{L}'$ that is a closest lattice point to $\pi_{\mathrm{span}(\mathcal{L}')}(\mathbf{x}-\mathbf{v})$ in $\mathcal{L}'$. By definition $\|\pi_{\mathrm{span}(\mathcal{L}')}(\mathbf{x}-\mathbf{v})-\mathbf{u}\| \le \mu(\mathcal{L}')$. Observe that

$$\begin{aligned}\|\mathbf{x}-(\mathbf{v}+\mathbf{u})\|^2 &= \|\pi_{\mathrm{span}(\mathcal{L}')}(\mathbf{x}-\mathbf{v}-\mathbf{u})\|^2 + \|\pi_{\mathrm{span}(\mathcal{L}/\mathcal{L}')}(\mathbf{x}-\mathbf{v}-\mathbf{u})\|^2 \\ &= \|\pi_{\mathrm{span}(\mathcal{L}')}(\mathbf{x}-\mathbf{v})-\mathbf{u}\|^2 + \|\pi_{\mathrm{span}(\mathcal{L}/\mathcal{L}')}(\mathbf{x}-\mathbf{v})\|^2 \\ &< \|\pi_{\mathrm{span}(\mathcal{L}')}(\mathbf{x}-\mathbf{v})\|^2 + \|\pi_{\mathrm{span}(\mathcal{L}/\mathcal{L}')}(\mathbf{x}-\mathbf{v})\|^2 \\ &= \|\mathbf{x}-\mathbf{v}\|^2 ,\end{aligned}$$

which contradicts with the fact that $\|\mathbf{x}-\mathbf{v}\| = \mathrm{dist}(\mathbf{x},\mathcal{L}) = \min_{\mathbf{v}'\in\mathcal{L}} \|\mathbf{x}-\mathbf{v}'\|$. ◀

▶ **Lemma 2.3.** *For any lattice $\mathcal{L}$ and sublattice $\mathcal{L}' \subseteq \mathcal{L}$,*

$$\mu(\mathcal{L})^2 \le \mu(\mathcal{L}')^2 + \mu(\mathcal{L}/\mathcal{L}')^2 .$$

Proof. For any $\mathbf{x} \in \mathrm{span}(\mathcal{L})$, let $\mathbf{v} \in \mathcal{L}$ be a lattice point such that

$$\|\pi_{\mathrm{span}(\mathcal{L}/\mathcal{L}')}(\mathbf{x}-\mathbf{v})\| = \mathrm{dist}(\pi_{\mathrm{span}(\mathcal{L}/\mathcal{L}')}(\mathbf{x}), \mathcal{L}/\mathcal{L}') .$$

Without loss of generality it can be assumed that $\|\pi_{\mathrm{span}(\mathcal{L}')}(\mathbf{x}-\mathbf{v})\| \le \mu(\mathcal{L}')$ (since otherwise, we can use $\mathbf{v}+\mathbf{u}$ instead of $\mathbf{v}$, where $\mathbf{u}$ is a closest lattice point to $\pi_{\mathrm{span}(\mathcal{L}')}(\mathbf{x}-\mathbf{v})$ in $\mathcal{L}'$). Then

$$\begin{aligned}\mathrm{dist}(\mathbf{x},\mathcal{L})^2 &\le \|\mathbf{x}-\mathbf{v}\|^2 \\ &= \|\pi_{\mathrm{span}(\mathcal{L}')}(\mathbf{x}-\mathbf{v})\|^2 + \|\pi_{\mathrm{span}(\mathcal{L}/\mathcal{L}')}(\mathbf{x}-\mathbf{v})\|^2 \\ &\le \mu(\mathcal{L}')^2 + \mu(\mathcal{L}/\mathcal{L}')^2 .\end{aligned}$$

The bound holds for any vector $\mathbf{x}$. Hence $\mu(\mathcal{L})^2 \le \mu(\mathcal{L}')^2 + \mu(\mathcal{L}/\mathcal{L}')^2$, as desired. ◀

3 Embedding Tori into Hilbert Space

The goal of this section is to prove Lemma 3.6, which summarizes the properties of the Gaussian embedding from [1], including a modified contraction property which we make explicit (see left-hand side of (1)). The proof closely follows that of [1, Theorem 1.4]. We start with some preliminary definitions and results from [1].

For $s > 0$ and $\mathbf{x} \in \mathbb{R}^n$ we define $\rho_s(\mathbf{x}) = \exp(-\pi\|\mathbf{x}/s\|^2)$. For any discrete set A, its Gaussian mass $\rho_s(A)$ is defined as $\sum_{\mathbf{x}\in A} \rho_s(\mathbf{x})$. The *smoothing parameter* of a lattice $\mathcal{L}$ is defined with respect to an $\varepsilon > 0$ and is given by

$$\eta_\varepsilon(\mathcal{L}) = \min\{s : \rho_{1/s}(\mathcal{L}^*) \le 1+\varepsilon\} .$$

▶ **Lemma 3.1** ([1, Lemma 2.5])**.** *For any $n \ge 1$ and lattice $\mathcal{L} \subseteq \mathbb{R}^n$, $\eta_\varepsilon(\mathcal{L}^*) \le \frac{2\sqrt{n}}{\lambda_1(\mathcal{L})}$ where $\varepsilon = 2^{-10n}$.*

Consider the function

$$h_{\mathcal{L},s}(\mathbf{x}) = 1 - \frac{\rho_s(\mathcal{L}-\mathbf{x})}{\rho_s(\mathcal{L})} .$$

Below we list some basic properties of this function, which ideally we would like to be proportional to the squared distance from the lattice. This is indeed the case, assuming the distance is not too large compared to s, and that s itself is small compared to the geometry of the lattice. The upper bound is shown in Item 1, and the lower bound is established in Items 2 and 3 (which give very similar bounds). When the distance is sufficiently larger than s, the function reaches saturation, as shown in Item 4.

▶ **Lemma 3.2** ([1, Lemmas 3.1 and 3.2]). *For any $n \geq 1$, lattice $\mathcal{L} \subseteq \mathbb{R}^n$, $s > 0$, and vector $\mathbf{x} \in \mathbb{R}^n$,*

1. $s^2 \cdot h_{\mathcal{L},s}(\mathbf{x}) \leq \pi \cdot \mathrm{dist}(\mathbf{x}, \mathcal{L})^2$,
2. $s^2 \cdot h_{\mathcal{L},s}(\mathbf{x}) \geq c \cdot \mathrm{dist}(\mathbf{x}, \mathcal{L})^2$ *if* $s \leq \frac{1}{2\,\eta_\varepsilon(\mathcal{L}^*)}$ *for some* $0 < \varepsilon \leq \frac{1}{1000}$ *and* $\mathrm{dist}(\mathbf{x}, \mathcal{L}) \leq \frac{s}{\sqrt{2}}$, *where c is an absolute constant,*
3. $h_{\mathcal{L},s}(\mathbf{x}) \geq 1 - e^{-\pi\,\mathrm{dist}(\mathbf{x},\mathcal{L})^2/s^2} - 2^{-11n}$ *if* $\lambda_1(\mathcal{L}) \geq 4\sqrt{n} \cdot s$,
4. $h_{\mathcal{L},s}(\mathbf{x}) \geq 1 - 2^{-11n}$ *if* $\mathrm{dist}(\mathbf{x}, \mathcal{L}) > 2\sqrt{n} \cdot s$.

▶ **Definition 3.3** ([1, Section 5]). *For lattice $\mathcal{L} \subseteq \mathbb{R}^n$ and $s > 0$, the embedding $H_{\mathcal{L},s} : \mathbb{R}^n/\mathcal{L} \to L_2(\mathbb{R}^n/\mathcal{L})$ maps vector $\mathbf{x} \in \mathbb{R}^n$ to the function $H_{\mathcal{L},s}(\mathbf{x}) \in L_2(\mathbb{R}^n/\mathcal{L})$ given by*

$$H_{\mathcal{L},s}(\mathbf{x})(\mathbf{y}) = \frac{s}{\sqrt{2\rho_s(\mathcal{L})}} \left(\frac{2}{s}\right)^{n/2} \rho_{\frac{s}{\sqrt{2}}}(\mathcal{L} + \mathbf{y} - \mathbf{x}) \ .$$

▶ **Lemma 3.4** ([1, Proposition 5.1]). *For any $n \geq 1$, lattice $\mathcal{L} \subseteq \mathbb{R}^n$, $s > 0$, and vectors $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, $\mathrm{dist}_{L_2(\mathbb{R}^n/\mathcal{L})}(H_{\mathcal{L},s}(\mathbf{x}), H_{\mathcal{L},s}(\mathbf{y}))^2 = s^2 \cdot h_{\mathcal{L},s}(\mathbf{x} - \mathbf{y})$.*

▶ **Definition 3.5** ([1, Section 5.1]). *For lattice $\mathcal{L} \subseteq \mathbb{R}^n$, $s > 0$, and $k \geq 1$, the embedding $H^{(k)}_{\mathcal{L},s}$ is defined by $H^{(k)}_{\mathcal{L},s} = (H_{\mathcal{L},s_1}, \ldots, H_{\mathcal{L},s_k})$ where $s_i = 2^{i-1}s$. We often take $s = \lambda_1(\mathcal{L})/(4\sqrt{n})$, in which case we omit the subscript s and simply write $H^{(k)}_{\mathcal{L}}$.*

▶ **Lemma 3.6.** *For any $n \geq 1$, lattice $\mathcal{L} \subseteq \mathbb{R}^n$, $k \geq 1$, and vectors $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$,*

$$\frac{c_H}{n} \cdot \min(\mathrm{dist}_{\mathbb{R}^n/\mathcal{L}}(\mathbf{x}, \mathbf{y}), 2^{k-1}\,\lambda_1(\mathcal{L}))^2 \leq \mathrm{dist}_{L_2(\mathbb{R}^n/\mathcal{L})^k}(H^{(k)}_{\mathcal{L}}(\mathbf{x}), H^{(k)}_{\mathcal{L}}(\mathbf{y}))^2 \leq \pi k \cdot \mathrm{dist}_{\mathbb{R}^n/\mathcal{L}}(\mathbf{x}, \mathbf{y})^2 \ , \tag{1}$$

where $c_H > 0$ is an absolute constant.

Proof. By Lemma 3.4, and recalling the notation $s_i = 2^{i-1}s$ where $s = \frac{\lambda_1(\mathcal{L})}{4\sqrt{n}}$,

$$\begin{aligned}\mathrm{dist}_{L_2(\mathbb{R}^n/\mathcal{L})^k}(H^{(k)}_{\mathcal{L}}(\mathbf{x}), H^{(k)}_{\mathcal{L}}(\mathbf{y}))^2 &= \sum_{i=1}^{k} \mathrm{dist}_{L_2(\mathbb{R}^n/\mathcal{L})}(H_{\mathcal{L},s_i}(\mathbf{x}), H_{\mathcal{L},s_i}(\mathbf{y}))^2 \\ &= \sum_{i=1}^{k} s_i^2 \cdot h_{\mathcal{L},s_i}(\mathbf{x} - \mathbf{y}) \ .\end{aligned}$$

Noting that $\mathrm{dist}_{\mathbb{R}^n/\mathcal{L}}(\mathbf{x}, \mathbf{y}) = \mathrm{dist}(\mathbf{x} - \mathbf{y}, \mathcal{L})$, the upper bound in (1) follows from Item 1 in Lemma 3.2:

$$\sum_{i=1}^{k} s_i^2 \cdot h_{\mathcal{L},s_i}(\mathbf{x} - \mathbf{y}) \leq \sum_{i=1}^{k} \pi \cdot \mathrm{dist}(\mathbf{x} - \mathbf{y}, \mathcal{L})^2 = \pi k \cdot \mathrm{dist}(\mathbf{x} - \mathbf{y}, \mathcal{L})^2 \ .$$

For the lower bound in (1), we will show that for any $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, there exists $i \in \{1, \ldots, k\}$ such that

$$s_i^2 \cdot h_{\mathcal{L},s_i}(\mathbf{x} - \mathbf{y}) \geq \frac{c_H}{n} \cdot \min(\mathrm{dist}(\mathbf{x} - \mathbf{y}, \mathcal{L}), 2^{k-1}\,\lambda_1(\mathcal{L}))^2 \ . \tag{2}$$

We consider three cases.

1. $\mathrm{dist}(\mathbf{x} - \mathbf{y}, \mathcal{L}) \leq \frac{\lambda_1(\mathcal{L})}{4\sqrt{2n}} = \frac{s}{\sqrt{2}}$. Note that according to Lemma 3.1, $s \leq \frac{1}{2\,\eta_\varepsilon(\mathcal{L}^*)}$ for some $0 < \varepsilon \leq \frac{1}{1000}$. Then by Item 2 of Lemma 3.2,

$$s^2 \cdot h_{\mathcal{L},s}(\mathbf{x} - \mathbf{y}) \geq c \cdot \mathrm{dist}(\mathbf{x} - \mathbf{y}, \mathcal{L})^2 \geq \frac{c}{n} \cdot \mathrm{dist}(\mathbf{x} - \mathbf{y}, \mathcal{L})^2 \ ,$$

which proves (2) with $i = 1$.

2. $\frac{s}{\sqrt{2}} < \operatorname{dist}(\mathbf{x}-\mathbf{y},\mathcal{L}) \le \lambda_1(\mathcal{L}) = 4\sqrt{n}\cdot s$. By Item 3 of Lemma 3.2,

$$\begin{aligned} s^2 \cdot h_{\mathcal{L},s}(\mathbf{x}-\mathbf{y}) &\ge s^2 \cdot (1 - e^{-\pi/2} - 2^{-11n}) \\ &= \frac{1 - e^{-\pi/2} - 2^{-11n}}{16n} \cdot \lambda_1(\mathcal{L})^2 \\ &\ge \frac{1 - e^{-\pi/2} - 2^{-11n}}{16n} \cdot \operatorname{dist}(\mathbf{x}-\mathbf{y},\mathcal{L})^2 , \end{aligned}$$

which again proves (2) with $i = 1$.

3. $\operatorname{dist}(\mathbf{x}-\mathbf{y},\mathcal{L}) > 4\sqrt{n}\cdot s$. Let $j \in \{2,\dots,k\}$ be the largest index such that $2\sqrt{n}\cdot s_j < \operatorname{dist}(\mathbf{x}-\mathbf{y},\mathcal{L})$. Notice that if $j < k$ then $4\sqrt{n}\cdot s_j = 2\sqrt{n}\cdot s_{j+1} \ge \operatorname{dist}(\mathbf{x}-\mathbf{y},\mathcal{L})$, and that if $j = k$, then $4\sqrt{n}\cdot s_j = 2^{k-1}\,\lambda_1(\mathcal{L})$. Then by Item 4 of Lemma 3.2,

$$\begin{aligned} s_j^2 \cdot h_{\mathcal{L},s_j}(\mathbf{x}-\mathbf{y}) &\ge s_j^2 \cdot (1 - 2^{-11n}) \\ &= \frac{1 - 2^{-11n}}{16n} \cdot (4\sqrt{n}\cdot s_j)^2 \\ &\ge \frac{1 - 2^{-11n}}{16n} \cdot \min(\operatorname{dist}(\mathbf{x}-\mathbf{y},\mathcal{L}), 2^{k-1}\,\lambda_1(\mathcal{L}))^2 , \end{aligned}$$

which proves (2) with $i = j$. ◀

4 Embedding into Tori

The goal of this section is to prove Lemma 4.13, which shows that there exists an embedding from an arbitrary torus into a tuple of tori with good geometry. The embedding is constructed based on "good filtrations," which we define and instantiate in Section 4.1. The definition of the embedding is given in Section 4.2, and its expansion and contraction properties are shown in Section 4.3 and Section 4.4 respectively. The contraction property matches the modified notion of contraction used in Lemma 3.6.

4.1 Good Filtrations

In this section we define the notion of a (q,γ)-*filtration* (Definition 4.1) and show how to construct a good one for every lattice (Lemma 4.3). We also include a small technical lemma that will be useful later (Lemma 4.4).

A *filtration* of a lattice $\mathcal{L}$ is a chain of sublattices $\{\mathbf{0}\} = \mathcal{L}_0 \subset \mathcal{L}_1 \subset \cdots \subset \mathcal{L}_m = \mathcal{L}$. We call m the *size* of the filtration.

▶ **Definition 4.1.** *For $q \ge 1$, $\gamma > 1$, we say that a filtration $\{\mathbf{0}\} = \mathcal{L}_0 \subset \mathcal{L}_1 \subset \cdots \subset \mathcal{L}_m = \mathcal{L}$ is a* (q,γ)-filtration *if it satisfies both*

1. $\mu(\mathcal{L}_j/\mathcal{L}_{j-1}) \le q\,\lambda_1(\mathcal{L}_j/\mathcal{L}_{j-1})/2$ *for all* $1 \le j \le m$, *and*
2. $\lambda_1(\mathcal{L}_{j+1}/\mathcal{L}_j) \ge \gamma\,\lambda_1(\mathcal{L}_j/\mathcal{L}_{j-1})$ *for all* $1 \le j < m$.

Our construction of good filtrations is based on Korkine-Zolotarev bases, defined next. Recall first that for a sequence of vectors $(\mathbf{b}_1,\dots,\mathbf{b}_n)$, its *Gram-Schmidt orthogonalization* $(\mathbf{b}'_1,\dots,\mathbf{b}'_n)$ is defined by

$$\mathbf{b}'_i = \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{i,j}\mathbf{b}'_j , \quad \text{where } \mu_{i,j} = \frac{\langle \mathbf{b}_i, \mathbf{b}'_j\rangle}{\langle \mathbf{b}'_j, \mathbf{b}'_j\rangle} ,$$

i.e., $\mathbf{b}'_i$ is the projection of $\mathbf{b}_i$ on the space orthogonal to $\operatorname{span}(\mathbf{b}_1,\dots,\mathbf{b}_{i-1})$.

▶ **Definition 4.2.** *A basis* $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ *for a lattice* $\mathcal{L} \subseteq \mathbb{R}^n$ *is called a* Korkine-Zolotarev basis *if*

- $\mathbf{b}'_i$ *is a shortest vector of* $\mathcal{L}/\mathcal{L}_{i-1}$ *for all* $1 \le i \le n$*, and*
- $|\mu_{i,j}| \le 1/2$ *for all* $1 \le j < i \le n$*,*

where $(\mathbf{b}'_1, \ldots, \mathbf{b}'_n)$ *is the Gram-Schmidt orthogonalization of* $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$*,* $\mu_{i,j}$ *are the corresponding coefficients, and* $\mathcal{L}_i$ *is the lattice generated by* $(\mathbf{b}_1, \ldots, \mathbf{b}_i)$ *(with* $\mathcal{L}_0 = \{\mathbf{0}\}$*).*

It is easy to prove that a Korkine-Zolotarev basis exists for any lattice. We remark that the second property above will not be used in this paper.

▶ **Lemma 4.3.** *For any* $n \ge 1$*, lattice* $\mathcal{L} \subseteq \mathbb{R}^n$*, and* $\gamma > 1$*, there exists a* $(\gamma\sqrt{n}, \gamma)$*-filtration of* $\mathcal{L}$*.*

Proof. Let $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ be a Korkine-Zolotarev basis of $\mathcal{L}$. Let $(\mathbf{b}'_1, \ldots, \mathbf{b}'_n)$ be its Gram-Schmidt orthogonalization, and consider the filtration $\{\mathbf{0}\} = \mathcal{L}_0 \subset \mathcal{L}_1 \subset \cdots \subset \mathcal{L}_n = \mathcal{L}$ where $\mathcal{L}_i$ is the lattice generated by $(\mathbf{b}_1, \ldots, \mathbf{b}_i)$. From Definition 4.2 we know that $\lambda_1(\mathcal{L}/\mathcal{L}_{i-1}) = \|\mathbf{b}'_i\| = \lambda_1(\mathcal{L}_k/\mathcal{L}_{i-1})$, for all $1 \le i \le k \le n$. Construct a coarsening of this filtration, $\{\mathbf{0}\} = \mathcal{L}_{i_0} \subset \mathcal{L}_{i_1} \subset \cdots \subset \mathcal{L}_{i_m} = \mathcal{L}$, as follows. Let $i_0 = 0$ and for $j \ge 1$, $i_j \in \{i_{j-1}+1, \ldots, n\}$ be the largest index such that $\|\mathbf{b}'_k\| \le \gamma\|\mathbf{b}'_{i_{j-1}+1}\|$ for all $k \in \{i_{j-1}+1, \ldots, i_j\}$. Finally, stop when $i_m = n$. We are going to show that this coarser filtration is a $(\gamma\sqrt{n}, \gamma)$-filtration.

We observe that for all $1 \le j \le m$,

$$\lambda_1(\mathcal{L}_{i_j}/\mathcal{L}_{i_{j-1}}) = \|\mathbf{b}'_{i_{j-1}+1}\| \,.$$

Then, by construction of the coarsening, for all $1 \le j < m$,

$$\lambda_1(\mathcal{L}_{i_{j+1}}/\mathcal{L}_{i_j}) = \|\mathbf{b}'_{i_j+1}\| > \gamma\|\mathbf{b}'_{i_{j-1}+1}\| = \gamma\,\lambda_1(\mathcal{L}_{i_j}/\mathcal{L}_{i_{j-1}}) \,.$$

This proves the second property of a $(\gamma\sqrt{n}, \gamma)$-filtration. Moreover,

$$\begin{aligned}
\mu(\mathcal{L}_{i_j}/\mathcal{L}_{i_{j-1}})^2 &\le \sum_{k=i_{j-1}+1}^{i_j} \mu(\mathcal{L}_k/\mathcal{L}_{k-1})^2 \\
&= \sum_{k=i_{j-1}+1}^{i_j} \|\mathbf{b}'_k\|^2/4 \\
&\le \sum_{k=i_{j-1}+1}^{i_j} \gamma^2\|\mathbf{b}'_{i_{j-1}+1}\|^2/4 \\
&\le \gamma^2 n \cdot \lambda_1(\mathcal{L}_{i_j}/\mathcal{L}_{i_{j-1}})^2/4 \,,
\end{aligned}$$

where the first inequality is by Lemma 2.3 and the second inequality is by construction of the coarsening. This proves the first property of a $(\gamma\sqrt{n}, \gamma)$-filtration. ◀

We end by proving a small property of (q, γ)-filtrations.

▶ **Lemma 4.4.** *For any* (q, γ)*-filtration* $\{\mathbf{0}\} = \mathcal{L}_0 \subset \mathcal{L}_1 \subset \cdots \subset \mathcal{L}_m = \mathcal{L}$ *and* $1 \le j \le m$*,*

$$\mu(\mathcal{L}_j) \le \frac{q}{\sqrt{1 - 1/\gamma^2}} \cdot \lambda_1(\mathcal{L}_j/\mathcal{L}_{j-1})/2 \,.$$

Consequently, if $\gamma \ge 2$*, then* $\mu(\mathcal{L}_j) \le q\,\lambda_1(\mathcal{L}_j/\mathcal{L}_{j-1})$*.*

Proof. The inequality can be proved as follows:

$$\begin{aligned}\mu^2(\mathcal{L}_j) &\le \sum_{i=1}^{j} \mu^2(\mathcal{L}_i/\mathcal{L}_{i-1}) \\ &\le \sum_{i=1}^{j} q^2\, \lambda_1^2(\mathcal{L}_i/\mathcal{L}_{i-1})/4 \\ &\le \sum_{i=1}^{j} \frac{q^2}{\gamma^{2(j-i)}} \cdot \lambda_1^2(\mathcal{L}_j/\mathcal{L}_{j-1})/4 \\ &\le \frac{q^2}{1-1/\gamma^2} \cdot \lambda_1^2(\mathcal{L}_j/\mathcal{L}_{j-1})/4\ ,\end{aligned}$$

where the first inequality uses Lemma 2.3, the second inequality uses the first property in Definition 4.1, and the third inequality uses the second property in Definition 4.1. ◀

4.2 The Embedding

Let $\mathcal{F}$ be a filtration $\{\mathbf{0}\} = \mathcal{L}_0 \subset \mathcal{L}_1 \subset \cdots \subset \mathcal{L}_m = \mathcal{L}$ of a lattice $\mathcal{L} \subseteq \mathbb{R}^n$. The filtration naturally induces an orthogonal decomposition of $\mathbb{R}^n$ into m subspaces, namely, $\mathrm{span}(\mathcal{L}_j/\mathcal{L}_{j-1})$ for $j = 1, \ldots, m$. We use $\pi_{\mathcal{F},j}$ to denote $\pi_{\mathrm{span}(\mathcal{L}_j/\mathcal{L}_{j-1})}$, the projection on the j-th subspace. We will similarly use $\pi^{\geq}_{\mathcal{F},j}$, $\pi^{<}_{\mathcal{F},j}$, $\pi^{>}_{\mathcal{F},j}$, and $\pi^{\leq}_{\mathcal{F},j}$ to denote projections on the span of prefixes and suffixes of this decomposition. Specifically, for $1 \le j \le m$ we have $\pi^{\geq}_{\mathcal{F},j} = \pi_{\mathrm{span}(\mathcal{L}/\mathcal{L}_{j-1})}$, $\pi^{<}_{\mathcal{F},j} = \pi_{\mathrm{span}(\mathcal{L}_{j-1})}$, $\pi^{>}_{\mathcal{F},j} = \pi_{\mathrm{span}(\mathcal{L}/\mathcal{L}_j)}$, and $\pi^{\leq}_{\mathcal{F},j} = \pi_{\mathrm{span}(\mathcal{L}_j)}$.

▶ **Definition 4.5.** *For filtration $\mathcal{F}$ of size m, $0 < \alpha < 1$, and $1 \le j \le m$, the embedding $E_{\mathcal{F},\alpha,j}$ is defined by*

$$E_{\mathcal{F},\alpha,j}(\mathbf{x}) = \sum_{i=j}^{m} \alpha^{i-j} \pi_{\mathcal{F},i}(\mathbf{x})\ .$$

Note that since $E_{\mathcal{F},\alpha,j}$ is linear, for any lattice $\mathcal{L} \subseteq \mathbb{R}^n$ and vector $\mathbf{x} \in \mathbb{R}^n$, $E_{\mathcal{F},\alpha,j}(\mathbf{x}+\mathcal{L}) = E_{\mathcal{F},\alpha,j}(\mathbf{x}) + E_{\mathcal{F},\alpha,j}(\mathcal{L})$, and thus $E_{\mathcal{F},\alpha,j}$ is a well-defined embedding from the torus $\mathbb{R}^n/\mathcal{L}$ to the torus $E_{\mathcal{F},\alpha,j}(\mathbb{R}^n/\mathcal{L})$.

▶ **Definition 4.6.** *For a filtration $\mathcal{F}$ of size m and $0 < \alpha < 1$, the embedding $E_{\mathcal{F},\alpha}$ is defined by $E_{\mathcal{F},\alpha} = (E_{\mathcal{F},\alpha,1}, \ldots, E_{\mathcal{F},\alpha,m})$ with the metric being ℓ_2 of the tori metrics.*

4.3 Expansion of the Embedding

▶ **Definition 4.7** (Realization of distance in torus)**.** *For any $n \ge 1$, lattice $\mathcal{L} \subseteq \mathbb{R}^n$, and vector $\mathbf{x} \in \mathbb{R}^n$, since $\mathrm{dist}(\mathbf{x}, \mathcal{L}) = \min_{\mathbf{v}\in\mathcal{L}} \|\mathbf{x} - \mathbf{v}\|$, there always exists $\mathbf{v} \in \mathcal{L}$ such that $\mathrm{dist}(\mathbf{x}, \mathcal{L}) = \|\mathbf{x} - \mathbf{v}\|$. We say such minimizer $\mathbf{v}$* realizes *the distance $\mathrm{dist}(\mathbf{x}, \mathcal{L})$. Similarly, for vectors $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, we say $\mathbf{v}$* realizes *the distance $\mathrm{dist}_{\mathbb{R}^n/\mathcal{L}}(\mathbf{x}, \mathbf{y})$ if $\mathrm{dist}_{\mathbb{R}^n/\mathcal{L}}(\mathbf{x}, \mathbf{y}) = \|\mathbf{x} - \mathbf{y} - \mathbf{v}\|$.*

▶ **Lemma 4.8** (Expansion of the embedding)**.** *For any $n \ge 1$, lattice $\mathcal{L} \subseteq \mathbb{R}^n$ with filtration $\mathcal{F}$, $0 < \alpha < 1$, and vectors $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$,*

$$\begin{aligned}\mathrm{dist}_{E_{\mathcal{F},\alpha}(\mathbb{R}^n/\mathcal{L})}(E_{\mathcal{F},\alpha}(\mathbf{x}), E_{\mathcal{F},\alpha}(\mathbf{y}))^2 &:= \sum_{j=1}^{m} \mathrm{dist}_{E_{\mathcal{F},\alpha,j}(\mathbb{R}^n/\mathcal{L})}(E_{\mathcal{F},\alpha,j}(\mathbf{x}), E_{\mathcal{F},\alpha,j}(\mathbf{y}))^2 \\ &\le \frac{1}{1-\alpha^2} \cdot \mathrm{dist}_{\mathbb{R}^n/\mathcal{L}}(\mathbf{x}, \mathbf{y})^2\ .\end{aligned}$$

Proof. Let m be the size of $\mathcal{F}$. For all $\mathbf{v} \in \mathcal{L}$, the embedded distance can be bounded from above by

$$\begin{aligned}\sum_{j=1}^{m} \mathrm{dist}_{E_{\mathcal{F},\alpha,j}(\mathbb{R}^n/\mathcal{L})}(E_{\mathcal{F},\alpha,j}(\mathbf{x}), E_{\mathcal{F},\alpha,j}(\mathbf{y}))^2 &\le \sum_{j=1}^{m} \|E_{\mathcal{F},\alpha,j}(\mathbf{x}-\mathbf{y}-\mathbf{v})\|^2 \\ &= \sum_{j=1}^{m}\sum_{i=j}^{m} \alpha^{2(i-j)} \|\pi_{\mathcal{F},i}(\mathbf{x}-\mathbf{y}-\mathbf{v})\|^2 \\ &\le \frac{1}{1-\alpha^2} \cdot \sum_{i=1}^{m} \|\pi_{\mathcal{F},i}(\mathbf{x}-\mathbf{y}-\mathbf{v})\|^2 \\ &= \frac{1}{1-\alpha^2} \cdot \|\mathbf{x}-\mathbf{y}-\mathbf{v}\|^2 \,,\end{aligned}$$

which, for $\mathbf{v}$ realizing $\mathrm{dist}_{\mathbb{R}^n/\mathcal{L}}(\mathbf{x},\mathbf{y})$, gives $\frac{1}{1-\alpha^2} \cdot \mathrm{dist}_{\mathbb{R}^n/\mathcal{L}}(\mathbf{x},\mathbf{y})^2$ as desired. ◀

4.4 Contraction of the Embedding

▶ **Lemma 4.9.** *For any $n \ge 1$, lattice $\mathcal{L} \subseteq \mathbb{R}^n$, lattice point $\mathbf{v}' \in \mathcal{L}$ realizing $\mathrm{dist}(\mathbf{x},\mathcal{L})$, and lattice point $\mathbf{v} \in \mathcal{L}$,*

$$\|\mathbf{x}-\mathbf{v}\| \ge \frac{1}{2}\|\mathbf{v}-\mathbf{v}'\| \,.$$

Consequently, if $\mathbf{v}$ does not realize $\mathrm{dist}(\mathbf{x},\mathcal{L})$, then $\mathbf{v} \ne \mathbf{v}'$ and

$$\|\mathbf{x}-\mathbf{v}\| \ge \frac{1}{2}\,\lambda_1(\mathcal{L}) \,.$$

Proof. By definition, $\|\mathbf{x}-\mathbf{v}'\| \le \|\mathbf{x}-\mathbf{v}\|$. Then by the triangle inequality, $\|\mathbf{v}-\mathbf{v}'\| \le \|\mathbf{x}-\mathbf{v}\| + \|\mathbf{x}-\mathbf{v}'\| \le 2\|\mathbf{x}-\mathbf{v}\|$, as desired. ◀

▶ **Lemma 4.10.** *For any (q,γ)-filtration $\mathcal{F}$ given by $\{\mathbf{0}\} = \mathcal{L}_0 \subset \mathcal{L}_1 \subset \cdots \subset \mathcal{L}_m = \mathcal{L}$, $1/\gamma \le \alpha < 1$, and $1 \le j \le m$, $\lambda_1(E_{\mathcal{F},\alpha,j}(\mathcal{L})) = \lambda_1(\mathcal{L}_j/\mathcal{L}_{j-1})$.*

Proof. We prove the claim by induction on j. When $j = m$, $E_{\mathcal{F},\alpha,m}(\mathcal{L}) = \mathcal{L}_m/\mathcal{L}_{m-1}$, and thus the claim holds trivially.

Suppose the claim holds for $j+1$. Then for j, note that $\mathcal{L}_j/\mathcal{L}_{j-1} \subseteq E_{\mathcal{F},\alpha,j}(\mathcal{L})$. Therefore $\lambda_1(E_{\mathcal{F},\alpha,j}(\mathcal{L}))$ is the minimum of $\lambda_1(\mathcal{L}_j/\mathcal{L}_{j-1})$ and the minimum length of vectors in the set $E_{\mathcal{F},\alpha,j}(\mathcal{L}) \setminus (\mathcal{L}_j/\mathcal{L}_{j-1})$. Since $E_{\mathcal{F},\alpha,j} = \pi_{\mathcal{F},j} + \alpha E_{\mathcal{F},\alpha,j+1}$, the length of any vector in $E_{\mathcal{F},\alpha,j}(\mathcal{L}) \setminus (\mathcal{L}_j/\mathcal{L}_{j-1})$ is bounded from below by

$$\begin{aligned}\alpha\,\lambda_1(E_{\mathcal{F},\alpha,j+1}(\mathcal{L})) &= \alpha\,\lambda_1(\mathcal{L}_{j+1}/\mathcal{L}_j) \\ &\ge \alpha\gamma\,\lambda_1(\mathcal{L}_j/\mathcal{L}_{j-1}) \\ &\ge \lambda_1(\mathcal{L}_j/\mathcal{L}_{j-1}) \,,\end{aligned}$$

where the equality is the induction assumption and the first inequality uses the second property in Definition 4.1. Hence $\lambda_1(E_{\mathcal{F},\alpha,j}(\mathcal{L})) = \lambda_1(\mathcal{L}_j/\mathcal{L}_{j-1})$, as desired. ◀

Combining Lemma 4.10 with Lemma 4.4 as well as Definition 4.1, we immediately get the following corollary.

▶ **Corollary 4.11.** *For any (q,γ)-filtration $\mathcal{F}$ given by $\{\mathbf{0}\} = \mathcal{L}_0 \subset \mathcal{L}_1 \subset \cdots \subset \mathcal{L}_m = \mathcal{L}$ with $\gamma \ge 2$ and $1/\gamma \le \alpha < 1$,*

1. $\mu(\mathcal{L}_j) \le q\,\lambda_1(E_{\mathcal{F},\alpha,j}(\mathcal{L}))$ *for all* $1 \le j \le m$, *and*
2. $\lambda_1(E_{\mathcal{F},\alpha,j+1}(\mathcal{L})) \ge \gamma\,\lambda_1(E_{\mathcal{F},\alpha,j}(\mathcal{L}))$ *for all* $1 \le j < m$.

▶ **Lemma 4.12** (Contraction of the embedding). *For any* $n \ge 1$, *lattice* $\mathcal{L} \subseteq \mathbb{R}^n$ *with* (q,γ)-*filtration* $\mathcal{F}$ *of size* m *satisfying* $\gamma \ge 2$ *and* $q \le \gamma^2/32$, $\frac{1}{2} \le \alpha < 1$, *and vectors* $\mathbf{x},\mathbf{y} \in \mathbb{R}^n$,

$$\sum_{j=1}^{m} \min\big(\mathrm{dist}_{E_{\mathcal{F},\alpha,j}(\mathbb{R}^n/\mathcal{L})}(E_{\mathcal{F},\alpha,j}(\mathbf{x}), E_{\mathcal{F},\alpha,j}(\mathbf{y})), q^2\,\lambda_1(E_{\mathcal{F},\alpha,j}(\mathcal{L}))\big)^2 \ge c_E \cdot \mathrm{dist}_{\mathbb{R}^n/\mathcal{L}}(\mathbf{x},\mathbf{y})^2\ , \tag{3}$$

where $c_E > 0$ *is an absolute constant.*

Proof. For simplicity, we omit the subscript $\mathcal{F}$ in the notations $\pi_{\mathcal{F},j}$, $\pi^{\ge}_{\mathcal{F},j}$, $\pi^{<}_{\mathcal{F},j}$, $\pi^{>}_{\mathcal{F},j}$, $\pi^{\le}_{\mathcal{F},j}$, $E_{\mathcal{F},\alpha,j}$ and $E_{\mathcal{F},\alpha}$ in this proof.

Let $\mathbf{v} \in \mathcal{L}$ be a lattice point that realizes $\mathrm{dist}_{\mathbb{R}^n/\mathcal{L}}(\mathbf{x},\mathbf{y})$. Then $\mathrm{dist}_{\mathbb{R}^n/\mathcal{L}}(\mathbf{x},\mathbf{y}) = \|\mathbf{x}-\mathbf{y}-\mathbf{v}\|$. Hence our goal is equivalently to show that the left-hand side of (3) satisfies

$$\sum_{j=1}^{m} \min\big(\mathrm{dist}_{E_{\alpha,j}(\mathbb{R}^n/\mathcal{L})}(E_{\alpha,j}(\mathbf{x}), E_{\alpha,j}(\mathbf{y})), q^2\,\lambda_1(E_{\alpha,j}(\mathcal{L}))\big)^2 \ge c_E \cdot \|\mathbf{x}-\mathbf{y}-\mathbf{v}\|^2\ . \tag{4}$$

Let $j_1 \in \{0,1,\ldots,m\}$ be the smallest index satisfying that for all $j \in \{j_1+1,\ldots,m\}$, $E_{\alpha,j}(\mathbf{v})$ realizes $\mathrm{dist}_{E_{\alpha,j}(\mathbb{R}^n/\mathcal{L})}(E_{\alpha,j}(\mathbf{x}), E_{\alpha,j}(\mathbf{y}))$. Then for all $j \in \{j_1+1,\ldots,m\}$,

$$\begin{aligned}\mathrm{dist}_{E_{\alpha,j}(\mathbb{R}^n/\mathcal{L})}(E_{\alpha,j}(\mathbf{x}), E_{\alpha,j}(\mathbf{y})) &= \|E_{\alpha,j}(\mathbf{x}-\mathbf{y}-\mathbf{v})\| \\ &\ge \|\pi_j(\mathbf{x}-\mathbf{y}-\mathbf{v})\|\ .\end{aligned} \tag{5}$$

Moreover, according to Lemma 2.2 and Corollary 4.11,

$$\|\pi_j(\mathbf{x}-\mathbf{y}-\mathbf{v})\| \le \|\pi^{\le}_j(\mathbf{x}-\mathbf{y}-\mathbf{v})\| \le \mu(\mathcal{L}_j) \le q\,\lambda_1(E_{\alpha,j}(\mathcal{L})) \le q^2\,\lambda_1(E_{\alpha,j}(\mathcal{L}))\ . \tag{6}$$

Combining (5) and (6), the left-hand side of (4) is bounded from below by

$$\sum_{j=j_1+1}^{m} \|\pi_j(\mathbf{x}-\mathbf{y}-\mathbf{v})\|^2 = \|\pi^{>}_{j_1}(\mathbf{x}-\mathbf{y}-\mathbf{v})\|^2\ . \tag{7}$$

If it is the case that

$$\|\pi^{>}_{j_1}(\mathbf{x}-\mathbf{y}-\mathbf{v})\|^2 \ge \frac{1}{2}\|\mathbf{x}-\mathbf{y}-\mathbf{v}\|^2\ ,$$

then (7) clearly suffices to prove (4). So from now on we assume that

$$\begin{aligned}&\|\pi^{>}_{j_1}(\mathbf{x}-\mathbf{y}-\mathbf{v})\|^2 < \frac{1}{2}\|\mathbf{x}-\mathbf{y}-\mathbf{v}\|^2\ , \\ \text{i.e., }&\|\pi^{\le}_{j_1}(\mathbf{x}-\mathbf{y}-\mathbf{v})\|^2 > \frac{1}{2}\|\mathbf{x}-\mathbf{y}-\mathbf{v}\|^2\ .\end{aligned} \tag{8}$$

In particular, this implies $j_1 > 0$. Then, by definition of j_1, $E_{\alpha,j_1}(\mathbf{v})$ does not realize $\mathrm{dist}_{E_{\alpha,j_1}(\mathbb{R}^n/\mathcal{L})}(E_{\alpha,j_1}(\mathbf{x}), E_{\alpha,j_1}(\mathbf{y}))$, which, by using Lemma 4.9 with lattice $E_{\alpha,j_1}(\mathcal{L})$, implies

$$\|E_{\alpha,j_1}(\mathbf{x}-\mathbf{y}-\mathbf{v})\| \ge \frac{1}{2}\,\lambda_1(E_{\alpha,j_1}(\mathcal{L}))\ . \tag{9}$$

Under assumption (8), it suffices to prove that there exists an index $j_0 \in \{1, \ldots, m\}$ such that

$$\min\left(\mathrm{dist}_{E_{\alpha,j_0}(\mathbb{R}^n/\mathcal{L})}(E_{\alpha,j_0}(\mathbf{x}), E_{\alpha,j_0}(\mathbf{y})), q^2\,\lambda_1(E_{\alpha,j_0}(\mathcal{L}))\right)^2 \geq c \cdot \|\pi^{\leq}_{j_1}(\mathbf{x}-\mathbf{y}-\mathbf{v})\|^2 ,$$

or equivalently,

$$\|E_{\alpha,j_0}(\mathbf{x}-\mathbf{y}-\mathbf{v}')\|^2 \geq c \cdot \|\pi^{\leq}_{j_1}(\mathbf{x}-\mathbf{y}-\mathbf{v})\|^2 \text{ , and} \tag{10}$$

$$q^4\,\lambda_1^2(E_{\alpha,j_0}(\mathcal{L})) \geq c \cdot \|\pi^{\leq}_{j_1}(\mathbf{x}-\mathbf{y}-\mathbf{v})\|^2 , \tag{11}$$

where $\mathbf{v}' \in \mathcal{L}$ is a lattice point such that $E_{\alpha,j_0}(\mathbf{v}')$ realizes $\mathrm{dist}_{E_{\alpha,j_0}(\mathbb{R}^n/\mathcal{L})}(E_{\alpha,j_0}(\mathbf{x}), E_{\alpha,j_0}(\mathbf{y}))$, and c is some absolute constant. Note that, without loss of generality, it can be assumed that

$$\|\pi^{<}_{j_0}(\mathbf{x}-\mathbf{y}-\mathbf{v}')\| \leq \mu(\mathcal{L}_{j_0-1}) \tag{12}$$

(since otherwise, we can use $\mathbf{v}'+\mathbf{u}$ instead of $\mathbf{v}'$, where $\mathbf{u} \in \mathcal{L}_{j_0-1}$ realizes $\mathrm{dist}(\pi^{<}_{j_0}(\mathbf{x}-\mathbf{y}-\mathbf{v}'), \mathcal{L}_{j_0-1})$).

We choose $j_0 = j_1$ if

$$\mu(\mathcal{L}_{j_1-1}) \leq \frac{1}{4}\,\lambda_1(E_{\alpha,j_1}(\mathcal{L})) ,$$

and otherwise $j_0 = j_1 - 1$. By Corollary 4.11 and the condition $q \leq \gamma^2/32$, we know that

$$\mu(\mathcal{L}_{j_1-2}) \leq \frac{q}{\gamma^2} \cdot \lambda_1(E_{\alpha,j_1}(\mathcal{L})) \leq \frac{1}{32}\,\lambda_1(E_{\alpha,j_1}(\mathcal{L})) .$$

Moreover, as $\mathcal{L}_{j_1}/\mathcal{L}_{j_1-1}$ is both a quotient of $\mathcal{L}_{j_1}$ and a sublattice of $E_{\alpha,j_1}(\mathcal{L})$,

$$\mu(\mathcal{L}_{j_1}) \geq \mu(\mathcal{L}_{j_1}/\mathcal{L}_{j_1-1}) \geq \frac{1}{2}\,\lambda_1(\mathcal{L}_{j_1}/\mathcal{L}_{j_1-1}) \geq \frac{1}{2}\,\lambda_1(E_{\alpha,j_1}(\mathcal{L}))$$

(and the last inequality is actually an equality due to Lemma 4.10). Therefore j_0 satisfies

$$\mu(\mathcal{L}_{j_0-1}) \leq \frac{1}{4}\,\lambda_1(E_{\alpha,j_1}(\mathcal{L})) \text{ , and} \tag{13}$$

$$\mu(\mathcal{L}_{j_0}) > \frac{1}{4}\,\lambda_1(E_{\alpha,j_1}(\mathcal{L})) . \tag{14}$$

We first prove (11) for this choice of j_0:

$$\begin{aligned} q^2\,\lambda_1(E_{\alpha,j_0}(\mathcal{L})) &\geq q\,\mu(\mathcal{L}_{j_0}) \\ &> \frac{q}{4} \cdot \lambda_1(E_{\alpha,j_1}(\mathcal{L})) \\ &\geq \frac{1}{4}\,\mu(\mathcal{L}_{j_1}) \\ &\geq \frac{1}{4}\|\pi^{\leq}_{j_1}(\mathbf{x}-\mathbf{y}-\mathbf{v})\| , \end{aligned}$$

where the first and third inequalities use Corollary 4.11, the second inequality follows from (14), and the last inequality uses Lemma 2.2.

We next prove (10) for this choice of j_0. We begin with showing that

$$\pi^{\geq}_{j_2}(\mathbf{v}') = \pi^{\geq}_{j_2}(\mathbf{v}) , \tag{15}$$

where $j_2 = \min(j_1 + 1, m)$. Suppose towards contradiction that $\pi^{>}_{j_2}(\mathbf{v}') \neq \pi^{>}_{j_2}(\mathbf{v})$ (implying $j_2 < m$, and thus $j_2 = j_1 + 1$). Then, by definition, $\|E_{\alpha,j_1+2}(\mathbf{v} - \mathbf{v}')\| \geq \lambda_1(E_{\alpha,j_1+2}(\mathcal{L}))$. Hence

$$\begin{aligned}
\|\pi^{\leq}_{j_1}(\mathbf{x} - \mathbf{y} - \mathbf{v})\| &> \frac{1}{2}\|\mathbf{x} - \mathbf{y} - \mathbf{v}\| \\
&\geq \frac{1}{2}\|E_{\alpha,j_0}(\mathbf{x} - \mathbf{y} - \mathbf{v})\| \\
&\geq \frac{1}{4}\|E_{\alpha,j_0}(\mathbf{v} - \mathbf{v}')\| \\
&\geq \frac{1}{4}\|\pi^{\geq}_{j_1+2}(E_{\alpha,j_0}(\mathbf{v} - \mathbf{v}'))\| \\
&= \frac{\alpha^{j_1-j_0+2}}{4}\|E_{\alpha,j_1+2}(\mathbf{v} - \mathbf{v}')\| \\
&\geq \frac{\alpha^{j_1-j_0+2}}{4}\,\lambda_1(E_{\alpha,j_1+2}(\mathcal{L}))\ ,
\end{aligned}$$

where the first inequality follows from (8) and the third inequality uses Lemma 4.9 with lattice $E_{\alpha,j_0}(\mathcal{L})$. On the other hand, we know that $\|\pi^{\leq}_{j_1}(\mathbf{x} - \mathbf{y} - \mathbf{v})\| \leq \mu(\mathcal{L}_{j_1})$ according to Lemma 2.2. Then we have

$$\frac{\alpha^{j_1-j_0+2}}{4}\,\lambda_1(E_{\alpha,j_1+2}(\mathcal{L})) < \mu(\mathcal{L}_{j_1}) \leq \frac{q}{\gamma^2}\,\lambda_1(E_{\alpha,j_1+2}(\mathcal{L}))\ , \tag{16}$$

where the last inequality uses Corollary 4.11. Since $\alpha^{j_1-j_0+2} \geq \alpha^3 \geq 1/8$, (16) contradicts the condition $q \leq \gamma^2/32$.

Based on (15), we continue to prove (10) with the following observation:

$$\begin{aligned}
\|E_{\alpha,j_0}(\mathbf{x} - \mathbf{y} - \mathbf{v}')\|^2 &= \sum_{i=j_0}^{m} \alpha^{2(i-j_0)}\|\pi_i(\mathbf{x} - \mathbf{y} - \mathbf{v}')\|^2 \\
&\geq \alpha^{2(j_2-j_0)} \sum_{i=j_0}^{j_2} \|\pi_i(\mathbf{x} - \mathbf{y} - \mathbf{v}')\|^2 \\
&= \alpha^{2(j_2-j_0)}(\|\mathbf{x} - \mathbf{y} - \mathbf{v}'\|^2 - \|\pi^{\leq}_{j_0}(\mathbf{x} - \mathbf{y} - \mathbf{v}')\|^2 - \|\pi^{\geq}_{j_2}(\mathbf{x} - \mathbf{y} - \mathbf{v}')\|^2) \\
&\geq \alpha^{2(j_2-j_0)}(\|\mathbf{x} - \mathbf{y} - \mathbf{v}\|^2 - \mu^2(\mathcal{L}_{j_0-1}) - \|\pi^{\geq}_{j_2}(\mathbf{x} - \mathbf{y} - \mathbf{v})\|^2)\ , \quad (17)
\end{aligned}$$

where the last inequality uses the following three facts: (i) as $\mathbf{v}$ realizes $\mathrm{dist}_{\mathbb{R}^n/\mathcal{L}}(\mathbf{x}, \mathbf{y})$, $\|\mathbf{x} - \mathbf{y} - \mathbf{v}'\| \geq \|\mathbf{x} - \mathbf{y} - \mathbf{v}\|$; (ii) the term $\|\pi^{\leq}_{j_0}(\mathbf{x} - \mathbf{y} - \mathbf{v}')\|$ is bounded from above by (12); and (iii) $\pi^{>}_{j_2}(\mathbf{x} - \mathbf{y} - \mathbf{v}') = \pi^{>}_{j_2}(\mathbf{x} - \mathbf{y} - \mathbf{v})$ due to (15). Moreover, according to (13) and (9),

$$\begin{aligned}
\mu(\mathcal{L}_{j_0-1}) &\leq \frac{1}{4}\,\lambda_1(E_{\alpha,j_1}(\mathcal{L})) \\
&\leq \frac{1}{2}\|E_{\alpha,j_1}(\mathbf{x} - \mathbf{y} - \mathbf{v})\| \\
&\leq \frac{1}{2}\|\mathbf{x} - \mathbf{y} - \mathbf{v}\|\ ,
\end{aligned}$$

and according to (8),

$$\begin{aligned}
\|\pi^{>}_{j_2}(\mathbf{x} - \mathbf{y} - \mathbf{v})\|^2 &\leq \|\pi^{>}_{j_1}(\mathbf{x} - \mathbf{y} - \mathbf{v})\|^2 \\
&< \frac{1}{2}\|\mathbf{x} - \mathbf{y} - \mathbf{v}\|^2\ .
\end{aligned}$$

Hence (17) is further bounded from below by

$$\alpha^{2(j_2-j_0)}\Big(1-\frac{1}{4}-\frac{1}{2}\Big)\|\mathbf{x}-\mathbf{y}-\mathbf{v}\|^2 \geq \frac{\alpha^4}{4}\|\mathbf{x}-\mathbf{y}-\mathbf{v}\|^2 \geq \frac{\alpha^4}{4}\|\pi_{\widetilde{j_1}}^{\leq}(\mathbf{x}-\mathbf{y}-\mathbf{v})\|^2 .$$

This completes the proof of (10), and the proof of the lemma. ◀

4.5 Summary of Embedding into Tori

By Lemma 4.3, for any lattice $\mathcal{L}$, there exists an $(n\sqrt{n}, n)$-filtration[2] $\mathcal{F}$ of $\mathcal{L}$. Applying Lemmas 4.8 and 4.12 to the embedding $E_{\mathcal{F},\alpha}$ with $\alpha = 1/2$, we have the following.

▶ **Lemma 4.13.** *For any sufficiently large $n \geq 1$ and lattice $\mathcal{L} \subseteq \mathbb{R}^n$, there exists $m \geq 1$ and embedding $F_{\mathcal{L}} = (F_{\mathcal{L},1}, \ldots, F_{\mathcal{L},m})$ such that each $F_{\mathcal{L},j}$ maps the torus $\mathbb{R}^n/\mathcal{L}$ to some other torus, and $F_{\mathcal{L}}$ satisfies*

$$\sum_{j=1}^{m} \mathrm{dist}_{F_{\mathcal{L},j}(\mathbb{R}^n/\mathcal{L})}(F_{\mathcal{L},j}(\mathbf{x}), F_{\mathcal{L},j}(\mathbf{y}))^2 \leq c_{E,u}\cdot \mathrm{dist}_{\mathbb{R}^n/\mathcal{L}}(\mathbf{x},\mathbf{y})^2 \text{ , and}$$

$$\sum_{j=1}^{m} \min\big(\mathrm{dist}_{F_{\mathcal{L},j}(\mathbb{R}^n/\mathcal{L})}(F_{\mathcal{L},j}(\mathbf{x}), F_{\mathcal{L},j}(\mathbf{y})), p(n)\,\lambda_1(F_{\mathcal{L},j}(\mathcal{L}))\big)^2 \geq c_{E,l}\cdot \mathrm{dist}_{\mathbb{R}^n/\mathcal{L}}(\mathbf{x},\mathbf{y})^2 ,$$

where $c_{E,u}$ and $c_{E,l}$ are positive absolute constants and $p(n)$ is a fixed polynomial.

5 Putting it All Together

▶ **Theorem 1.1.** *For any lattice $\mathcal{L} \subseteq \mathbb{R}^n$ there exists a metric embedding of $\mathbb{R}^n/\mathcal{L}$ into Hilbert space with distortion $O(\sqrt{n \log n})$.*

Proof. It suffices to show the embedding for sufficiently large n (by, say, using the embedding from [3] for small n). Consider the composition

$$\Big(H^{(k)}_{F_{\mathcal{L},1}(\mathcal{L})} \circ F_{\mathcal{L},1}, \ldots, H^{(k)}_{F_{\mathcal{L},m}(\mathcal{L})} \circ F_{\mathcal{L},m}\Big) ,$$

where $(F_{\mathcal{L},1}, \ldots, F_{\mathcal{L},m})$ is the embedding provided by Lemma 4.13. Let $k = \lceil \log_2 p(n) \rceil + 1$ (where $p(n)$ is the fixed polynomial in Lemma 4.13). By Lemma 3.6 and Lemma 4.13, noting that the modified contraction properties in both match, it follows immediately that the composed embedding has distortion at most

$$\sqrt{\frac{\pi k n \cdot c_{E,u}}{c_H \cdot c_{E,l}}} ,$$

where c_H, $c_{E,u}$ and $c_{E,l}$ are all absolute constants. Note that $k = \Theta(\log n)$. Hence the distortion of the composed embedding is $O(\sqrt{n \log n})$. ◀

[2] This choice of filtration actually only shows the Lemma 4.13 for sufficiently large n. Choosing a $(32n\sqrt{n}, 32n)$-filtration gives us the lemma for all $n \geq 1$.

References

1 Ishay Haviv and Oded Regev. The Euclidean distortion of flat tori. *J. Topol. Anal.*, 5(2):205–223, 2013. Preliminary version in APPROX 2010. doi:10.1142/S1793525313500064.

2 Piotr Indyk. Algorithmic applications of low-distortion geometric embeddings. In *42nd IEEE Symposium on Foundations of Computer Science (Las Vegas, NV, 2001)*, pages 10–33. IEEE Computer Soc., Los Alamitos, CA, 2001.

3 Subhash Khot and Assaf Naor. Nonembeddability theorems via Fourier analysis. *Math. Ann.*, 334(4):821–852, 2006. Preliminary version in FOCS 2005. doi:10.1007/s00208-005-0745-0.

4 John Milnor and Dale Husemoller. *Symmetric bilinear forms*. Springer-Verlag, New York-Heidelberg, 1973. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 73.