Electronic Colloquium on Computational Complexity, Report No. 66 (2003)

# Almost perfect lattices, the covering radius problem, and applications to Ajtai's connection factor *

Daniele Micciancio†

September 2, 2003

**Abstract**

Lattices have received considerable attention as a potential source of computational hardness to be used in cryptography, after a breakthrough result of Ajtai (STOC 1996) connecting the average-case and worst-case complexity of various lattice problems. The purpose of this paper is twofold. On the expository side, we present a rigorous self contained proof of results along the lines of Ajtai's seminal work. At the same time, we explore to what extent Ajtai's original results can be quantitatively improved. As a by-product, we define a random class of lattices such that computing short nonzero vectors in the class with non-negligible probability is at least as hard as approximating the length of the shortest nonzero vector in *any* $n$-dimensional lattice within worst-case approximation factors $\gamma(n) = n^3\omega(\sqrt{\log n \log\log n})$. This improves previously known best connection factor $\gamma(n) = n^{4+\epsilon}$ (Cai and Nerurkar, FOCS 1997) by more that $\omega(n)$. We also show how our reduction implies the existence of collision resistant cryptographic hash functions based on the worst-case inapproximability of the shortest vector problem within factors $\gamma(n) = n^3\omega(\sqrt{\log n \log\log n})$.

In the process we distill various new lattice problems that might be of independent interest, related to the covering radius, the bounded distance decoding problem, approximate counting of lattice points inside convex bodies, and the efficient construction of lattices with good geometric and algorithmic decoding properties. We also show how further investigation of these new lattice problems might lead to even stronger connections between the average-case and worst-case complexity of the shortest vector problem, possibly leading to connection factors as low as $\gamma(n) = n^{1.5}\omega(\log n)$

## 1 Introduction

It has long been realized that the relevant notion of hardness in cryptography is *average-case* hardness: if the key of a cryptographic function is chosen at random, then no probabilistic polynomial time algorithm can break the scheme with non-negligible probability. In the past few years, computational problems on point lattices have attracted considerable interest for their potential cryptographic applications because of a remarkable connection discovered by Ajtai [1] between their worst-case and average-case complexity. Specifically, Ajtai defined a class of random lattices such that finding short vectors in a lattice chosen uniformly at random from the class is at least as hard as approximating the length of the shortest nonzero vector in any $n$-dimensional lattice (as well as solving various other lattice problems) within a factor polynomial in $n$. This allows to build secure cryptographic functions based on the conjectured *worst-case* intractability of the underlying lattice problem. In particular, [1] showed that if no algorithm can efficiently approximate the length of the shortest nonzero vector in any $n$-dimensional lattice within (worst-case) polynomial approximation factors $\gamma(n) = n^{O(1)}$, then *one-way functions* exist. Subsequently, Goldreich, Goldwasser and Halevi [15] observed that under essentially the same assumptions as Ajtai's, one can prove the existence of *collision resistant hash functions*, a particularly useful kind of one-way function families with many applications in cryptography.

*Preliminary versions of this paper appeared in the proceedings of STOC 2002 with the title "Improved cryptographic hash functions with worst-case/average-case connection" [30], and as Chapter 8 of the book "Complexity of lattice problems: a cryptographic perspective" [31]. Research supported in part by NSF Career Award CCR-0093029.

†University of California, San Diego. La Jolla, California. USA. Email: daniele@cs.ucsd.edu



ISSN 1433-8092

It should be remarked that building cryptographic functions that are as hard to break as the worst case instance of the underlying mathematical problem is especially important in the case of lattices because lattice approximation algorithms (like the LLL algorithm [23]) are believed to perform much better on the average than their worst-case theoretical upper bounds. Still, the worst case approximation factor achieved by the best (probabilistic) polynomial time lattice approximation algorithm known to date [36, 3] is almost exponential in the rank $n$ of the lattice, so it is reasonable to assume that achieving polynomial approximation factors $\gamma(n) = n^{O(1)}$ is computationally hard (in the worst case). However, as lattice problems get easier and easier as the approximation factor $\gamma(n)$ increases, it is both theoretically interesting and practically important to determine the smallest factor $\gamma(n)$ such that finding short vectors in a suitably chosen random lattice is at least as hard as approximating some other lattice problem within worst-case factor $\gamma(n)$.

No specific polynomial $\gamma(n)$ is given in [1]. In fact, the proof in [1] shows[1] that if one can efficiently find short vectors in random lattices with non-negligible probability $\delta(n) = 1/n^{O(1)}$, then one can efficiently approximate the length of the shortest nonzero vector in any $n$-dimensional lattice within a polynomial factor $\gamma(n) = n^{O(1)}/\delta(n)$, where the smaller the success probability $\delta(n)$, the larger the approximation factor $\gamma(n)$.[2] Moreover, even for large $\delta(n)$ (say $\delta(n) = 1/2$), the factor $\gamma(n)$ given by [1] is rather large.[3] Following Ajtai's seminal work, Cai and Nerurkar [8] showed that finding short vectors in Ajtai's random lattices (with non-negligible probability $\delta(n) = 1/n^{O(1)}$) is at least as hard as computing maximal sets of linearly independent vectors that are within a factor $n^{3+\epsilon}$ from the shortest (for any fixed $\epsilon > 0$, independently of the success probability $\delta(n)$). It immediately follows (using standard relations between lattice problems) that finding short vectors in Ajtai's random lattices is at least as hard as approximating the length of the shortest nonzero vector in any $n$-dimensional lattice within a factor $\gamma(n) = n^{4+\epsilon}$.

In this paper we explore to what extent these factors connecting the average-case with the worst-case complexity of lattice problems can be further reduced. In the process, we introduce and start investigating various new lattice problems that might be of independent interest, and are discussed in more detail in the following subsections. On one side, we introduce a kind of lattices (that we call "almost perfect" in analogy with perfect codes), and use them to define a new random class of lattices such that finding short vectors on the average is potentially harder than in the random class proposed by Ajtai. On the other side, we connect the average-case complexity of finding short vectors in our random class to the worst-case complexity of various new lattice problems, like approximating the *covering radius* of a lattice. Using these new problems, we are able to improve the connection factor for the shortest vector problem established in [1, 8]. Specifically, we show that finding short vectors in our random lattices (with non-negligible probability), is at least as hard as

- approximating the length of the shortest nonzero vector in any $n$-dimensional lattice within a factor $\gamma(n) = \tau(n) \cdot n^{2.5}\omega(\log n)$, where $\tau(n) \in [1, \sqrt{n}]$ is a function that depends only on the family of almost perfect lattices used and $\omega(\log n)$ is an arbitrary superlogarithmic function.

Even for $\tau(n) = \sqrt{n}$ (which corresponds to Ajtai's random class of lattices as a special case), this improves the connection factor $\gamma(n) = n^{4+\epsilon}$ of [8] by more than a factor $n$. We also relate the average case complexity of computing short lattice vectors in our random lattices to other (worst-case) lattice problems, like

- computing maximal sets of linearly independent vectors that are within a factor $\gamma(n) = \tau(n) \cdot n^2 \cdot \omega(\log n)$ from the shortest,
- approximating within a factor $\gamma(n) = \tau(n) \cdot n^2 \cdot \omega(\log n)$ the covering radius of any $n$-dimensional lattice,
- finding, given an $n$-dimensional lattice $\mathbf{B}$ and a target point $\mathbf{t}$, a lattice point whose distance from

[1] To be precise, [1] only proves the result for $\delta(n) = 1/2$, and remarks that the proof can be generalized to any non-negligible $\delta(n) = 1/n^{O(1)}$.

[2] It should be remarked that, as observed in [1], setting $\delta(n) = 1/2$ already gives weak one-way functions, which can be transformed (using standard techniques, see [13]) into strong one-way functions based on the hardness of approximating the shortest vector problem within a fixed polynomial factor $\gamma(n) = n^{O(1)}$. However, in order to argue that no efficient algorithm can find short vectors in random lattices with non-negligible probability, [1] seems to require that no efficient algorithm can approximate the worst-case lattice problems within *any* polynomial factors.

[3] No specific value of $\gamma(n)$ is given in [1], but [8] estimates a factor $\gamma(n) = n^8$ can be derived from the proof.

the target $\mathbf{t}$ is at most $\gamma(n) = \tau(n) \cdot n^2 \cdot \omega(\log n)$ times the maximum possible distance $\rho(\mathbf{B}) = \max_{\mathbf{t}'} \text{dist}(\mathbf{t}', \mathcal{L}(\mathbf{B}))$ where $\mathbf{t}'$ ranges over the entire space spanned by $\mathbf{B}$.

Even for $\tau(n) = \sqrt{n}$, the first relation improves previously known best connection factor $n^{3+\epsilon}$ of [8] by more than $\sqrt{n}$. The other two relations are the first results connecting the complexity of finding short vectors to the covering radius problem. Although both problems have not been previously considered in computational complexity, they are both natural computational problems on lattices that might be of independent interest. Computing the covering radius is a problem that is not even known to be solvable in *non-deterministic* polynomial time. The last problem is a "bounded distance decoding" variant of the well studied closest vector problem, where the error instead of being measured with respect to the distance of the given target, is measured with respect to the worst case distance over all possible target vectors.

All our results are obtained as corollaries to a main theorem that shows that finding short vectors in our random lattices is at least as hard as finding maximal sets of linearly independent vectors of length at most $\tau(n)\sqrt{n} \cdot \omega(\log n)$ times a new lattice invariant that we call the "generalized uniform radius". Notice how this factor is extremely small: depending on the value of $\tau(n)$, $\gamma(n)$ can be as small as $\sqrt{n} \cdot \omega(\log n)$ This suggests that further investigation of almost perfect lattices and the connection between the uniform radius and other lattice invariants might lead to even stronger connections between the average-case and worst-case complexity of computing short lattice vectors. In particular, we conjecture that there exists random classes of lattices such that finding short vectors on the average in lattices randomly chosen from the class is at least as hard as approximating the length of the shortest nonzero vector in any $n$-dimensional lattice within a factor $\gamma(n) = n^{1.5} \cdot \omega(\log n)$.

## 1.1 New lattice problems.

Two fundamental constants associated to any lattice are the *packing radius* and the *covering radius*: the packing radius is the largest radius such that (open) spheres centered at distinct lattice points do not intersect, and the packing radius is the smallest radius such that (closed) spheres centered at all lattice points cover the entire space. Equivalently, the *packing radius* can be defined as the largest $r$ such that any (open) sphere of radius $r$ contains *at most one* lattice point. Similarly, the *covering radius* can be defined as the smallest $r$ such that any (closed) sphere of radius $r$ contains *at least one* lattice point. In this paper we introduce a new quantity, the *uniform radius*, defined as the smallest $r$ such that all spheres of radius $r$ contain *approximately the same number* of lattice points. (See Section 3 for a formal definition.) For technical reasons, we introduce also a variant of the uniform radius, the *generalized uniform radius*, which considers not only spheres, but arbitrary convex bodies.

Of all these quantities, only the *packing radius* has received some attention from a computational complexity point of view. It is easy to see that for any lattice, the packing radius equals half the length of the shortest nonzero lattice vector, so (approximately) computing the packing radius is computationally equivalent to computing the (approximate) length of the shortest nonzero lattice vector. (See Subsection 2.2 for a discussion of the computational complexity of this problem.)

Determining the *covering radius* of a lattice is a classic problem in the geometry of numbers, but it has received so far very little attention from a computational complexity point of view. We suggest that the covering radius is, by itself, an interesting problem to be studied as a potential source of computational hardness. No NP-hardness result for the problem is known at the time of this writing. However, the exact solution to the covering radius problem is not even known to be computable in NP (non-deterministic polynomial time), and the analogous problem for linear codes is known to be complete for the second level of the polynomial hierarchy [26], a class of problems presumably much harder than NP-complete ones.

The problem of estimating the *(generalized) uniform radius*, has been implicitly considered before in connection with vector quantization [25], and volume estimation problems [21], but only for the special case of the integer lattice $\mathbb{Z}^n$ and specific convex bodies (spheres or polyhedra). In this paper we generalize this natural geometric problem to arbitrary lattices and convex bodies, and show how the problem naturally arises in the analysis of the average-case hardness of lattice problems.

## 1.2 Almost perfect lattices.

The packing radius and covering radius have been extensively studied in coding theory. *Codes* are sets of strings (called *codewords*) of some fixed length $n$ over a finite alphabet $\Sigma$, with the (Hamming) distance between strings measured as the number of positions in which the two strings differ. Similarly to lattices, the packing radius and covering radius of a code are defined as the largest and smallest radii such that the Hamming spheres centered at codewords are disjoint or cover the entire space $\Sigma^n$, respectively. A code is called *perfect* if the packing radius equals the covering radius. In other words, the code is perfect if it is possible to partition the entire space $\Sigma^n$ with equal (Hamming) spheres centered at the codewords. Interestingly, perfect codes are rare but do exist (see [17, Section 5]). However, the same is not true for lattices: it is not possible to partition the Euclidean space $\mathbb{R}^n$ with equal spheres of radius bounded away from 0. However, one can attempt to partition Euclidean space with almost spherical bodies. Any lattice naturally defines a partition of space into regions, the *Voronoi cells*, each associated to a lattice point. The cell of lattice point $\mathbf{x}$ is the set of all points that are closer to $\mathbf{x}$ than to any other lattice point. It is easy to see that each Voronoi cell contains a sphere of radius equal to the packing radius, and is completely contained in a sphere of radius equal to the covering radius. The covering radius is always at least as large as the packing radius, and the smaller the gap between the two radii, the closer the Voronoi cells to perfect spheres. We say that a lattice is $\tau$-perfect if the covering radius is at most $\tau$ times the packing radius. We are interested in lattices that are $\tau$-perfect for $\tau > 1$ as small as possible. Notice that the integer lattice $\mathbb{Z}^n$ is $\tau(n)$-perfect for $\tau(n) = \sqrt{n}$, so we can assume without loss of generality that $\tau(n) \in [1, \sqrt{n}]$. We say that a sequence of lattices is *almost perfect* if it is $\tau(n)$-perfect for some constant $\tau(n) = O(1)$ independent of the dimension $n$. With some abuse of terminology, we will also informally use the term "almost perfect" to refer to any $\tau(n)$-perfect lattice where $\tau(n) = o(\sqrt{n})$ is asymptotically better than the integer lattice $\mathbb{Z}^n$.

Another fundamental problem in coding theory is the maximum likelihood decoding: given a target point, find the codeword closest to the target. The analogous problem on lattices is usually called the closest vector problem: given a lattice and a target vector, find the lattice point closest to it. Differently from lattices, in coding theory most work has focused on finding efficient decoding algorithms for specific codes, whereas in the closest vector problem the lattice is usually considered as part of the input. In this paper, we consider the lattice decoding problem for specific lattices. We say that a lattice is *easily decodable* if there is an efficient algorithm that on input a target point, outputs the lattice point closest to the target. (Formally, we need to consider a sequence of lattices in higher and higher dimension. See Section 4 for details.) For example, the integer lattice $\mathbb{Z}^n$ is easily decodable: given a target point $\mathbf{y} \in \mathbb{Q}^n$, the closest lattice point is easily found by rounding each coordinate of $\mathbf{y}$ to the closest integer.

The random classes of lattices defined in this paper are based on easily decodable $\tau(n)$-perfect lattices, and the smaller $\tau(n)$ is, the harder is to find short vectors in the random lattices. So, it is natural to ask what is the smallest value of $\tau(n)$ for which we can efficiently build *easily decodable* $\tau(n)$-perfect lattices. It is known [35, 7] that almost perfect lattices exist. Unfortunately, the proofs in [35, 7] do not give an efficient procedure to build and decode these lattices. Various examples of easily decodable lattices are given in [9], but they are all $\tau(n)$-perfect for $\tau(n) = \Theta(\sqrt{n})$. It is natural to ask if almost perfect easily decodable lattices exist at all. In this paper we initiate the study of almost perfect lattices from a computational point of view, and we give the first efficient construction of easily decodable lattices with $\tau(n) = O(\sqrt{n \log\log n / \log n})$ asymptotically smaller than $\sqrt{n}$.

Our almost perfect lattices allow to slightly improve (by a factor $O(\sqrt{\log n / \log\log n})$) the connection between the worst-case and average-case complexity of lattice problems. Although not substantial, this improvement in the connection factor is significant because it shows that there are random classes of lattices for which finding short vectors is potentially harder than for the random class originally considered by Ajtai. Moreover, it suggests that it might be possible to find even better easily decodable almost perfect lattices that allow to further reduce the connection factors for all lattice problems considered in this paper by almost $\sqrt{n}$.

## 1.3 Related work

This work is directly builds upon techniques of Ajtai [1], Cai and Nerurkar [8] and Goldreich, Goldwasser and Halevi [15], and it is the final version of [30]. Below we review some additional papers that are less

directly related, but still relevant to this work.

The question of determining under what conditions the number of lattice points inside a convex body $\mathcal{Q}$ is roughly proportional to the volume has been extensively studied, but mostly for the case of the integer lattice $\mathbb{Z}^n$. For example Mazo and Odlyzko [25] study the problem when $\mathcal{Q}$ is a sphere of radius $r$, in connection with universal quantization and low density subset sum problems. In particular they show that for $r = O(\sqrt{n})$ the number of integer lattice points in the sphere can deviate from the expected value by factors exponential in $n$, but claim that if $r = n^{1/2+\epsilon}$ (for any $\epsilon > 0$) then the number of integer lattice points in the sphere is always asymptotic to the volume, no matter where the center is located. A different class of convex bodies is considered by Kannan and Vempala in [21], but, as usual, only for the special case of the integer lattice $\mathbb{Z}^n$. In [21] $\mathcal{Q}$ is an $n$-dimensional convex polytope with $m$ facets, and the result is that the number of integer lattice points in $\mathcal{Q}$ is proportional to the volume provided that $\mathcal{Q}$ contains a sphere of radius $O(n \cdot \sqrt{\log m})$.[4] A result for arbitrary convex bodies is proved by Dyer, Frieze and Kannan [11] who show that the number of integer lattice points in $\mathcal{Q}$ is proportional to the volume of $\mathcal{Q}$, provided $\mathcal{Q}$ contains a sphere of radius $O(n^{1.5})$. In Section 3 we generalize the result of [11] to arbitrary lattices, and show that the number of lattice points in $\mathcal{Q}$ is proportional to the volume provided that $\mathcal{Q}$ contains a sphere of radius $O(n)$ times bigger than the covering radius of the lattice (see Theorem 1).

The covering radius problem has been extensively studied from a mathematical point of view, leading for example to the transference theorems of Banaszczyk [4], but it has received little or no attention from a computational point of view. Two relevant results about the covering radius problem are McLoughlin's proof [26] that the analogous problem on linear codes is hard for the second level of the polynomial hierarchy, and Kannan's algorithm [20] showing that a variant of the covering radius problem (where the norm defined by an input parallelotope is used, instead of the usual Euclidean norm) can be solved in polynomial time for any fixed dimension. Kannan's result is quite remarkable because finding fixed dimension polynomial time algorithms for problems at the second level of the polynomial hierarchy is usually much harder than for problems solvable in non-deterministic polynomial time.

The problem of decoding specific lattices has been considered in coding theory, for example in connection with vector quantization. In [9] Conway and Sloane give polynomial time decoding algorithms for the root lattices $A_n, D_n$ and their duals $A_n^*, D_n^*$, as well as various other low dimensional lattices.[5] From a computational complexity point of view, the problem has been considered under the name "closest vector problem with preprocessing". Adapting similar results of Bruck and Naor [6] and Lobstein [24] for coding and subset-sum problems, Micciancio [27] showed that there are sequences of lattices such that solving the closest vector problem is NP-hard. These results have been improved by Feige and Micciancio [12] and then Regev [33] to show that (unless P = NP) there are lattices and codes that cannot be efficiently decoded even approximately, up to some constant factor. Notice that the goal of [27, 12, 33] is opposite to ours: while [27, 12, 33] give explicit constructions of lattices that cannot be easily decoded, in this paper we search for explicit constructions of easily decodable lattices.

Almost perfect lattices have been extensively studied from a mathematical point of view. In particular, Rogers [35] proved that there exist $\tau(n)$-perfect lattices for $\tau(n) < 3$, and Butler [7] improved the result to $\tau(n) = 2 + o(1)$. Our exponential time construction of almost perfect lattices in Theorem 2 is essentially an algorithmic variant of the Rogers' proof. Butler's proof does not seem to easily yield any algorithm.

In this paper we consider the worst case complexity of computing short vectors (as well as solving other computational lattice approximation problems) in *any* lattice. In a recent breakthrough paper [34], Regev has given encryption schemes and collision resistant hash functions that are as hard to break as computing shortest nonzero vectors in lattices with *special structure*. The results proved in [34] achieve approximation factors $O(n^{1.5})$ smaller than any other known reduction, but only for lattices where the shortest vector is *unique* is some technical sense. This special structure is common in the construction of lattice based public key encryption schemes [2], but does not seem necessary to build one-way or collision resistant hash functions. In Section 9 we explain how the techniques presented in this paper might lead to one-way and collision resistant hash functions that are as hard to break as solving the shortest vector problem (or other

[4] As a side remark, the motivation to study this problem in [21] is somehow opposite to ours, as they count the number of lattice points in a polytope to estimate its volume. Here, we try to get a bound on the number of lattice points, for convex bodies $\mathcal{Q}$ of known volume.

[5] Asymptotically, only results for infinite families of lattices are interesting because the closest vector problem is known to be solvable in polynomial time in any fixed dimension [19].

lattice problems) in *any* lattice, within approximation factors similar to those established in [34] for the special class of lattices possessing unique shortest vectors.

### 1.4 Outline.

The rest of the paper is organized as follows. In Section 2 we introduce some notation and give some background about lattice problems and their computational complexity. In Section 3 we define the (generalized) uniform radius and relate it to other lattice quantities. In Section 4 we initiate the algorithmic study of almost perfect lattices and present a polynomial time construction of easily decodable $\tau(n)$-perfect lattices with $\tau(n) = o(\sqrt{n})$. These lattices are used in Section 5 to define a new random class of lattices that generalizes Ajtai's one. In Sections 6 and 7 we prove that finding short vectors in the random lattices of Section 5 is at least as hard as finding short (relative to the generalized uniform radius) linearly independent vectors in the worst case. In Section 8 we relate this problem to other well known lattice problems, like approximating the length of the shortest vector in a lattice. Section 9 concludes with a brief summary of our main results, and some open problems whose solution would allow to improve the connection factors established in this paper.

## 2 Preliminaries

In this section, after introducing some notation that will be used in the paper, we briefly recall some basic notions about lattices (including their computational complexity and their connection with finite groups) and statistical distance. For more detailed exposition of this background material the reader is referred to [31].

For any finite set $S$, the size of $S$ is denoted $\#S$. Let $\mathbb{R}$ and $\mathbb{Z}$ be the sets of the reals and the integers, respectively. The $m$-dimensional Euclidean space is denoted $\mathbb{R}^m$. We use bold lower case letters (e.g., $\mathbf{x}$) to denote vectors, and bold upper case letters (e.g., $\mathbf{M}$) to denote matrices. If $\mathcal{Q} \subseteq \mathbb{R}^n$ is an arbitrary region of space, and $\mathbf{x} \in \mathbb{R}^n$ is a vector, $\mathcal{Q} + \mathbf{x} = \{\mathbf{y} + \mathbf{x} \colon \mathbf{y} \in \mathcal{Q}\}$ denotes a copy of $\mathcal{Q}$ shifted by $\mathbf{x}$. The $\ell_2$ norm of a vector $\mathbf{x} \in \mathbb{R}^n$ is defined as $\|\mathbf{x}\| = \sqrt{\sum x_i^2}$. For a matrix $\mathbf{M} = [\mathbf{m}_1, \ldots, \mathbf{m}_n]$, we define $\|\mathbf{M}\| = \max_i \|\mathbf{m}_i\|$, where $\mathbf{m}_i$ are the columns of $\mathbf{M}$. For vector $\mathbf{x} \in \mathbb{R}^n$ and set $S \subseteq \mathbb{R}^n$, let $\mathrm{dist}(\mathbf{v}, S) = \min_{\mathbf{w} \in S} \|\mathbf{v} - \mathbf{w}\|$ be the distance between $\mathbf{v}$ and $S$. For vector $\mathbf{x} \in \mathbb{R}^n$ and real $r$, let $\mathcal{B}(\mathbf{v}, r) = \{\mathbf{w} \in \mathbb{R}^n : \mathrm{dist}(\mathbf{v}, \mathbf{w}) < r\}$ be the open ball of radius $r$ centered in $\mathbf{v}$, and $\bar{\mathcal{B}}(\mathbf{v}, r) = \{\mathbf{w} \in \mathbb{R}^n : \mathrm{dist}(\mathbf{v}, \mathbf{w}) \leq r\}$ its topological closure. When the center $\mathbf{v} = \mathbf{0}$ is the origin, then we simply write $\mathcal{B}(r)$ and $\bar{\mathcal{B}}(r)$. We often use matrix notation to denote sets of vectors. For example, matrix $\mathbf{S} \in \mathbb{R}^{m \times n}$ represents the set of $m$-dimensional vectors $\{\mathbf{s}_1, \ldots, \mathbf{s}_n\}$, where $\mathbf{s}_1, \ldots, \mathbf{s}_n$ are the columns of $\mathbf{S}$. The linear space spanned by a set of vectors $\mathbf{S}$ is denoted $\mathrm{span}(\mathbf{S})$. For any set of linearly independent vectors $\mathbf{S}$, we define the half open parallelepiped $\mathcal{P}(\mathbf{S}) = \{\mathbf{S}\mathbf{x} : 0 \leq x_i < 1\}$.

For any two positive reals $a, b \geq 0$, we write $a \gtrsim b$ if $a \geq (1/2) \cdot b$, and $a \lesssim b$ if $a \lesssim (3/2) \cdot b$. We say that $a$ is approximately equal to $b$ (written $a \approx b$), if both $a \lesssim b$ and $a \gtrsim b$, i.e., the relative additive error $|a - b|/b$ is at most $1/2$. Notice that $a \approx b$ is not a symmetric relation, i.e., $a \approx b$ does not imply $b \approx a$. For any $a, b, c \geq 0$, if $a \approx c$ and $b \approx c$, then $a$ and $b$ are within a factor 3 from the other, i.e., $a/3 \leq b \leq 3a$.

### 2.1 Lattices

An $m$-dimensional *lattice* is the set of all integer combinations $\{\sum_{i=1}^{n} x_i \mathbf{b}_i \colon x_i \in \mathbb{Z}\}$ of $n$ linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$ in $\mathbb{R}^m$ $(m \geq n)$. The set of vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$ is called a *basis* for the lattice, and the integer $n = \dim(\mathrm{span}(\mathbf{B}))$ is called the *rank* of the lattice. If the rank $n$ equals the dimension $m$, then the lattice is called *full rank* or *full dimensional*. Lattices are infinite Abelian groups with respect to the vector addition operation, and can be equivalently defined as discrete additive subgroups of $\mathbb{R}^m$. A basis can be compactly represented by the matrix $\mathbf{B} = [\mathbf{b}_1 | \ldots | \mathbf{b}_n] \in \mathbb{R}^{m \times n}$ having the basis vectors as columns. The lattice generated by $\mathbf{B}$ is denoted $\mathcal{L}(\mathbf{B})$. Notice that $\mathcal{L}(\mathbf{B}) = \{\mathbf{B}\mathbf{x} \colon \mathbf{x} \in \mathbb{Z}^n\}$, where $\mathbf{B}\mathbf{x}$ is the usual matrix-vector multiplication. We use notation $\mathcal{L}(\mathbf{B})$ to denote the set $\{\mathbf{B}\mathbf{x} \colon \mathbf{x} \in \mathbb{Z}^n\}$ even when vectors $\mathbf{B}$ are not linearly independent.

The *minimum distance* of a lattice $\mathcal{L}(\mathbf{B})$, (denoted $\lambda_1(\mathbf{B})$), is the minimum distance between any two (distinct) lattice points and equals the length of the shortest nonzero lattice vector:

$$\lambda_1(\mathbf{B}) = \min\{\mathrm{dist}(\mathbf{x},\mathbf{y}) : \mathbf{x} \neq \mathbf{y} \in \mathcal{L}(\mathbf{B})\} = \min\{\|\mathbf{x}\| : \mathbf{x} \in \mathcal{L}(\mathbf{B}) \setminus \{\mathbf{0}\}\}.$$

This definition can be generalized to define the $i$th successive minimum as the smallest $\lambda_i$ such that $\bar{\mathcal{B}}(\lambda_i)$ contains $i$ linearly independent lattice points:

$$\lambda_i(\mathbf{B}) = \min\{r\colon \dim(\mathrm{span}(\mathcal{L}(\mathbf{B}) \cap \bar{\mathcal{B}}(r))) \geq i\}$$

Another important constant associated to a lattice is the covering radius: the covering radius $\rho(\mathbf{B})$ of a lattice is the maximum distance $\mathrm{dist}(\mathbf{x}, \mathcal{L}(\mathbf{B}))$ where $\mathbf{x}$ ranges over the linear span of $\mathbf{B}$:

$$\rho(\mathbf{B}) = \max_{\mathbf{x} \in \mathrm{span}(\mathbf{B})} \{\mathrm{dist}(\mathbf{x}, \mathcal{L}(\mathbf{B}))\}.$$

A sublattice of $\mathcal{L}(\mathbf{B})$ is a lattice $\mathcal{L}(\mathbf{S})$ such that $\mathcal{L}(\mathbf{S}) \subseteq \mathcal{L}(\mathbf{B})$. $\mathcal{L}(\mathbf{S})$ is a *full rank* sublattice of $\mathcal{L}(\mathbf{B})$ if it has the same rank as $\mathcal{L}(\mathbf{B})$. The determinant of a (rank $n$) lattice $\det(\mathcal{L}(B))$ is the ($n$-dimensional) volume of the fundamental parallelepiped $\mathcal{P}(\mathbf{B})$. If $\mathcal{L}(\mathbf{B})$ is full dimensional, then $\det(\mathcal{L}(\mathbf{B}))$ equals the absolute value of the determinant of the $n \times n$ basis matrix $|\det(\mathbf{B})|$. Hadamard's bound give a simple way to bound the determinant of a lattice as $\det(\mathcal{L}(\mathbf{B})) \leq \prod_i \|\mathbf{b}_i\|$. Hadamard's bound can be much larger than the actual value of the determinant, and it equals the determinant if and only if the basis $\mathbf{B}$ is orthogonal. The ratio $\mathrm{defect}(\mathbf{B}) = \prod_i \|\mathbf{b}_i\| / \det(\mathcal{L}(\mathbf{B}))$ is called the *orthogonality defect* of $\mathbf{B}$. Minkowski's first theorem states that any rank $n$ lattice $\mathcal{L}(\mathbf{B})$ contains a nonzero vector of length at most

$$\lambda_1(\mathbf{B}) \leq \sqrt{n}\det(\mathcal{L}(\mathbf{B}))^{1/n}.$$

The following definition plays an important role in our proofs.

**Definition 1** *Let $\Lambda$ be a lattice and $\mathbf{x} \in \Lambda$ an arbitrary lattice point. The (open)* Voronoi *cell of $\mathbf{x}$ is the set $\mathcal{V}(\mathbf{x}, \Lambda)$ of all points $\mathbf{z} \in span(\Lambda)$ that are closer to $\mathbf{x}$ than to any other lattice point:*

$$\mathcal{V}(\mathbf{x}, \Lambda) = \{\mathbf{z} \in span(\Lambda) \mid \forall \mathbf{y} \in \mathcal{L}(\mathbf{B}).\, \mathrm{dist}(\mathbf{z}, \mathbf{x}) < \mathrm{dist}(\mathbf{z}, \mathbf{y})\}.$$

*The closed cell $\bar{\mathcal{V}}(\mathbf{x}, \Lambda)$ is the topological closure of $\mathcal{V}(\mathbf{x}, \Lambda)$, i.e., the set of all points that are at least as close to $\mathbf{x}$ as to any other lattice point:*

$$\bar{\mathcal{V}}(\mathbf{x}, \Lambda) = \{\mathbf{z} \in span(\Lambda) \mid \forall \mathbf{y} \in \mathcal{L}(\mathbf{B}).\, \mathrm{dist}(\mathbf{z}, \mathbf{x}) \leq \mathrm{dist}(\mathbf{z}, \mathbf{y})\}. \quad (1)$$

For simplicity, the Voronoi cell of the origin $\mathbf{x} = \mathbf{0}$ is denoted $\mathcal{V}(\Lambda)$. We need some simple properties about Voronoi cells, as listed below. All properties are easily verified and their proof is left to the reader.

**Proposition 1** *Let $\Lambda$ be a lattice with covering radius $\rho$ and minimum distance $\lambda_1$. Then the Voronoi cells of $\Lambda$ satisfy the following properties:*

- *All Voronoi cells $\mathcal{V}(\mathbf{x}, \Lambda)$ (with $\mathbf{x} \in \Lambda$) are shifted copies $\mathcal{V}(\mathbf{x}, \Lambda) = \mathcal{V}(\Lambda) + \mathbf{x}$ of the fundamental cell associated to the origin.*
- *$\mathcal{V}(\mathbf{x}, \Lambda)$ is a bounded, open, convex set, symmetric about lattice point $\mathbf{x}$.*
- *Each cell $\mathcal{V}(\mathbf{x}, \Lambda)$ contains a sphere of radius $\lambda_1/2$, and it is completely contained in a sphere of radius $\rho$: $\mathcal{B}(\mathbf{x}, \lambda_1/2) \subset \mathcal{V}(\mathbf{x}, \Lambda) \subset \mathcal{B}(\mathbf{x}, \rho)$.*
- *The volume of $\mathcal{V}(\mathbf{x}, \Lambda)$ (or, equivalently, $\bar{\mathcal{V}}(\mathbf{x}, \Lambda)$) equals $\mathrm{vol}(\mathcal{V}(\mathbf{x}, \Lambda)) = \mathrm{vol}(\bar{\mathcal{V}}(\mathbf{x}, \Lambda)) = \det(\Lambda)$.*
- *For any two distinct lattice points $\mathbf{x} \neq \mathbf{y} \in \Lambda$, the corresponding Voronoi cells are disjoint, i.e., $\mathcal{V}(\mathbf{x}, \Lambda) \cap \bar{\mathcal{V}}(\mathbf{y}, \Lambda) = \emptyset$.*
- *The union of all closed Voronoi cells covers the entire space, i.e., $\bigcup_{\mathbf{x} \in \Lambda} \bar{\mathcal{V}}(\mathbf{x}, \Lambda) = span(\Lambda)$ .*

## 2.2 Computational problems on lattices

When discussing computational issues related to lattices, it is customary to assume that the lattices are represented by a basis matrix $\mathbf{B}$ and that $\mathbf{B}$ has integer entries. Other representations are possible, e.g., an integer lattice can be defined as the set of integer solutions to a system of homogeneous modular linear equations. These alternative representations are computationally equivalent to giving a basis, i.e., for example, given a system of homogeneous modular linear equations one can compute in polynomial time a basis for the corresponding lattice.

In this paper we consider the following problems on lattices. All problems are defined in their approximation version, where the approximation factor $\gamma(n)$ can be a function of the rank $n$ of the lattice. The exact version of the problems correspond to approximation factor $\gamma(n) = 1$.

**Definition 2** *The* Shortest Vector Problem *(*SVP*), given a lattice basis* $\mathbf{B}$*, asks for a nonzero lattice vector* $\mathbf{v} \in \mathcal{L}(\mathbf{B})$ *of length at most* $\gamma(n) \cdot \lambda_1(\mathbf{B})$*. The problem can be defined also in a* length estimation *version, where given a basis* $\mathbf{B}$*, one only has to find a value* $\hat{\lambda}_1$ *such that* $\lambda_1(\mathbf{B}) \leq \hat{\lambda}_1 \leq \gamma(n) \cdot \lambda_1(\mathbf{B})$.

The two versions of the problem are not known to be equivalent for $\gamma(n) > 1$, i.e., given an oracle to (approximately) compute the length of the shortest nonzero lattice vector in any lattice, it is not clear how to find short lattice vectors.[6] The shortest vector problem is NP-hard (under randomized reductions), even in its length estimation version, for any approximation factors $\gamma(n) < \sqrt{2}$ [29]. The (decision version of the) problem is clearly solvable in NP. For $\gamma(n) = O(\sqrt{n/\log n})$ the problem is in coAM [14], and for $\gamma(n) = n$ it is also in coNP [22, 4]. Finally, when $\gamma(n) = e^{O(n \log\log n/\log n)}$ the problem can be solved in random polynomial time [3], and deterministic polynomial time solutions are known only for $\gamma(n) = e^{O(n(\log\log n)^2/\log n)}$ [36].

**Definition 3** *The* Shortest Independent Vectors Problem *(*SIVP*), given a lattice basis* $\mathbf{B}$ *of rank* $n$*, asks for a set of* $n$ *linearly independent lattice vectors* $\mathbf{S} \subseteq \mathcal{L}(\mathbf{B})$ *such that* $\|\mathbf{S}\| \leq \gamma(n) \cdot \lambda_n(\mathbf{B})$*. The problem can be defined also in a* length estimation *version, where given a basis* $\mathbf{B}$*, one only has to find a value* $\hat{\lambda}_n$ *such that* $\lambda_n(\mathbf{B}) \leq \hat{\lambda}_n \leq \gamma(n) \cdot \lambda_n(\mathbf{B})$.

SIVP is NP-hard (as usual, already in the length estimation version) for any constant factor $\gamma(n) = O(1)$ [5]. The (decision version of) SIVP is clearly in NP. On the algorithmic side, it is possible to reduce approximating SIVP within a factor $\sqrt{n} \cdot \gamma(n)$ (or $n\gamma(n)$ in the length estimation version) to approximating SVP within a factor $\gamma(n)$. This immediately gives polynomial time algorithms for approximation factors $\gamma(n) = e^{O(n(\log\log n)^2/\log n)}$.

**Definition 4** *The* Covering Radius Problem *(*CRP*), given a lattice basis* $\mathbf{B}$*, asks for a value* $\hat{\rho}$ *such that* $\rho(\mathbf{B}) \leq \hat{\rho} \leq \gamma(n) \cdot \rho(\mathbf{B})$.

At the time of this writing, no NP-hardness result is known for CRP. However, we do not even know how to solve the problem (in its exact version, i.e., $\gamma(n) = 1$) in non-deterministic polynomial time (NP), and the analogous problem for linear codes is known to be hard for the second level of the polynomial hierarchy [26]. So, it is reasonable to conjecture that the same is true for the covering radius problem on lattices.

**Definition 5** *The* Closest Vector Problem *(*CVP*), given a lattice basis* $\mathbf{B}$ *and target vector* $\mathbf{t}$*, asks for a lattice point* $\mathbf{v} \in \mathcal{L}(\mathbf{B})$ *such that* $\mathrm{dist}(\mathbf{t}, \mathbf{v}) \leq \gamma(n) \cdot \mathrm{dist}(\mathbf{t}, \mathcal{L}(\mathbf{B}))$*. The problem can be defined also in a* distance estimation *version, where given a basis* $\mathbf{B}$ *and target* $\mathbf{t}$*, one only has to find a value* $\hat{d}$ *such that* $\mathrm{dist}(\mathbf{t}, \mathcal{L}(\mathbf{B})) \leq \hat{d} \leq \gamma(n) \cdot \mathrm{dist}(\mathbf{t}, \mathcal{L}(\mathbf{B}))$.

The closest vector problem is known to be at least as hard as the shortest vector problem [16] for any approximation factor $\gamma(n)$. Moreover, it is NP-hard for quasi polynomial approximation factors $\gamma(n) = n^{O(1/\log\log n)}$ [10]. For $\gamma(n) = O(\sqrt{n/\log n})$ the problem is in coAM [14], and for $\gamma(n) = n$ the problem

[6] A reduction for the exact case ($\gamma = 1$) is given in [18]. This is the only direct reduction known to date. Technically, a reduction between the two problems also exists for approximation factors $\gamma$ for which approximating $\lambda_1$ is NP-hard or finding short vectors is solvable in polynomial time. No reduction is known for any other intermediate approximation factor.

is also in coNP [22, 4]. Finally, the problem can be approximated in deterministic polynomial time within $\gamma(n) = e^{O(n(\log\log n)^2/\log n)}$ [36, 18].

In the closest vector problem, the target point $\mathbf{t}$ can be arbitrarily far from the lattice. In coding theory, Vardy [37] has considered a variant of the closest vector problem where the distance of the target from the code is guaranteed to be less than the packing radius of the code. This problem (called the *bounded distance decoding* problem, BDD) is interesting because decoding within the packing radius, if solvable, has unique solution. (For this reason, the packing radius is sometime called also the "unique decoding" radius.) For lattices, the analogous problem would be the following: given a lattice $\mathbf{B}$ and a point $\mathbf{t}$ within distance $d = \lambda_1(\mathbf{B})/2$ from $\mathcal{L}(\mathbf{B})$, find a (unique) lattice point within distance $d$ from $\mathbf{t}$. In general we can consider the bounded distance decoding problem on lattices for values of $d$ different from $\lambda_1(\mathbf{B})/2$, although when $d > \lambda_1(\mathbf{B})/2$ the solution is not guaranteed to be unique. Another interesting case is when $d = \rho(\mathbf{B}) = \max_{\mathbf{x}} \mathrm{dist}(\mathbf{x}, \mathcal{L}(\mathbf{B}))$ equals the covering radius of the lattice. This value is interesting because there is always a lattice point within distance $\rho(\mathbf{B})$ from the target. Below we formally define an approximation version of this problem.

**Definition 6** *The* Covering Bounded Distance Decoding *problem (*BDD$^\rho$*), given a lattice* $\mathbf{B}$ *and a target point* $\mathbf{t} \in$ *span*$(\mathbf{B})$*, asks for a lattice point* $\mathbf{x} \in \mathcal{L}(\mathbf{B})$ *such that* $\|\mathbf{t} - \mathbf{x}\| \leq \gamma(n)\rho(\mathbf{B})$.

The following relations are known among the parameters of a lattice $\mathcal{L}(\mathbf{B})$ (see [31, 4]).

**Proposition 2** *For any rank* $n$ *lattice* $\mathbf{B}$*,*

$$\lambda_1(\mathbf{B}) \leq \lambda_n(\mathbf{B}) \leq 2\rho(\mathbf{B}) \leq \sqrt{n}\lambda_n(\mathbf{B}). \tag{2}$$

*Moreover, if* $\mathbf{B}^*$ *is the dual lattice*[7] *of* $\mathbf{B}$*, then*

$$1 \leq \lambda_1(\mathbf{B})2\rho(\mathbf{B}^*) \leq n \tag{3}$$

*and*

$$1 \leq \lambda_1(\mathbf{B})\lambda_n(\mathbf{B}^*) \leq n. \tag{4}$$

## 2.3 Lattices and Groups

Let $\mathcal{L}(\mathbf{L})$ be a lattice. Any sublattice $\mathcal{L}(\mathbf{M}) \subseteq \mathcal{L}(\mathbf{L})$ defines a natural equivalence relation on $\mathcal{L}(\mathbf{L})$ as follows: two lattice points $\mathbf{x}, \mathbf{y} \in \mathcal{L}(\mathbf{L})$ are equivalent (written $\mathbf{x} \equiv_{\mathbf{M}} \mathbf{y}$) if and only if $\mathbf{x} - \mathbf{y} \in \mathcal{L}(\mathbf{M})$. The reader can easily check that $\equiv_{\mathbf{M}}$ is an equivalence relation, i.e., it is reflexive ($\mathbf{x} \equiv_{\mathbf{M}} \mathbf{x}$), symmetric ($\mathbf{x} \equiv_{\mathbf{M}} \mathbf{y} \Leftrightarrow \mathbf{y} \equiv_{\mathbf{M}} \mathbf{x}$) and transitive ($\mathbf{x} \equiv_{\mathbf{M}} \mathbf{y} \wedge \mathbf{y} \equiv_{\mathbf{M}} \mathbf{z} \Rightarrow \mathbf{x} \equiv_{\mathbf{M}} \mathbf{z}$). The $\equiv_{\mathbf{M}}$-equivalence class of $\mathbf{x} \in \mathcal{L}(\mathbf{L})$ (denoted $[\mathbf{x}]_{\mathbf{M}}$) is the set of all $\mathbf{y} \in \mathcal{L}(\mathbf{L})$ such that $\mathbf{x} \equiv_{\mathbf{M}} \mathbf{y}$. The quotient $\mathcal{L}(\mathbf{L})/\mathcal{L}(\mathbf{M})$ is the set of all $\equiv_{\mathbf{M}}$-equivalence classes of $\mathcal{L}(\mathbf{L})$. The equivalence relation $\equiv_{\mathbf{M}}$ is a congruence relation with respect to the addition operation, i.e., if $\mathbf{x} \equiv_{\mathbf{M}} \mathbf{x}'$ and $\mathbf{y} \equiv_{\mathbf{M}} \mathbf{y}'$, then $(\mathbf{x} + \mathbf{y}) \equiv_{\mathbf{M}} (\mathbf{x}' + \mathbf{y}')$. It follows that for any two equivalence classes $[\mathbf{x}]_{\mathbf{M}}$ and $[\mathbf{y}]_{\mathbf{M}}$, the sum $[\mathbf{x} + \mathbf{y}]_{\mathbf{M}}$ is well defined, i.e., it does not depend on the choice of representatives $\mathbf{x}$, $\mathbf{y}$, and the quotient $\mathcal{L}(\mathbf{L})/\mathcal{L}(\mathbf{M})$ is an additive group with the sum operation just described. Notice that if $\mathcal{L}(\mathbf{L})$ is regarded as an Abelian group, then sublattice $\mathcal{L}(\mathbf{M})$ is a subgroup of $\mathcal{L}(\mathbf{L})$ and $(\mathcal{L}(\mathbf{L})/\mathcal{L}(\mathbf{M}), +)$ is just the standard quotient group.

Group $\mathcal{L}(\mathbf{L})/\mathcal{L}(\mathbf{M})$ is finite if and only if $\mathcal{L}(\mathbf{M})$ is a full rank sublattice of $\mathcal{L}(\mathbf{L})$, in which case, the cardinality of the group is

$$\#(\mathcal{L}(\mathbf{L})/\mathcal{L}(\mathbf{M})) = |\det(\mathbf{M})/\det(\mathbf{L})|.$$

Elements of this group can be represented using several standard techniques, e.g., selecting a unique representative from each equivalence class. It is easy to see that for every equivalence class $[\mathbf{x}]_{\mathbf{M}}$ there exists a

[7] The dual lattice of $\mathcal{L}(\mathbf{B})$ is the set of all vectors $\mathbf{x} \in \mathrm{span}(\mathbf{B})$ that have integer scalar product with all lattice vectors. We won't use any property of dual lattices other The only properties of dual lattices used in this paper (beside the one stated in the proposition) are that a basis for the dual lattice can be computed in polynomial time given $\mathbf{B}$, and that the dual of the dual is the original lattice.

unique element $\mathbf{x}' \in \mathcal{L}(\mathbf{L}) \cap \mathcal{P}(\mathbf{M})$ such that $\mathbf{x} \equiv_{\mathbf{M}} \mathbf{x}'$. So, a possible set of (unique) representatives is given by the set

$$\mathcal{L}(\mathbf{L}) \cap \mathcal{P}(\mathbf{M})$$

of all lattice points that belong to the half open parallelepiped $\mathcal{P}(\mathbf{M})$. Given an arbitrary lattice point $\mathbf{x} \in \mathcal{L}(\mathbf{B})$, the corresponding representative can be efficiently computed as follows: write $\mathbf{x}$ as $\mathbf{Mz}$, define $z_i' = \lfloor z_i \rfloor$ for all $i = 1, \ldots, n$, and set $\mathbf{x}' = \mathbf{M}(\mathbf{z} - \mathbf{z}')$.

The representation of group elements using vectors in $\mathcal{P}(\mathbf{M}) \cap \mathcal{L}(\mathbf{L})$, although polynomial, is not very efficient. In particular, the number of bits necessary to store a single group elements can be much larger than $\log_2 \#G$. Other more efficient ways to represent group elements are possible, for example using the Hermite Normal Form, or Smith Normal Form. These representations allow to store group elements using only $\log |G|$ bits, and perform the group operations in linear time. The techniques described in this paper are largely independent from the way group elements are represented, so we do not elaborate on this any further, and refer the reader to [28, 31] for more details.

Later in this paper we need to sample elements from group $G = \mathcal{L}(\mathbf{L})/\mathcal{L}(\mathbf{M})$ uniformly at random. This can be easily done using an elementary group theoretic technique described in the following proposition.

**Proposition 3** *Let $G$ be a finite Abelian group and $g_1, \ldots, g_n$ a generating set for $G$. Then, if $d_1, \ldots, d_n$ are chosen uniformly at random in $\{1, \ldots, \#G\}$, the group element*

$$g = \sum_{i=1}^{n} d_i g_i$$

*is distributed uniformly at random over $G$.*

**Proof:** It easily follows by decomposing $G$ into the product of cyclic groups. □

Of particular interest in this paper are quotient groups $G = \mathcal{L}(\mathbf{L})/\mathcal{L}(\mathbf{M})$ where $\mathbf{M}$ defines an almost *orthogonal* sublattice of $\mathcal{L}(\mathbf{L})$. The following lemma gives a possible way to build almost orthogonal sublattices for any input lattice $\mathcal{L}(\mathbf{L})$.

**Lemma 1** *Let $\Lambda$ be a full rank $n$-dimensional lattice, $\sigma$ a positive real, and $D$ be a decoding procedure that on input a vector $\mathbf{x} \in \mathbb{R}^n$ returns a lattice point $D(\mathbf{x}) \in \Lambda$ such that $\mathrm{dist}(D(\mathbf{x}), \mathbf{x}) \leq \sigma$. For any $\alpha \geq 2\sqrt{n} \cdot \sigma$, one can efficiently find (with $n$ calls to $D$) a basis of a full rank sublattice $\mathbf{S} \subset \Lambda$ such that for all $\mathbf{x} \in \mathbb{R}^n$*

$$\|\mathbf{Sx}\| \approx \alpha \cdot \|\mathbf{x}\|.$$

**Proof:** Let $\mathbf{s}_i = D(\alpha \cdot \mathbf{e}_i)$, where $\mathbf{e}_1, \ldots, \mathbf{e}_n$ are the standard unit vectors in $\mathbb{R}^n$. Clearly $\mathbf{s}_i \in \Lambda$ for all $i = 1, \ldots, n$. Let $\mathbf{x} \in \mathbb{R}^n$ be an arbitrary vector. We want to prove that $\|\mathbf{Sx}\| \approx \alpha \cdot \|\mathbf{x}\|$. We know that $\mathbf{s}_i = \alpha \cdot \mathbf{e}_i + \mathbf{r}_i$ where $\|\mathbf{r}_i\| = \|D(\alpha \cdot \mathbf{e}_i) - \alpha \cdot \mathbf{e}_i\| \leq \sigma$. Therefore,

$$\|\mathbf{Sx}\| = \|(\alpha \cdot \mathbf{I} + \mathbf{R})\mathbf{x}\| = \|\alpha \cdot \mathbf{x} + \mathbf{Rx}\|.$$

By triangle inequality,

$$\alpha \cdot \|\mathbf{x}\| - \|\mathbf{Rx}\| \leq \|\mathbf{Sx}\| \leq \alpha \cdot \|\mathbf{x}\| + \|\mathbf{Rx}\|.$$

So, we need to prove that $\|\mathbf{Rx}\| \leq \frac{\alpha}{2}\|\mathbf{x}\|$. By triangle inequality and Cauchy-Swartz,

$$\|\mathbf{Rx}\| \leq \sum_{i=1}^{n} \|\mathbf{r}_i\| \cdot |x_i| \leq \sigma \cdot \sum_{i=1}^{n} |x_i| \leq \sqrt{n}\sigma \cdot \|\mathbf{x}\| \leq \frac{\alpha}{2} \cdot \|\mathbf{x}\|.$$

This proves that $\|\mathbf{Sx}\| \approx \alpha \cdot \|\mathbf{x}\|$. The linear independence of vectors $\mathbf{S}$ immediately follows because if $\mathbf{S}$ were linearly dependent, then one could find a nonzero vector $\mathbf{x}$ such that $\mathbf{Sx} = \mathbf{0}$, contradicting $\|\mathbf{Sx}\| \approx \alpha \cdot \|\mathbf{x}\| > 0$. □

So far, we have shown how to use lattices and sublattices to define finite Abelian groups. It is also possible to use finite Abelian groups to define lattices.

**Proposition 4** *Let $G$ be a finite Abelian group, and $g_1, \ldots, g_n$ a sequence of elements of $G$. Then, the set*

$$\Lambda(g_1, \ldots, g_n) = \{\mathbf{x} \in \mathbb{Z}^n : \sum_{i=1}^{n} x_i g_i = 0\}$$

*is a lattice, and its determinant satisfies*

$$\det(\Lambda(g_1, \ldots, g_n)) \leq \#G.$$

**Proof:** The fact $\Lambda(g_1, \ldots, g_n)$ is a lattice is elementary. The bound on the determinant can be easily proved using the decomposition of $G$ into the product of cyclic groups. □

## 2.4 Statistical distance

The statistical distance is a measure of how two probability distributions are far apart from each other, and it is a convenient tool in the analysis of randomized algorithms and reductions. In this subsection we define the statistical distance and prove some simple facts that will be used in the analysis of the algorithms in this paper. All the properties of the statistical distance stated in this subsection are easily verified. For more details the reader is referred to [31].

**Definition 7** *Let $X$ and $Y$ be two discrete random variables over a (countable) set $A$. The statistical distance between $X$ and $Y$ is the quantity*

$$\Delta(X, Y) = \frac{1}{2} \sum_{a \in A} |\Pr\{X = a\} - \Pr\{Y = a\}|.$$

We say that two random variables $X, Y$ are identically distributed (written $X \equiv Y$) if and only if $\Pr\{X = a\} = \Pr\{Y = a\}$ for every $a \in A$. The reader can easily check that the statistical distance satisfies the usual properties of distance functions, i.e., $\Delta(X, Y) \geq 0$ (with equality if and only if $X \equiv Y$), $\Delta(X, Y) = \Delta(Y, X)$, and $\Delta(X, Z) \leq \Delta(X, Y) + \Delta(Y, Z)$.

The following property of the statistical distance is useful when analyzing a probabilistic algorithm that is part of a larger randomized process.

**Proposition 5** *Let $X, Y$ be random variables over a set $A$, and let $Z$ be a third random variable over a (possibly different) set $B$. If $Z$ is statistically independent from $X$ and $Y$. Then*

$$\Delta((X, Z), (Y, Z)) = \Delta(X, Y).$$

Using Proposition 5 and the triangle inequality we get the following useful bound.

**Proposition 6** *Let $X_1, \ldots, X_k$ and $Y_1, \ldots, Y_k$ be two lists of totally independent random variables. Then*

$$\Delta((X_1, \ldots, X_k), (Y_1, \ldots, Y_k)) \leq \sum_{i=1}^{k} \Delta(X_i, Y_i). \tag{5}$$

The following proposition shows that applying a (possibly randomized) function to two distributions does not increase the statistical distance.

**Proposition 7** *Let $X, Y$ be two random variables over a common set $A$. For any (possibly randomized) function $f$ with domain $A$, the statistical distance between $f(X)$ and $f(Y)$ is at most*

$$\Delta(f(X), f(Y)) \leq \Delta(X, Y) \tag{6}$$

The next proposition and corollary show how to use the statistical distance to estimate expectations and probabilities.

**Proposition 8** *If $X$ and $Y$ are random variables over set $A$ and $f: A \to [a,b]$ is a real valued function, then*

$$|\,Exp[f(X)] - Exp[f(Y)]| \leq |b-a| \cdot \Delta(X,Y) \tag{7}$$

As a corollary, we immediately obtain the following.

**Corollary 1** *If $X$ and $Y$ are random variables over set $A$ and $p: A \to \{0,1\}$ is a predicate, then*

$$|\Pr[p(X)=1] - \Pr[p(Y)=1]| \leq \Delta(X,Y). \tag{8}$$

The last proposition gives a standard amplification technique that allows to generate almost uniform samples from a group by adding a relatively small number of independent samples that are not too far from uniform.

**Proposition 9** *Let $(G,+)$ be a finite group and let $A_1, \ldots, A_k$ be $k$ independent (but possibly not identically distributed) random variables over $G$ such that*[8] $\Pr\{A_i = g\} \approx 1/\#G$ *for all $i = 1, \ldots, k$ and any $g \in G$. Then, the statistical distance between the sum $A = \sum_{i=1}^{k} A_i$ and the uniform distribution $U$ over $G$ is at most*

$$\Delta\left(\sum_{i=1}^{k} A_i, U\right) \leq \frac{1}{2^{k+1}}.$$

# 3 Covering radius and uniform radius

Let $\mathcal{L}(\mathbf{B})$ be an $n$-dimensional lattice and let $\mathcal{Q}$ be a convex body in $\mathbb{R}^n$. It can be shown that if we consider a randomly shifted copy of the body $\mathcal{Q} + \mathbf{x}$ (where $\mathbf{x}$ is chosen uniformly at random)[9], then the expected number of lattice points equals exactly

$$\operatorname*{Exp}_{\mathbf{x}}[\#(\mathcal{L}(\mathbf{B}) \cap (\mathcal{Q} + \mathbf{x}))] = \frac{\mathrm{vol}(\mathcal{Q})}{|\det(\mathbf{B})|}.$$

In particular, if $\mathcal{Q}$ is a sphere of radius $r$, then

$$\operatorname*{Exp}_{\mathbf{x}}[\#(\mathcal{L}(\mathbf{B}) \cap \mathcal{B}(\mathbf{x}, r))] = \frac{\mathrm{vol}(\mathcal{B}(r))}{|\det(\mathbf{B})|}.$$

This corresponds to the intuition that the determinant $|\det(\mathbf{B})|$ is the inverse of the density of lattice points in space. Notice that the actual number of lattice points in a specific $\mathcal{Q}$ may deviate arbitrarily from the expectation, even for the special case of spherical $\mathcal{Q}$. Consider for example a lattice generated by two orthogonal vectors $\mathbf{e}_1$ and $D\mathbf{e}_2$, where $D$ is a large constant. Notice that the determinant of the lattice is $D$, so on the average we would expect to find $\mathrm{vol}(\mathcal{Q})/D$ lattice points inside $\mathcal{Q}$. Now, let $\mathcal{Q} = \mathcal{B}(\mathbf{x}, \sqrt{D})$ be the open disc of radius $\sqrt{D}$. The area of $\mathcal{Q}$ is $\mathrm{vol}(\mathcal{Q}) = \pi D$, so on the average we would expect to find $\pi$ lattice points in $\mathcal{Q}$. However, if $\mathbf{x} = 0$, the number of lattice points in $\mathcal{Q}$ is $2\lceil\sqrt{D}\rceil - 3$. Even worse, if $\mathbf{x} = (D/2)\mathbf{e}_2$, then $\mathcal{Q}$ does not contain any lattice point at all.

We define the *uniform radius* of a lattice as the smallest value $r = \zeta(\mathbf{B})$ such that any sphere $\mathcal{B}(\mathbf{x}, r)$ contains a number of lattice points close to the expected value.

**Definition 8** *For any $n$-dimensional lattice $\mathcal{L}(\mathbf{B})$, the* uniform radius $\zeta(\mathbf{B})$ *is the smallest positive real $r$ such that*

$$\#(\mathcal{L}(\mathbf{B}) \cap \mathcal{B}(\mathbf{x}, r)) \approx \frac{\mathrm{vol}(\mathcal{B}(r))}{|\det(\mathbf{B})|}$$

*for any $\mathbf{x} \in span(\mathbf{B})$.*

[8] Remember that $a \approx b$ means that the relative error $|a-b|/|b|$ is at most $1/2$.

[9] Intuitively, we would like to choose $\mathbf{x}$ uniformly at random from $\mathbb{R}^n$, but this is not possible because $\mathbb{R}^n$ has infinite measure. This problems is easily solved observing that it is enough to choose $\mathbf{x}$ uniformly at random from the fundamental region $\mathcal{P}(\mathbf{B})$ of the lattice, because the lattice repeats identically when translated by $\mathbf{Bx}$ for $\mathbf{x} \in \mathbb{Z}^n$.

The following proposition shows that the uniform radius $\zeta(\mathbf{B})$ is at least as large as the covering radius $\rho(\mathbf{B})$. Later we will also show that the uniform radius is never much bigger than that.

**Proposition 10** *For any lattice* $\mathbf{B}$, $\rho(\mathbf{B}) \leq \zeta(\mathbf{B})$.

**Proof:** The proof is immediate because for $r < \rho(\mathbf{B})$ any sphere of radius $r$ centered in a deep hole (i.e., a point in space at distance $\rho(\mathbf{B})$ from the lattice) does not contain any lattice point. □

The uniform radius can be used to estimate the number of lattice points contained in a sphere. Later in this paper, we need to estimate the number of lattice points inside arbitrary convex bodies. So, we generalize the definition of the uniform radius to arbitrary convex bodies.

**Definition 9** *For any n-dimensional lattice* $\mathcal{L}(\mathbf{B})$, *the* generalized uniform radius $\hat{\zeta}(\mathbf{B})$ *is the smallest positive real* $r$ *such that for any convex body* $\mathcal{Q}$ *containing a sphere* $\mathcal{B}(\mathbf{x}, r) \subseteq \mathcal{Q}$ *of radius* $r$, *the number of lattice points inside the body satisfies*

$$\#(\mathcal{L}(\mathbf{B}) \cap \mathcal{Q}) \approx \frac{\mathrm{vol}(\mathcal{Q})}{|\det(\mathbf{B})|}.$$

Clearly, the generalized uniform radius is at least as large at the uniform radius: for any lattice $\mathbf{B}$, $\zeta(\mathbf{B}) \leq \hat{\zeta}(\mathbf{B})$. In particular, $\hat{\zeta}(\mathbf{B})$ is always at least as large as the covering radius $\rho(\mathbf{B})$. We bound the (generalized) uniform radius from above, and show that for any lattice $\mathbf{B}$, the (generalized) uniform radius is not much larger than then covering radius. Specifically, we show that $\hat{\zeta}(\mathbf{B}) = O(n \cdot \rho(\mathbf{B}))$. A similar result was proved by Dyer, Frieze and Kannan in [11], for the special case of $\mathcal{L}(\mathbf{B}) = \mathbb{Z}^n$. We observe that the proof of [11] is a general volume argument and it does not use any special property of lattice $\mathbb{Z}^n$. So, it can be easily adapted to arbitrary lattices. Below we recall two simple geometric lemmas proved in [11], and then use them to prove the bound on $\hat{\zeta}(\mathbf{B})$.

**Lemma 2 ([11, Proposition 1])** *Suppose* $\mathcal{Q}$ *is a convex body in* $\mathbb{R}^n$ *containing the unit ball* $\mathcal{B}(1)$, *and let* $\epsilon > 0$ *be any positive real. Then all points within distance* $\epsilon$ *from* $\mathcal{Q}$ *belong to* $(1+\epsilon)\mathcal{Q}$.

**Lemma 3 ([11, Proposition 2])** *Suppose* $\mathcal{Q}$ *is a convex body in* $\mathbb{R}^n$ *containing the unit ball* $\mathcal{B}(1)$, *and let* $0 < \epsilon \leq 1$. *Then, all points within distance* $\epsilon$ *from* $(1-\epsilon)\mathcal{Q}$ *belong to* $\mathcal{Q}$.

We can now prove the bound on the uniform radius in terms of the covering radius.

**Theorem 1** *For any n-dimensional lattice* $\mathbf{B}$,

$$\hat{\zeta}(\mathbf{B}) \leq 3n\rho(\mathbf{B}).$$

**Proof:** Let $\mathbf{B}$ be a full rank lattice in $\mathbb{R}^n$ with covering radius $\rho(\mathbf{B})$, and let $\mathcal{Q}$ be a convex body containing a sphere of radius $r = 3n\rho(\mathbf{B})$. We want to prove that $\#(\mathcal{L}(\mathbf{B}) \cap \mathcal{Q}) \approx \frac{\mathrm{vol}(\mathcal{Q})}{\det(\mathbf{B})}$. Define $\mathbf{B}' = \mathbf{B}/r$ and $\mathcal{Q}' = \mathcal{Q}/r$, and let

$$S = \mathcal{L}(\mathbf{B}') \cap \mathcal{Q}' = \frac{\mathcal{L}(\mathbf{B}) \cap \mathcal{Q}}{r}.$$

Clearly, $\#S = \#(\mathcal{L}(\mathbf{B}') \cap \mathcal{Q}') = \#(\mathcal{L}(\mathbf{B}) \cap \mathcal{Q})$. We want to prove that

$$\#S \approx \frac{\mathrm{vol}(\mathcal{Q}')}{|\det(\mathbf{B}')|} = \frac{\mathrm{vol}(\mathcal{Q})}{|\det(\mathbf{B})|}.$$

Consider the union of all open Voronoi cells $\mathcal{V}(\mathbf{x}, \mathbf{B}')$ with centers $\mathbf{x} \in S$. Notice that all points $\mathbf{y} \in \mathcal{V}(\mathbf{x}, \mathbf{B}')$ are within distance $\rho(\mathbf{B}') = \rho(\mathbf{B})/r$ from $\mathbf{x}$. Moreover $\mathcal{Q}'$ contains a sphere of radius 1. Therefore, by Lemma 2, for all $\mathbf{x} \in S \subset \mathcal{Q}'$ and $\mathbf{y} \in \mathcal{V}(\mathbf{x}, \mathbf{B}')$, we have $\mathbf{y} \in \mathcal{Q}' \cdot (1 + \rho(\mathbf{B})/r)$, i.e., $\mathcal{V}(\mathbf{x}, \mathbf{B}') \subseteq (1 + \rho(\mathbf{B})/r) \cdot \mathcal{Q}'$.

(Scaling performed using as origin the center of the unit sphere contained in $\mathcal{Q}'$.) Since all $\mathcal{V}(\mathbf{x}, \mathbf{B}')$ are disjoint, and have the same volume, we have

$$\begin{aligned} \#S &= \frac{\sum_{\mathbf{x}\in S} \mathrm{vol}\left(\mathcal{V}(\mathbf{x}, \mathbf{B}')\right)}{\mathrm{vol}(\mathcal{V}(\mathbf{B}'))} \\ &= \frac{\mathrm{vol}\left(\bigcup_{\mathbf{x}\in S} \mathcal{V}(\mathbf{x}, \mathbf{B}')\right)}{\mathrm{vol}(\mathcal{V}(\mathbf{B}'))} \\ &\leq \frac{\mathrm{vol}(\mathcal{Q}' \cdot (1 + \rho(\mathbf{B})/r))}{|\det(\mathbf{B}')|} \\ &= \left(1 + \frac{\rho(\mathbf{B})}{r}\right)^n \frac{\mathrm{vol}(\mathcal{Q})}{|\det \mathbf{B}|}. \end{aligned}$$

Finally, using the assumption $r \geq 3n\rho(\mathbf{B})$, we get

$$\begin{aligned} \left(1 + \frac{\rho(\mathbf{B})}{r}\right)^n &< \left(1 + \frac{1}{3n-1}\right)^n \\ &= \frac{1}{\left(1 - \frac{1}{3n}\right)^n} \\ &\leq \frac{1}{1 - \frac{1}{3}} = \frac{3}{2}. \end{aligned}$$

This proves the upper bound $\#S \lesssim \mathrm{vol}(\mathcal{Q})/|\det \mathbf{B}|$.

We now turn to the lower bound. Let $S'$ be the set of all lattice points $\mathbf{x} \in \mathbf{B}'$ such that the closed Voronoi cell $\bar{\mathcal{V}}(\mathbf{x}, \mathbf{B}')$ intersects $(1 - \rho(\mathbf{B})/r)\mathcal{Q}'$. Notice that if $\bar{\mathcal{V}}(\mathbf{x}, \mathbf{B}')$ intersects $(1 - \rho(\mathbf{B})/r)\mathcal{Q}'$, then $\mathbf{x}$ must be within distance $\rho(\mathbf{B}') = \rho(\mathbf{B})/r$ from $(1 - \rho(\mathbf{B})/r) \cdot \mathcal{Q}'$. So, by Lemma 3, $\mathbf{x} \in \mathcal{Q}'$. This proves that $S' \subseteq S$, and $\#S \geq \#S'$. Since Voronoi cells cover $\mathbb{R}^n$, $(1 - \rho(\mathbf{B})/r)\mathcal{Q}'$ is fully contained in the union $\bigcup_{\mathbf{x}\in S'} \bar{\mathcal{V}}(\mathbf{x}, \mathbf{B}')$, and

$$\begin{aligned} \#S' &= \frac{\sum_{\mathbf{x}\in S'} \mathrm{vol}(\bar{\mathcal{V}}(\mathbf{x}, \mathbf{B}'))}{\mathrm{vol}(\mathcal{V}(\mathbf{B}'))} \\ &\geq \frac{\mathrm{vol}(\bigcup_{\mathbf{x}\in S'} \bar{\mathcal{V}}(\mathbf{x}, \mathbf{B}'))}{\mathrm{vol}(\mathcal{V}(\mathbf{B}'))} \\ &\geq \frac{\mathrm{vol}((1 - \rho(\mathbf{B})/r)\mathcal{Q}')}{|\det(\mathbf{B}')|} \\ &= \left(1 - \frac{\rho(\mathbf{B})}{r}\right)^n \frac{\mathrm{vol}(\mathcal{Q})}{|\det(\mathbf{B})|}. \end{aligned}$$

Using the assumption $r \geq 3n\rho(\mathbf{B})$, we immediately get

$$\left(1 - \frac{\rho(\mathbf{B})}{r}\right)^n > \left(1 - \frac{1}{2n}\right)^n \geq 1 - \frac{1}{2}.$$

This proves the lower bound $\#S \gtrsim \mathrm{vol}(\mathcal{Q})/|\det(\mathbf{B})|$, and completes the proof of the theorem. □

Using inequality $\rho(\mathbf{B}) \leq \sqrt{n} \cdot \lambda_n(\mathbf{B})/2$ from (2) we can bound $\hat{\zeta}(\mathbf{B})$ in terms of $\lambda_n(\mathbf{B})$:

$$\hat{\zeta}(\mathbf{B}) \leq \frac{3}{2} n^{1.5} \lambda_n(\mathbf{B}). \tag{9}$$

Similarly, using transference theorem (3), we can bound $\hat{\zeta}(\mathbf{B})$ in terms of the length of the shortest nonzero vector in the dual lattice:

$$\hat{\zeta}(\mathbf{B}) \leq \frac{3}{2} n^2 / \lambda_1(\mathbf{B}^*). \tag{10}$$

These bounds can be used to relate the average-case complexity of finding short vectors in random lattices to the to the worst-case complexity of approximating SIVP or the length estimation version of SVP.

It would be interesting to improve bounds (9) and (10). In particular, is it true that $\hat{\zeta}(\mathbf{B}) = O(n \cdot \lambda_n(\mathbf{B}))$ for any $n$-dimensional lattice $\mathbf{B}$? Is it true that $\hat{\zeta}(\mathbf{B}) = O(n/\lambda_1(\mathbf{B}^*))$? Proving these improved bounds would immediately result in a reduction of the connection factor for SIVP by a factor $O(\sqrt{n})$, and for SVP by a factor $O(n)$.

# 4 Easily decodable almost perfect lattices

We are interested in lattices that have both good algorithmic and geometric properties. Algorithmically, we would like lattices where the closest vector problem can be efficiently solved. Notice that, despite the NP-hardness of CVP, the closest vector problem may be efficiently solvable for *specific* lattices. For example, in the integer lattice $\mathbb{Z}^n$, a lattice vector $\mathbf{x} \in \mathbb{Z}^n$ closest to a given target $\mathbf{t} \in \mathbb{Q}^n$ can be easily found rounding each coordinate of $\mathbf{t}$ to the closest integer $x_i = \lceil t_i \rfloor$. Since for any fixed dimension the closest vector problem can be solved in polynomial time, in order to properly formulate this problem one needs to consider not a single lattice, but an infinite sequence of lattices in increasing dimension. For simplicity, in the definition below we focus on full dimensional lattices, although this restriction is not necessary.

**Definition 10** *Let $\{\mathbf{L}_n\}_{n\geq 1}$ be a sequence of full rank lattices $\mathcal{L}(\mathbf{L}_n) \subseteq \mathbb{R}^n$. We say that the sequence $\{\mathbf{L}_n\}_{n\geq 1}$ is* easily decodable *if there exists a polynomial time algorithm $\mathrm{CVP}_{\mathbf{L}}$ such that for any $n \geq 1$ and $\mathbf{t} \in \mathbb{Q}^n$, $\mathrm{CVP}_{\mathbf{L}}(\mathbf{t})$ outputs a lattice vector in $\mathcal{L}(\mathbf{L}_n)$ closest to $\mathbf{t}$.*

The simplest example of easily decodable sequence of lattices is given by the integer lattices $\mathbb{Z}^n$ defined by matrices $\mathbf{L}_n = \mathbf{I}_n$. Other easily decodable lattices considered in [9] are the *root lattices* $A_n, D_n$, and their duals $D_n^*$ and $A_n^*$.[10]

From a geometric point of view, we would like the Voronoi cells of the lattice to be as spherical as possible. Remember that the Voronoi cell $\mathcal{V}(\mathbf{L}_n)$ contains a sphere $\mathcal{B}(\lambda_1/2)$ with radius equal to the packing radius, and is completely contained in a sphere $\mathcal{B}(\rho(\mathbf{L}_n))$ with radius equal to the covering radius. So, the closer the covering radius is to the packing radius, the better Voronoi cells are approximated by spheres. This motivate the following definition.

**Definition 11** *For any $\tau \geq 1$, a lattice $\mathcal{L}(\mathbf{L})$ is $\tau$-perfect if*

$$\rho(\mathbf{L}) \leq \tau \cdot \left(\frac{\lambda_1(\mathbf{L})}{2}\right).$$

*For any function $\tau(n)$, a sequence of (full rank) lattices $\{\mathbf{L}_n\}_{n\geq 1}$ (where $n$ is the dimension of $\mathcal{L}(\mathbf{L}_n)$) is $\tau(n)$-perfect if $\mathcal{L}(\mathbf{L}_n)$ is $\tau(n)$-perfect for any $n \geq 1$.*

We are interested in sequences of lattices such that $\tau(n)$ is as small as possible. Moreover, we would like the lattices to be easily decodable. The integer lattice $\mathbb{Z}^n$, as well as all other sequences $A_n, A_n^*, D_n, D_n^*$ of easily decodable lattices considered in [9], are $\tau(n)$-perfect for $\tau(n) = \Theta(\sqrt{n})$. So, it is natural to ask if non trivial easily decodable almost perfect lattices (i.e., $\tau(n)$-perfect lattices with $\tau(n) = o(\sqrt{n})$) exist, or the $o(\sqrt{n})$-perfectness and easy decodability requirements are incompatible.

In this section we start the algorithmic study of almost perfect lattices and give the first efficient construction of non-trivial easily decodable almost perfect lattices. Our lattices are $\tau(n)$-perfect for $\tau(n) = \sqrt{n \log\log n / \log n} = o(\sqrt{n})$. Although this is not a substantial improvement over $\tau(n) = \Theta(\sqrt{n})$ from a quantitative point of view, it is qualitatively interesting because it shows that non-trivial easily decodable almost perfect lattices exist.

We first present a construction of 3-perfect lattices such that the construction and the decoding algorithm run in exponential time $n^{O(n)}$. Then we show how to use small dimensional lattices obtained using this construction to efficiently construct $O(\sqrt{n \log\log n / \log n})$-perfect lattices such that the closest vector problem can be solved in polynomial time. The construction is based on the following simple lemma.

[10] Conway and Sloane [9] also describe other efficient decoding algorithms for specific lattices, but $\mathbb{Z}^n, A_n, A_n^*, D_n, D_n^*$ are the only infinite sequences of lattices considered for which the problem of efficient decoding admits an interesting asymptotic formulation.

**Lemma 4** *For any lattice* $\mathbf{B}$*, there exist a lattice vector* $\mathbf{v} \in \mathcal{L}(\mathbf{B})$ *such that* $\mathrm{dist}(\mathbf{v}/3, \mathcal{L}(\mathbf{B})) \geq (2/3)\rho(\mathbf{B})$*. In particular, if* $\rho(\mathbf{B}) \geq 3 \cdot \lambda_1(\mathbf{B})/2$ *then* $\mathrm{dist}(\mathbf{v}/3, \mathcal{L}(\mathbf{B})) \geq \lambda_1(\mathbf{B})$*.*

**Proof:** Let $\mathbf{h}$ be a deep hole, i.e., a point in $\mathrm{span}(\mathbf{B})$ at distance $\rho(\mathbf{B})$ from $\mathcal{L}(\mathbf{B})$. Consider the point $3\mathbf{h}$, and let $\mathbf{v} \in \mathcal{L}(\mathbf{B})$ be a lattice point closest to $3\mathbf{h}$. By definition of covering radius, it must be $\|\mathbf{v} - 3\mathbf{h}\| \leq \rho(\mathbf{B})$. Therefore, dividing by 3 we get $\|\mathbf{v}/3 - \mathbf{h}\| \leq \rho(\mathbf{B})/3$, and by triangle inequality

$$\mathrm{dist}(\mathbf{v}/3, \mathcal{L}(\mathbf{B})) \geq \mathrm{dist}(\mathbf{h}, \mathcal{L}(\mathbf{B})) - \mathrm{dist}(\mathbf{v}/3, \mathbf{h}) \geq \rho(\mathbf{B}) - \frac{1}{3}\rho(\mathbf{B}) = \frac{2}{3} \cdot \rho(\mathbf{B}).$$

□

We use the lemma to give an algorithmic construction of $\tau$-perfect lattices with $\tau < 3$. The following theorem is essentially an algorithmic variant of the proof of existence given in [35]. Both the procedure to build the lattice and to decode it run in time $n^{O(n)}$. It should be noted that for any $n$-dimensional lattice, in principle the closest vector problem can always be solved in time $n^{O(n)}$ [19]. However, the algorithm of [19] for general lattices is rather complicated. In the theorem below we show how to build a lattice $\mathbf{B}$ together with some (polynomial size) side information $\mathbf{V}$ that allows to solve the closest vector problem in lattice $\mathcal{L}(\mathbf{B})$, still in time $n^{O(n)}$ as in [19], but with a much simpler algorithm.

**Theorem 2** *There is an algorithm running in time* $n^{O(n)}$ *that on input* $n$ *outputs an* $n$*-dimensional* 3*-perfect lattice* $\mathbf{L}_n$*. Moreover, the sequence of lattices* $\{\mathbf{L}_n\}_{n \geq 1}$ *is decodable in time* $n^{O(n)}$*, i.e., there is an algorithm* $\mathrm{CVP}_{\mathbf{L}}$ *running in time* $n^{O(1)+n/2}$ *that on input a vector* $\mathbf{t} \in \mathbb{Q}^n$ *outputs a lattice vector* $\mathrm{CVP}_{\mathbf{L}}(\mathbf{t}) \in \mathcal{L}(\mathbf{L}_n)$ *closest to* $\mathbf{t}$*.*

**Proof:** The algorithm starts from an arbitrary $n$-dimensional easily decodable lattice $\mathcal{L}(\mathbf{B}_0)$, e.g., the integer lattice $\mathcal{L}(\mathbf{B}_0) = \mathbb{Z}^n$ generated by the identity matrix $\mathbf{B}_0 = \mathbf{I}$. Notice that the closest vector in $\mathbb{Z}^n$ to a target $\mathbf{t}$ can be easily found by rounding each coordinate of $\mathbf{t}$ to the closest integer. Below we assume that $\mathbf{B}_0 = \mathbf{I}$ and, in particular, $\det(\mathbf{B}_0) = 1$ and $\lambda_1(\mathbf{B}_0) = 1$, but the construction works for any easily decodable lattice.

Starting from $\mathbf{B}_0$, we iteratively build a sequence of lattice bases $\mathbf{B}_i$ and auxiliary vectors $\mathbf{v}_i$ for $i = 1, \ldots, m$ for some $m = O(n \log n)$ to be determined. The final output are basis $\mathbf{B} = \mathbf{B}_m$ and set of vectors $\mathbf{V} = [\mathbf{v}_1, \ldots, \mathbf{v}_m]$. For each $k = 1, \ldots, m$, vector $\mathbf{v}_k$ and basis $\mathbf{B}_k$ are computed as follows:

1. For any vector $\mathbf{s} \in \{-1, 0, +1\}^n$, let $\mathbf{t} = (1/3)\mathbf{B}_{k-1}\mathbf{s}$ and compute the distance of $\mathbf{t}$ from the lattice $\mathcal{L}(\mathbf{B}_{k-1})$. (We will show below how this can be done in time $n^{O(1)} \cdot 3^k$.)
2. If for all $\mathbf{s} \in \{-1, 0, +1\}^n$, $\mathrm{dist}(\mathbf{t}, \mathcal{L}(\mathbf{B}_{k-1}) < 1$, then set $m = k - 1$, and terminate with output $B = \mathbf{B}_{k-1}$ and $\mathbf{V} = [\mathbf{v}_1, \ldots, \mathbf{v}_{k-1}]$.
3. Otherwise (if $\mathrm{dist}(\mathbf{t}, \mathcal{L}(\mathbf{B}_{k-1}) \geq 1$ for some $\mathbf{s}$) proceeds as follows. Notice that since $\mathrm{dist}(\mathbf{t}, \mathcal{L}(\mathbf{B}_{k-1})) > 0$, it must be $\mathbf{s} \neq \mathbf{0}$.
4. Let $i \in \{1, \ldots, n\}$ such that $s_i \neq 0$.
5. Set $\mathbf{v}_k = \mathbf{t}$.
6. Set $\mathbf{B}_k$ to the matrix obtained by replacing the $i$th vector in $\mathbf{B}_{k-1}$ with $\mathbf{v}_k$.

The algorithm uses a procedure to find closest vectors in lattice $\mathcal{L}(\mathbf{B}_k)$. We will show that the maximum number of iterations performed by the algorithm is $m \leq (n/2)\log_3 n = O(n \log n)$, and that for any $k$, the closest vector problem in $\mathcal{L}(\mathbf{B}_k)$ can be solved in time $n^{O(1)} \cdot 3^k$. It follows that the total running time of the algorithm is

$$O(m \cdot n^{O(1)} \cdot 3^m) = n^{O(n)}$$

and that the closest vector problem in $\mathcal{L}(\mathbf{B})$ can also be solved in time $n^{O(1)+n/2}$.

The correctness of the algorithm is based on the fact that for any $k$,

- Vector $3\mathbf{v}_k$ belongs to the lattice $\mathcal{L}(\mathbf{B}_{k-1})$.

- $\mathbf{B}_k$ is a basis for the lattice generated by $[\mathbf{B}_{k-1}|\mathbf{v}_k]$.
- The shortest vector in $\mathcal{L}(\mathbf{B}_k)$ has length 1.

The first property immediately follows by construction. For the second property, it is clear that $\mathcal{L}(\mathbf{B}_k)$ is a subset of $\mathcal{L}([\mathbf{B}_{k-1}|\mathbf{v}_k])$. In order to prove $\mathcal{L}(\mathbf{B}_k) = \mathcal{L}([\mathbf{B}_{k-1}|\mathbf{v}_k])$ we only need to show that the $i$th vector of $\mathbf{B}_{k-1}$ (namely, $\mathbf{B}_{k-1}\mathbf{e}_i$) belongs to $\mathcal{L}(\mathbf{B}_k)$. Notice that $s_i \cdot \mathbf{B}_{k-1}\mathbf{e}_i = 3\mathbf{v}_k - \sum_{j\neq i} s_j \mathbf{B}_{k-1}\mathbf{e}_j = 3\mathbf{B}_k\mathbf{e}_i - \sum_{j\neq i} s_j \mathbf{B}_k\mathbf{e}_j$ belongs to $\mathcal{L}(\mathbf{B}_k)$. Since $s_i = \pm 1$, also $\mathbf{B}_{k-1}\mathbf{e}_i = \pm(s_i \cdot \mathbf{B}_{k-1}\mathbf{e}_i)$ belongs to $\mathcal{L}(\mathbf{B}_k)$. Now, let's get to the third property. Consider any nonzero vector in $\mathcal{L}(\mathbf{B}_k)$. Since $\mathcal{L}(\mathbf{B}_k) = \mathcal{L}([\mathbf{B}_{k-1}|\mathbf{v}_k])$, any such a vector can be written as $\mathbf{B}_{k-1}\mathbf{x} + \mathbf{v}_k \cdot y$. Moreover, since $3\mathbf{v}_k \in \mathcal{L}(\mathbf{B}_{k-1})$, we can assume without loss of generality that $y \in \{-1, 0, +1\}$. So, the length of $\mathbf{B}_{k-1}\mathbf{x} + \mathbf{v}_k \cdot y$ is at least the minimum of $\lambda_1(\mathbf{B}_{k-1})$ (if $y = 0$) or $\mathrm{dist}(\pm\mathbf{v}_k, \mathcal{L}(\mathbf{B}_{k-1}))$ (if $y = \pm 1$). But $\lambda_1(\mathbf{B}_{k-1}) \geq 1$ by induction, and $\mathrm{dist}(\pm\mathbf{v}_k, \mathcal{L}(\mathbf{B}_{k-1})) = \mathrm{dist}(\mathbf{v}_k, \mathcal{L}(\mathbf{B}_{k-1})) \geq 1$ by construction. It follows that $\lambda_1(\mathbf{B}_k) \geq 1$.

It is also easy to see that for any $k$, the determinant of lattice $\mathcal{L}(\mathbf{B}_k)$ equals $|\det(\mathbf{B}_k)| = 3^{-k}\det(\mathbf{B}_0) = 3^{-k}$ because each $\mathbf{B}_k$ can be obtained from $\mathbf{B}_{k-1}$ by first performing some elementary integer column operations, and then dividing a column by 3. We can now prove that the algorithm performs at most $m = O(n \log n)$ iterations. Since $\lambda_1(\mathbf{B}_k) = 1$ and $|\det(\mathbf{B}_k)| = 3^{-k}$, by Minkowski's theorem,

$$1 = \lambda_1(\mathbf{B}_k) \leq \sqrt{n}|\det(\mathbf{B}_k)|^{1/n} = \sqrt{n}3^{-(k/n)}.$$

It follows that

$$k \leq (1/2)n \log_3 n = O(n \log n)$$

is an upper bound on the maximum number of iterations. (It can also be shown by a volume argument that $m = \Theta(n \log n)$ iterations are required in order to reach termination.)

Next we prove that upon termination $\rho(\mathbf{L}_n) < 3 \cdot \lambda_1(\mathbf{L}_n)/2$. We show that if $\rho(\mathbf{L}_n) \geq (3/2) \cdot \lambda_1(\mathbf{L}_n)$, then the algorithm certainly performs one more iteration. By lemma 4, if $\rho(\mathbf{L}_n) \geq (3/2)\lambda_1(\mathbf{L}_n)$ then there exists a vector $\mathbf{v} = \mathbf{B}_{k-1}\mathbf{x} \in \mathcal{L}(\mathbf{B}_{k-1})$ such that

$$\mathrm{dist}(\mathbf{v}/3, \mathcal{L}(\mathbf{B}_{k-1})) \geq \lambda_1(\mathbf{B}_{k-1}) \geq 1.$$

Let $\mathbf{s} \in \{-1, 0, +1\}^n$ be such that $\mathbf{s} \equiv \mathbf{x} \pmod 3$, i.e., $(\mathbf{s} - \mathbf{x})/3 \in \mathbb{Z}^n$. We claim that the distance of $\mathbf{t} = (1/3)\mathbf{B}_{k-1}\mathbf{s}$ from the lattice $\mathcal{L}(\mathbf{B}_{k-1})$ is at least 1. Notice that

$$\mathbf{t} = (1/3)\mathbf{B}_{k-1}\mathbf{s} = \mathbf{B}_{k-1}\mathbf{x}/3 + \mathbf{B}_{k-1}(\mathbf{s} - \mathbf{x})/3 \in \mathbf{v}/3 + \mathcal{L}(\mathbf{B}_{k-1}).$$

It follows that $\mathrm{dist}(\mathbf{t}, \mathcal{L}(\mathbf{B}_{k-1})) = \mathrm{dist}(\mathbf{v}/3, \mathcal{L}(\mathbf{B}_{k-1})) \geq 1$, and therefore the algorithm does not terminate at iteration $k$.

We conclude the proof of the theorem by giving a simple algorithm to solve the closest vector problem in $\mathcal{L}(\mathbf{B}_k)$ in time $n^{O(1)} \cdot 3^k \leq n^{O(1)+n/2}$. Notice that any lattice point in $\mathcal{L}(\mathbf{B}_k)$ can be written as $\mathbf{B}_0\mathbf{x} + [\mathbf{v}_1, \ldots, \mathbf{v}_k]\mathbf{y}$ where $\mathbf{x} \in \mathbb{Z}^n$ and $\mathbf{y} \in \{-1, 0, +1\}^k$. So, in order to find the lattice point closest to some target $\mathbf{t}$, we can consider all vectors of the form $\mathbf{t} - [\mathbf{v}_1, \ldots, \mathbf{v}_k]\mathbf{y}$ and compute their distance from $\mathcal{L}(\mathbf{B}_0)$. Let $\mathbf{y}$ such that $\mathrm{dist}(\mathbf{t} - [\mathbf{v}_1, \ldots, \mathbf{v}_k]\mathbf{y}, \mathcal{L}(\mathbf{B}_k))$ is minimized, and let $\mathbf{B}_0\mathbf{x}$ the lattice vector closest to $\mathbf{t} - [\mathbf{v}_1, \ldots, \mathbf{v}_k]\mathbf{y}$. The lattice vector in $\mathcal{L}(\mathbf{B}_k)$ closest to $\mathbf{t}$ is $\mathbf{B}_0\mathbf{x} + [\mathbf{v}_1, \ldots, \mathbf{v}_k]\mathbf{y}$. □

The theorem gives an algorithmic construction of almost perfect lattices and an algorithm to solve the closest vector problem, however the running time is huge. The next theorem shows how to use these lattices for small values of $n$ to get a construction that runs in polynomial time.

**Theorem 3** *There exists a family of $\tau(n)$-perfect easily decodable lattices with $\tau(n) = O(\sqrt{n \log\log n / \log n})$.*

**Proof:** In order to keep the construction polynomial in $n$, we use Theorem 2 to build a 3-perfect lattice $\mathbf{M}$ in dimension $m = \log n / \log\log n$. Notice that such a lattice can be constructed in time

$$2^{O(m \log m)} = 2^{O(\log n \log(\log n / \log\log n)/\log\log n)} = n^{O(1)}.$$

Moreover, the closest vector problem in this lattice can also be solved in time $2^{O(m \log m)} = n^{O(1)}$.

Now set $\mathbf{L}_n$ to the direct sum of $(n/m)$ copies of $\mathbf{M}$. The lattice vector in $\mathcal{L}(\mathbf{L}_n)$ closest to a target $\mathbf{t}$ is easily found by breaking $\mathbf{t}$ into $n/m$ blocks, each with $m$ coordinates in it, and finding the $\mathcal{L}(\mathbf{M})$ vector closest to each block. Moreover, the length of the shortest nonzero vector in $\mathcal{L}(\mathbf{L}_n)$ is $\lambda_1(\mathbf{M})$ because vectors from different copies of $\mathbf{M}$ are orthogonal. Finally, the covering radius of $\mathbf{L}_n$ is $\sqrt{n/m}$ times $\rho(\mathbf{M})$. So, $\mathbf{L}_n$ is $\tau(n)$-perfect for

$$\tau(n) = \frac{\sqrt{n/m}\rho(\mathbf{M})}{\lambda_1(\mathbf{M})/2} \leq 3\sqrt{n/m} = O(\sqrt{n \log\log n / \log n}).$$

□

# 5 A generalized class of random lattices

In this section we define a class of random lattices that generalizes Ajtai's one. The class is parametrized by an easily decodable family of $\tau(n)$-perfect lattices $\{\mathcal{L}(\mathbf{L}_n)\}_{n>0}$ (with decoding algorithm $\mathrm{CVP}_{\mathbf{L}}$), and two functions $\alpha(n)$ and $m(n)$. For any $n > 0$, we use decoding algorithm $\mathrm{CVP}_{\mathbf{L}}$ and function $\alpha(n)$ to define a finite group $G_n$, and then use $G_n$ to define a finite collection of $m(n)$-dimensional lattices. Assume function $\alpha(n)$ satisfies

$$\alpha(n) \geq 2\sqrt{n}\rho(\mathbf{L}_n). \tag{11}$$

Using (11) and the fact that $\|\mathbf{x} - \mathrm{CVP}_{\mathbf{L}}(\mathbf{x})\| \leq \rho(\mathbf{L}_n)$ for all $\mathbf{x} \in \mathbb{R}^n$, Lemma 1 immediately gives a full rank sublattice $\mathbf{M}_n \subset \mathcal{L}(\mathbf{L}_n)$ such that

$$\forall \mathbf{x} \in \mathbb{R}^n . \|\mathbf{M}_n\mathbf{x}\| \approx \alpha(n) \cdot \|\mathbf{x}\|. \tag{12}$$

Group $G_n$ is defined as the quotient

$$G_n = \mathcal{L}(\mathbf{L}_n)/\mathcal{L}(\mathbf{M}_n) \tag{13}$$

of $\mathcal{L}(\mathbf{L}_n)$ modulo the "almost orthogonal" sublattice $\mathcal{L}(\mathbf{M}_n) \subset \mathcal{L}(\mathbf{L}_n)$.

The random lattices are defined as the set of solutions of a homogeneous linear equation over group $G_n$. More precisely, for any $m(n)$-tuple of group elements $\mathbf{g} = [g_1, \ldots, g_{m(n)}]^T \in G_n^{m(n)}$, define the $m(n)$-dimensional integer lattice

$$\Lambda(\mathbf{g}) = \{\mathbf{x} \in \mathbb{Z}^{m(n)} : \sum_{i=1}^{m(n)} x_i \cdot g_i = 0\}, \tag{14}$$

where equation $\sum x_i \cdot g_i = 0$ is over group $G_n$.

We know from Proposition 4 that $\Lambda(\mathbf{g})$ is a lattice with determinant at most $|\det(\Lambda(\mathbf{g}))| \leq \#G_n$. In the rest of this section, we prove that for any $\mathbf{g} \in G_n^{m(n)}$, lattice $\Lambda(\mathbf{g})$ always contains short (nonzero) vectors. The main result of this paper (proved in Sections 6 and 7) is that although these short vectors are guaranteed to exist, they are computationally hard to find when $\mathbf{g}$ is chosen uniformly at random. The following lemma bounds the size of group $G_n$.

**Lemma 5** *For any full rank $n$-dimensional lattice $\mathbf{L}_n$, and any full rank sublattice $\mathbf{M}_n \subset \mathcal{L}(\mathbf{L}_n)$ satisfying (12), the size of group $G_n$ defined in (13) is at most*

$$\#G_n < \left(\frac{3\alpha(n)\sqrt{n}}{2\lambda_1(\mathbf{L}_n)}\right)^n.$$

**Proof:** The size of the group is $\#G_n = |\det(\mathbf{M}_n)|/|\det(\mathbf{L}_n)|$. We bound the two determinants separately. By (12), the columns of $\mathbf{M}_n$ have length at most

$$\|\mathbf{M}_n\mathbf{e}_i\| \leq (3/2)\alpha(n) \cdot \|\mathbf{e}_i\| = 3\alpha(n)/2.$$

Therefore, by Hadamard's inequality

$$|\det(\mathbf{M}_n)| \leq (3\alpha(n)/2)^n.$$

We bound the determinant of $\mathbf{L}_n$ using Minkowski's inequality $\lambda_1(\mathbf{L}_n) < \sqrt{n}|\det(\mathbf{L}_n)|^{1/n}$. Solving for $\det(\mathbf{L}_n)$, we get that the determinant of $\mathcal{L}(\mathbf{L}_n)$ is greater than $(\lambda_1(\mathbf{L}_n)/\sqrt{n})^n$. Combining the two bounds, we get that group $G_n$ has cardinality

$$\#G_n = \frac{|\det(\mathbf{M}_n)|}{|\det(\mathbf{L}_n)|} < \left(\frac{3\alpha(n)\sqrt{n}}{2\lambda_1(\mathbf{L}_n)}\right)^n. \tag{15}$$

□

A bound on the size of the shortest vector in $\Lambda(\mathbf{g})$ easily follows from Proposition 4 and Minkowki's first theorem.

**Theorem 4** *Let $G_n$ be a group satisfying the hypothesis of Lemma 5. For any $\mathbf{g} \in G_n^{m(n)}$, the length of the shortest nonzero vector in the lattice $\Lambda(\mathbf{g})$ defined in (14) is at most*

$$\lambda_1(\Lambda(\mathbf{g})) < \sqrt{m(n)} \cdot \left(\frac{3\alpha(n)\sqrt{n}}{2\lambda_1(\mathbf{L}_n)}\right)^{n/m(n)}.$$

*In particular, if $\alpha(n) = \lambda_1(\mathbf{L}_n) \cdot n^{O(1)}$, and $m(n) = \Theta(n \log n)$, then $\Lambda(\mathbf{g})$ contains nonzero vectors of length at most $\lambda_1(\Lambda(\mathbf{g})) < O(\sqrt{m(n)}) = O(\sqrt{n \log n})$.*

# 6 The iterative process

Let $\{\Lambda(\mathbf{g})\}_{\mathbf{g} \in G_n^{m(n)}}$ be the class of random lattices defined in Section 5, and let $\beta(n)$ an upper bound on the length of the shortest nonzero vector in $\Lambda(\mathbf{g})$. (E.g., $\beta(n) = O(\sqrt{n \log n})$, assuming $\alpha(n) = n^{O(1)}\lambda_1(\mathbf{L}_n)$ and $m(n) = \Theta(n \log n)$ as in Theorem 4.) We want to prove that finding nonzero vectors in $\Lambda(\mathbf{g})$ of length at most $\beta(n)$ (when $\mathbf{g}$ is chosen uniformly at random) is at least as hard as the worst case instance of some other lattice problem. In particular, we consider the problem of finding (for any given $n$-dimensional input lattice $\mathbf{B}$) $n$ short linearly independent vectors $\mathbf{S} \subset \mathcal{L}(\mathbf{B})$ such that $\|\mathbf{S}\| \leq \eta(\mathbf{B})$, where $\eta(\mathbf{B})$ is some (non necessarily polynomial time computable) quantity associated to lattice $\mathcal{L}(\mathbf{B})$. Formally, given oracle access to a procedure $\mathcal{F}$ that on input $\mathbf{g} \in G_n^{m(n)}$ outputs (with non-negligible probability $\delta(n) = 1/n^{O(1)}$ over the random choice of $\mathbf{g}$ and its internal coin tosses) a nonzero lattice vector $\mathcal{F}(\mathbf{g}) \in \Lambda(\mathbf{g}) \setminus \{\mathbf{0}\}$ of length $\|\mathcal{F}(\mathbf{g})\| \leq \beta(n)$, we define a probabilistic polynomial time algorithm that on input any $n$-dimensional basis $\mathbf{B}$ produces (with high probability) a full rank sublattice $\mathbf{S} \subset \mathcal{L}(\mathbf{B})$ such that $\|\mathbf{S}\| \leq \eta(\mathbf{B})$. We remark that while $\mathcal{F}$ is guaranteed to work (with high probability) only when the input $\mathbf{g} \in G_n^{m(n)}$ is chosen uniformly at random, the algorithm to find a set $\mathbf{S}$ of short vectors should work for *any* $n$-dimensional input basis $\mathbf{B}$, and its success probability is computed only with respect to the internal randomness of the algorithm.

This is the problem considered in [1], where $\eta(\mathbf{B}) = \gamma(n) \cdot \mathrm{bl}(\mathbf{B})$, and $\mathrm{bl}(\mathbf{B})$ is the length of the shorted lattice basis, i.e., [1] shows how to find a set of linearly independent vectors $\mathbf{S}$ that are not much longer than (in fact, within a polynomial factor $\gamma(n) = n^{O(1)} \cdot \beta(n)$ from) $\|\mathbf{B}'\|$ for any basis $\mathbf{B}'$ such that $\mathcal{L}(\mathbf{B}) = \mathcal{L}(\mathbf{B}')$. In this paper, we consider a similar problem with $\eta(\mathbf{B}) = \gamma(n) \cdot \hat{\zeta}(\mathbf{B})$. i.e., we find a set of vectors that are not much longer than the generalized uniform radius $\hat{\zeta}(\mathbf{B})$. Comparing the length of $\mathbf{S}$ to the radius $\hat{\zeta}(\mathbf{B})$ allows to achieve an approximation factor $\gamma(n) = \tau(n)\beta(n) \cdot \omega(\sqrt{\log n})$ much smaller than any previous reduction. In turns, as shown in Section 8, relating the radius $\hat{\zeta}(\mathbf{B})$ to other lattice parameters allows to achieve improved connection factors for many classical lattice problems as those considered in [1] (e.g., approximating the length of the shortest vector, or finding short linearly independent vectors) as well as new ones (e.g., approximating the covering radius).

So, let's get to the reduction. Given a basis $\mathbf{B}$ of an $n$-dimensional lattice, we want to find $n$ linearly independent vectors $\mathbf{S}$ such that $\|\mathbf{S}\| \leq \eta(\mathbf{B})$. As in [1, 15], the set $\mathbf{S}$ is computed via an iterative process: starting from the input lattice basis $\mathbf{B}$, one builds sets of shorter and shorter linearly independent lattice vectors $\mathbf{S} \subset \mathcal{L}(\mathbf{B})$. The process ends when a set $\mathbf{S}$ is found that satisfies $\|\mathbf{S}\| \leq \eta(\mathbf{B})$ (with high probability). The core of this iterative process is a probabilistic procedure $\mathcal{A}$ that, on input lattice basis $\mathbf{B}$, and a set of $n$ linearly independent vectors $\mathbf{S} \subset \mathcal{L}(\mathbf{B})$, outputs a new lattice vector $\mathbf{s} \in \mathcal{L}(\mathbf{B})$ linearly independent

from $\mathbf{S} \setminus \{\mathbf{s}_i\}$ (for some $i \in \{1, \ldots, n\}$) such that $\|\mathbf{s}\| \leq \frac{1}{2}\|\mathbf{s}_i\|$. (These conditions on $\mathbf{s}$ can be compactly expressed as $\mathbf{s} \notin \text{span}\{\mathbf{s}_i : \|\mathbf{s}_i\| < 2\|\mathbf{s}\|\}$.) When successful, the probabilistic procedure allows to replace $\mathbf{s}_i$ with a shorter vector $\mathbf{s}$ of length at most $\frac{1}{2}\|\mathbf{s}_i\|$, while keeping the vectors in $\mathbf{S}$ linearly independent.[11] Since lattices are discrete objects, vectors $\mathbf{s}_i$ cannot be shortened indefinitely, and at some point the probabilistic procedure is bound to fail. So, as soon as the probabilistic procedure stops working we can conclude (with high probability) that $\|\mathbf{S}\| \leq \eta(\mathbf{B})$ holds true, i.e., we have found a set of short linearly independent vectors. This iterative process is formalized in the next lemma.

**Lemma 6** *Assume that there exists a (probabilistic) polynomial time procedure $\mathcal{A}(\cdot, \cdot)$ that on input a lattice basis $\mathbf{B}$ and a set of linearly independent vectors $\mathbf{S} \subset \mathcal{L}(\mathbf{B})$ such that $\|\mathbf{S}\| > \eta(\mathbf{B})$, outputs (with non-negligible probability $\delta(n) = 1/n^{O(1)}$ over its internal coin tosses) a lattice vector $\mathbf{s} = \mathcal{A}(\mathbf{B}, \mathbf{S}) \in \mathcal{L}(\mathbf{B})$ such that $\mathbf{s} \notin span\{\mathbf{s}_i \mid \|\mathbf{s}_i\| < 2\|\mathbf{s}\|\}$. Then, there is a probabilistic polynomial time (oracle) algorithm that on input any lattice basis $\mathbf{B}$, finds with probability exponentially close to 1 (and with polynomially many calls to $\mathcal{A}$), a set of linearly independent vectors $\mathbf{S} \subset \mathcal{L}(\mathbf{B})$ such that $\|\mathbf{S}\| \leq \eta(\mathbf{B})$.*

**Proof:** We remark that procedure $\mathcal{A}$ is assumed to work (with non-negligible probability) for *any* input $(\mathbf{B}, \mathbf{S})$ such that $\|\mathbf{S}\| > \eta(\mathbf{B})$. Let $\delta(n) = n^{-\Omega(1)}$ be the minimum probability that $\mathcal{A}(\mathbf{B}, \mathbf{S})$ is successful over all possible $n$-dimensional $\mathbf{B}$ and $\mathbf{S}$ such that $\|\mathbf{S}\| > \eta(\mathbf{B})$. Let $\mathbf{B}$ be the input basis for which we want to find linearly independent vectors $\mathbf{S} \subset \mathcal{L}(\mathbf{B})$ such that $\|\mathbf{S}\| \leq \eta(\mathbf{B})$. Set $\mathbf{S}$ is computed as follows:

1. Initialize $\mathbf{S} = \mathbf{B}$ (after optionally applying the LLL basis reduction algorithm to $\mathbf{B}$).
2. Repeatedly call $\mathbf{s} = \mathcal{A}(\mathbf{B}, \mathbf{S})$, until either $\mathbf{s} \notin \text{span}\{\mathbf{s}_i \mid \|\mathbf{s}_i\| < 2\|\mathbf{s}\|\}$ or the procedure fails more than
$$t = \frac{1}{\delta(n)} \ln\left(\frac{\log_2(\text{defect}(\mathbf{B}))}{\epsilon}\right)$$
consecutive times, where $\epsilon$ is the desired error probability.
3. If a vector $\mathbf{s} \notin \text{span}\{\mathbf{s}_i \mid \|\mathbf{s}_i\| < 2\|\mathbf{s}\|\}$ is found, let $i$ be such that $\|\mathbf{s}\| \leq \frac{1}{2}\|\mathbf{s}_i\|$ and $\mathbf{s}$ is linearly independent from $\mathbf{S} \setminus \{\mathbf{s}_i\}$. Replace $\mathbf{s}_i$ with $\mathbf{s}$ and go back to step 2.
4. If $\mathcal{A}$ failed more than $t$ times consecutively, then output $\mathbf{S}$.

The correctness of the procedure is based on the following observation: at iteration $k$, $\mathbf{S} \subset \mathcal{L}(\mathbf{B})$ is a set of $n$ linearly independent lattice vectors such that $\prod_i \|\mathbf{s}_i\| \leq 2^{-k} \cdot \prod_i \|\mathbf{b}_i\|$. This is certainly true right after initialization for $k = 0$. Now, assume by induction that $\mathbf{S} \subset \mathcal{L}(\mathbf{B})$ are $n$ linearly independent vectors such that $\prod_i \|\mathbf{s}_i\| \leq 2^{-k} \cdot \prod_i \|\mathbf{b}_i\|$. Assume also that a vector $\mathbf{s} \notin \text{span}\{\mathbf{s}_i \mid \|\mathbf{s}_i\| < 2\|\mathbf{s}\|\}$ is found. Since $\mathbf{S}$ is a set of $n$ linearly independent lattice vectors, we have $\mathcal{L}(\mathbf{B}) \subset \text{span}(\mathbf{S})$, and we can write $\mathbf{s}$ as a (not necessarily integer) linear combination of the vectors in $\mathbf{S}$. Let $\mathbf{s} = \sum_i \alpha_i \mathbf{s}_i$. From property $\mathbf{s} \notin \text{span}\{\mathbf{s}_i \mid \|\mathbf{s}_i\| < 2\|\mathbf{s}\|\}$, there must exists an index $i$ such that $\alpha_i \neq 0$ and $\|\mathbf{s}_i\| \geq 2\|\mathbf{s}\|$. It follows that $\mathbf{s}$ is linearly independent from $\mathbf{S} \setminus \{\mathbf{s}_i\}$. So, replacing $\mathbf{s}_i$ with $\mathbf{s}$, results in a set $\{\mathbf{s}_1, \ldots, \mathbf{s}_{i-1}, \mathbf{s}, \mathbf{s}_{i+1}, \ldots, \mathbf{s}_n\}$ of linearly independent lattice vectors such that $\|\mathbf{s}\| \cdot \prod_{j \neq i} \|\mathbf{s}_j\| = \frac{1}{2} \prod_j \|\mathbf{s}_j\| \leq 2^{-(k+1)} \cdot \prod_i \|\mathbf{b}_i\|$.

We can now get an upper bound on the number of iterations. Since $\mathcal{L}(\mathbf{S})$ is a full rank sublattice of $\mathcal{L}(\mathbf{B})$, we have $|\det(\mathbf{B})| \leq |\det(\mathbf{S})| \leq \prod_i \|\mathbf{s}_i\|$. Therefore, our bound on $\prod_i \|\mathbf{s}_i\|$ implies that if the algorithm performs $k$ iterations, then it must be $|\det(\mathbf{B})| \leq 2^{-k} \cdot \prod_i \|\mathbf{b}_i\|$, i.e.,

$$k \leq \log_2(\prod_i \|\mathbf{b}_i\| / \det(\mathbf{B})) = \log_2 \text{defect}(\mathbf{B}).$$

Notice that the maximum number of iterations $\log_2 \text{defect}(\mathbf{B})$ is polynomial in the size of the input $\mathbf{B}$ because the orthogonality defect can be computed in polynomial time.[12]

[11] The iterative process as described here follows the proof given in [15]. The iterative process as formulated in [1, 8] required a slightly more complicated basic procedure that on input $\mathbf{B}$ and $\mathbf{S}$ returns not just a vector $\mathbf{s}$, but an entire set of linearly independent vectors $\mathbf{S}'$ such that $\|\mathbf{S}'\| \leq \frac{1}{2}\|\mathbf{S}\|$, and the entire set $\mathbf{S}$ is replaced by $\mathbf{S}'$ at every iteration.

[12] Moreover, it can be shown that LLL reduced bases always have orthogonality defect at most $2^{O(n^2)}$. So, by applying the LLL reduction algorithm on the input basis $\mathbf{B}$ one can always guarantee that the number of iterations is $O(n^2)$, independently of the size of the input.

This proves that for any non-negligible $\delta(n) = n^{-O(1)}$, and $\epsilon \geq e^{n^{O(1)}}$, the algorithm outputs a set $\mathbf{S}$ in polynomial time. We need to prove that the final output $\mathbf{S}$ satisfies $\|\mathbf{S}\| \leq \eta(\mathbf{B})$ with high probability. We bound the probability that the algorithm terminates with a set $\mathbf{S}$ such that $\|\mathbf{S}\| > \eta(\mathbf{B})$. By union bound, the probability of outputting such a set is at most the maximum number of iterations times the probability of outputting such a set during any fixed iteration. Assume that the algorithm terminates at iteration $k$ and outputs a set $\mathbf{S}$ such that $\|\mathbf{S}\| > \eta(\mathbf{B})$. This happens only if $\mathcal{A}(\mathbf{B}, \mathbf{S})$ repeatedly fails in $t$ independent runs. Since in each run the failure probability is at most $1 - \delta(n)$, the probability that $\mathbf{S}$ is output at iteration $k$ is at most $(1 - \delta(n))^t \leq e^{-t \cdot \delta(n)} = \epsilon / \log_2 \text{defect}(\mathbf{B})$. Since the number of iterations is at most $\log_2 \text{defect}(\mathbf{B})$, by union bound the probability that the algorithm outputs a set $\mathbf{S}$ such that $\|\mathbf{S}\| > \eta(\mathbf{B})$ is at most $\epsilon$. $\square$

In order to use Lemma 6, we need to exhibit an algorithm that, on input linearly independent vectors such that $\|\mathbf{S}\| > \eta(\mathbf{B})$, finds with high probability a new short vector $\mathbf{s}$. This is formalized in the next lemma which will be proved in Section 7.

**Lemma 7** *Let $\{\mathbf{L}_n\}$ a family of easily decodable $\tau(n)$-perfect lattices, $\beta(n) \geq 1$, $m(n) = n^{O(1)}$ and $\gamma(n) = \beta(n)\tau(n) \cdot \omega(\sqrt{\log n})$. Then, if $G_n$ is the group associated to lattice $\mathcal{L}(\mathbf{L}_n)$ and function $\alpha(n) = n\lambda_1(\mathbf{L}_n)\gamma(n)/12$ defined in Section 5, then following is true. Assume there exists a probabilistic polynomial time procedure $\mathcal{F}$ that on input a uniformly chosen random vector $\mathbf{g} \in G_n^{m(n)}$, produces a nonzero lattice vector $\mathcal{F}(\mathbf{g}) \in \Lambda(\mathbf{g})$ of length $\|\mathcal{F}(\mathbf{g})\| \leq \beta(n)$ with non-negligible probability $\delta(n) = 1/n^{O(1)}$. Then, there exists a probabilistic polynomial time algorithm $\mathcal{A}^{\mathcal{F}}(\cdot, \cdot)$ that on input any $n$-dimensional lattice basis $\mathbf{B}$ and a set of linearly independent lattice vectors $\mathbf{S} \subset \mathcal{L}(\mathbf{B})$ such that $\|\mathbf{S}\| > \gamma(n) \cdot \hat{\zeta}(\mathbf{B})$, outputs a lattice vector $\mathbf{s} = \mathcal{A}^{\mathcal{F}}(\mathbf{B}, \mathbf{S}) \in \mathcal{L}(\mathbf{B})$ such that*

$$\Pr\{\mathbf{s} \notin \mathit{span}\{\mathbf{s}_i \mid 2\|\mathbf{s}_i\| < \|\mathbf{s}\|\} = \Omega(\delta(n)).$$

Combining Lemma 6 with Lemma 7, we get the following theorem, which is the main technical result of this paper.

**Theorem 5** *Let $\{\mathbf{L}_n\}$ a family of easily decodable $\tau(n)$-perfect lattices, $\beta(n) \geq 1$, $m(n) = n^{O(1)}$ and $\gamma(n) = \beta(n)\tau(n) \cdot \omega(\sqrt{\log n})$. If $G_n$ is the group associated to lattice $\mathcal{L}(\mathbf{L}_n)$ and function $\alpha(n) = n\lambda_1(\mathbf{L}_n)\gamma(n)/12$ defined in Section 5, then following is true. Assume there exists a probabilistic polynomial time procedure $\mathcal{F}$ that on input a uniformly chosen random vector $\mathbf{g} \in G_n^{m(n)}$, produces a nonzero lattice vector $\mathcal{F}(\mathbf{g}) \in \Lambda(\mathbf{g})$ of length $\|\mathcal{F}(\mathbf{g})\| \leq \beta(n)$ with non-negligible probability. Then, there is a probabilistic polynomial time algorithm that on input any lattice basis $\mathbf{B}$, finds with probability exponentially close to 1 a set of linearly independent vectors $\mathbf{S} \subset \mathcal{L}(\mathbf{B})$ such that $\|\mathbf{S}\| \leq \gamma(n) \cdot \hat{\zeta}(n)$.*

# 7 The iterative step

In this section we prove Lemma 7 from Section 6. Let $\mathcal{F}$ be a probabilistic polynomial time algorithm as in the lemma. We use $\mathcal{F}$ to build algorithm $\mathcal{A}^{\mathcal{F}}(\mathbf{B}, \mathbf{S})$. It is convenient in the design and analysis of $\mathcal{A}$ to assume that $\mathcal{F}$ is deterministic. So, first of all, in Subsection 7.1 we show how to probabilistically transform a randomized $\mathcal{F}$ into a deterministic procedure. In Subsection 7.2 we show how to use a deterministic $\mathcal{F}$ to build algorithm $\mathcal{A}$. The construction is based on a sampling algorithm that is described and analyzed in Subsection 7.3. In Subsection 7.4 we prove some technical lemmas that are useful in the analysis of the reduction. Finally, in Subsection 7.5 we prove that the algorithm of Subsection 7.2 satisfies Lemma 7. The properties of the sampling procedure established in Subsection 7.3 are used only in the proofs of the technical lemmas in Subsection 7.4, and these lemmas are only used in Subsection 7.5. So, at a first reading, the reader might want to skip Subsections 7.3 and 7.4, and jump directly to Subsection 7.5 to see how the technical lemmas are used to prove the main theorem.

## 7.1 Making the shortest vector procedure deterministic

Let $\mathcal{F}$ be a probabilistic procedure that on input a randomly chosen $\mathbf{g} \in G_n^{m(n)}$ outputs a vector $\mathbf{z} = \mathcal{F}(\mathbf{g})$ such that $\mathbf{z} \in \Lambda(\mathbf{g}) \setminus \{\mathbf{0}\}$ and $\|\mathbf{z}\| \leq \beta(n)$ with non-negligible probability $\delta(n) = n^{-O(1)}$. We show how to probabilistically convert $\mathcal{F}$ into a *deterministic* (polynomial time computable) function $\mathcal{F}'$ such that

$\mathcal{F}'(\mathbf{g}) \in \Lambda(\mathbf{g}) \setminus \{\mathbf{0}\}$ for *every* $\mathbf{g}$, and $\|\mathcal{F}'(\mathbf{g})\| \leq \beta(n)$ for a non-negligible fraction $\delta(n)/4$ of the inputs $\mathbf{g} \in G_n^{m(n)}$. The transformation is simple and uses standard probability amplification techniques.

**Lemma 8** *Assume there exists a probabilistic polynomial time algorithm $\mathcal{F}$ that on input a uniformly chosen random vector $\mathbf{g} \in G_n^{m(n)}$ produces a nonzero lattice vector in $\Lambda(\mathbf{g})$ of length $\|\mathcal{F}(g)\| \leq \beta(n)$ with probability $\delta(n)$. Then there exists a* deterministic *polynomial time algorithm $\mathcal{F}'$ such that $\mathcal{F}'(\mathbf{g}) \in \Lambda(\mathbf{g}) \setminus \{\mathbf{0}\}$ for all $\mathbf{g} \in G_n^{m(n)}$ and $\|\mathcal{F}'(\mathbf{g})\| \leq \beta(n)$ for a $\delta(n)/4$ fraction of the inputs $\mathbf{g} \in G_n^{m(n)}$. Moreover, there is an efficient (probabilistic) transformation from $\mathcal{F}$ to $\mathcal{F}'$ that succeeds with probability at least $1 - 2/e$.*

**Proof:** Consider $\mathcal{F}$ as a deterministic function that takes as input a vector $\mathbf{g} \in G_n^{m(n)}$ and a random string $r$. Let $X$ be the set of pairs $(\mathbf{g}, r)$ such that $\mathcal{F}$ is successful, i.e., $\mathcal{F}(\mathbf{g}, r) \in \Lambda(\mathbf{g}) \setminus \{\mathbf{0}\}$ and $\|\mathcal{F}(\mathbf{g}, r)\| \leq \beta(n)$. We know that $\Pr_{\mathbf{g},r}\{(\mathbf{g}, r) \in X\} \geq \delta(n)$. Choose $2/\delta(n)$ random strings $r_1, \ldots, r_{2/\delta(n)}$, and define $\mathcal{F}'(\mathbf{g})$ as follows:

- If $(\mathbf{g}, r_i) \notin X$ for all $i = 1, \ldots, 2/\delta(n)$, then $\mathcal{F}'(\mathbf{g})$ outputs an arbitrary (possibly long) vector in $\Lambda(\mathbf{g}) \setminus \{\mathbf{0}\}$.
- Otherwise $\mathcal{F}'(\mathbf{g}) = \mathcal{F}(\mathbf{g}, r_i)$, where $i$ is the smallest index such that $(\mathbf{g}, r_i) \in X$.

Clearly, $\mathcal{F}'(\mathbf{g}) \in \Lambda(\mathbf{g}) \setminus \{\mathbf{0}\}$ for all $\mathbf{g} \in G_n^{m(n)}$. We claim that with probability at least $1 - 2/e$ (over the choice of $r_1, \ldots, r_{2/\delta(n)}$), $\|\mathcal{F}'(\mathbf{g})\| \leq \beta(n)$ for a $\delta(n)/4$ fraction of the inputs $\mathbf{g}$. Let $Y$ be the set of all $\mathbf{g}$ such that $\Pr_r\{(\mathbf{g}, r) \in X\} \geq \delta(n)/2$. By Markov inequality

$$\begin{aligned}
\Pr_{\mathbf{g}}\{\mathbf{g} \notin Y\} &= \Pr_{\mathbf{g}}\{1 - \Pr_r\{(\mathbf{g}, r) \in X\} > 1 - \delta(n)/2\} \\
&\leq \frac{\mathrm{Exp}_{\mathbf{g}}[1 - \Pr_r\{(\mathbf{g}, r) \in X\}]}{1 - \delta(n)/2} \\
&= \frac{1 - \Pr_{\mathbf{g},r}\{(\mathbf{g}, r) \in X\}}{1 - \delta(n)/2} \\
&\leq \frac{1 - \delta(n)}{1 - \delta(n)/2} \\
&< 1 - \frac{\delta(n)}{2}.
\end{aligned}$$

This proves that $Y$ contains at least a $\delta(n)/2$ fraction of all $\mathbf{g} \in G_n^{m(n)}$. Now, consider the expected number of $\mathbf{g} \in Y$ such that $\|\mathcal{F}'(\mathbf{g})\| > \beta(n)$, expectation computed over the choice of $\mathbf{r} = (r_1, \ldots, r_{2/\delta(n)})$. By linearity of expectation,

$$\begin{aligned}
\mathrm{Exp}_{\mathbf{r}}[\#\{\mathbf{g} \in Y : \|\mathcal{F}'(\mathbf{g})\| > \beta(n)\}] &= \sum_{\mathbf{g} \in Y} \Pr_{\mathbf{r}}\{\|\mathcal{F}'(\mathbf{g})\| > \beta(n)\} \\
&\leq \sum_{\mathbf{g} \in Y} \left(1 - \frac{\delta(n)}{2}\right)^{2/\delta(n)} \\
&\leq (\#Y) \cdot e^{-1}.
\end{aligned}$$

It follow by Markov inequality that the number of $\mathbf{g} \in Y$ such that $\|\mathcal{F}'(\mathbf{g})\| > \beta(n)$ is larger than $(\#Y)/2$ with probability at most $2/e$ over the choice of $\mathbf{r}$. Therefore, with probability at least $1 - 2/e$ over the choice of randomness $\mathbf{r}$, $\|\mathcal{F}'(\mathbf{g})\| \leq \beta(n)$ for at least $\#Y/2$ values of $\mathbf{g}$, which is at least a $\delta(n)/4$ fraction of all $\mathbf{g} \in G_n^{m(n)}$. $\square$

## 7.2 The reduction

Let $\mathcal{F}$ be a deterministic procedure that on input a randomly chosen $\mathbf{g} \in G_n^{m(n)}$ outputs a nonzero lattice vector $\mathcal{F}(\mathbf{g}) \in \Lambda(\mathbf{g}) \setminus \{\mathbf{0}\}$. We define a probabilistic polynomial time oracle algorithm $\mathcal{A}^{(\cdot)}(\cdot, \cdot)$ that given full

rank $n$-dimensional lattice $\mathbf{B}$ and full rank sublattice $\mathbf{S} \subset \mathcal{L}(\mathbf{B})$ as input, and oracle access to $\mathcal{F}$, outputs a lattice vector

$$\mathbf{s} = \mathcal{A}^{\mathcal{F}}(\mathbf{B}, \mathbf{S}) \in \mathcal{L}(\mathbf{B}).$$

In Subsection 7.5 we will prove that if $\|\mathcal{F}(\mathbf{g})\| \leq \beta(n)$ for a non-negligible fraction $\delta(n) = n^{-O(1)}$ of the inputs $\mathbf{g}$ and $\|\mathbf{S}\| > \gamma(n) \cdot \hat{\zeta}(\mathbf{B})$ (for approximation factor $\gamma(n) = \tau(n)\beta(n) \cdot \omega(\sqrt{\log n})$), then

$$\Pr\{\mathbf{s} \notin \text{span}\{\mathbf{s}_i : \|\mathbf{s}_i\| < 2\|\mathbf{s}\|\}\} = \Omega(\delta(n)),$$

where the probability is computed over the random choices of algorithm $\mathcal{A}$ only.

Procedure $\mathcal{A}$ works as follows. First of all, notice that using Babai's nearest plane algorithm, matrix $\mathbf{S}$ allows to approximate any vector $\mathbf{x}$ with a lattice point $\mathbf{y} \in \mathcal{L}(\mathbf{S}) \subseteq \mathcal{L}(\mathbf{B})$ within distance $\sigma = (\sqrt{n}/2)\|\mathbf{S}\|$ from $\mathbf{x}$.[13] Therefore, using Lemma 1, we can find an almost orthogonal sublattice $\mathcal{L}(\mathbf{C}) \subset \mathcal{L}(\mathbf{B})$ such that

$$\forall \mathbf{x} \in \mathbb{R}^n . \|\mathbf{C}\mathbf{x}\| \approx n\|\mathbf{S}\| \cdot \|\mathbf{x}\|. \tag{16}$$

Define the linear transformation

$$\psi(\mathbf{x}) = \mathbf{C}\mathbf{M}_n^{-1}\mathbf{x}$$

such that $\psi(\mathbf{m}_i) = \mathbf{c}_i$ for all $i = 1, \ldots, n$. Using (12) and (16) we get that

$$\forall \mathbf{x} \in \mathbb{R}^n . \frac{1}{3}\|\psi(\mathbf{x})\| \leq \frac{n\|\mathbf{S}\|}{\alpha(n)} \cdot \|\mathbf{x}\| \leq 3\|\psi(\mathbf{x})\|. \tag{17}$$

Notice that $\mathcal{L}(\mathbf{M}_n)$ is a common sublattice of both $\mathcal{L}(\mathbf{L}_n)$ and $\psi^{-1}(\mathcal{L}(\mathbf{B}))$. Lemma 10 in the next subsection shows how to use function $\psi$ together with decoding algorithm $\text{CVP}_{\mathbf{L}}$ to simultaneously sample groups $G_n = \mathcal{L}(\mathbf{L}_n)/\mathcal{L}(\mathbf{M}_n)$ and $\mathcal{L}(\mathbf{B})/\mathcal{L}(\mathbf{C})$. The actual details of the sampling procedure are not important at this point. Below we describe how to use any sampling procedure to define algorithm $\mathcal{A}^{\mathcal{F}}(\mathbf{B}, \mathbf{S})$. After defining a full rank sublattice $\mathbf{C} \subset \mathcal{L}(\mathbf{S})$ and function $\psi$ satisfying (17), algorithm $\mathcal{A}^{\mathcal{F}}$ proceeds as follows:

1. Run the sampling procedure $m(n) \cdot k(n)$ times (where $k(n) = \omega(\log n)$ is a superlogarithmic function to be specified) to generate vectors $\mathbf{v}_{i,j} \in \mathcal{L}(\mathbf{B})$ and $\mathbf{w}_{i,j} \in \mathcal{L}(\mathbf{L}_n)$, for $i = 1, \ldots, m(n)$ and $j = 1, \ldots, k(n)$.
2. Let $a_{i,j} = [\mathbf{w}_{i,j}]_{\mathbf{M}_n} \in G_n$ be the group element corresponding to lattice point $\mathbf{w}_{i,j}$ and, for every $i = 1, \ldots, m(n)$, define group element $a_i = \sum_{j=1}^{k(n)} a_{i,j}$.
3. Use oracle $\mathcal{F}$ to compute vector $\mathbf{z} = \mathcal{F}(\mathbf{a}) \in \Lambda(\mathbf{a}) \setminus \{\mathbf{0}\}$, where $\mathbf{a} = [a_1, \ldots, a_{m(n)}]^T$.
4. For any $i, j$, let $\mathbf{y}_{i,j} = \mathbf{v}_{i,j} - \psi(\mathbf{w}_{i,j})$, and output

$$\mathbf{s} = \sum_{i=1}^{m(n)} z_i \sum_{j=1}^{k(n)} \mathbf{y}_{i,j}. \tag{18}$$

In the following lemma we prove that algorithm $\mathcal{A}^{\mathcal{F}}$ is correct, i.e., the output vector $\mathbf{s}$ always belongs to $\mathcal{L}(\mathbf{B})$.

**Lemma 9** *Let $\mathbf{s}$ be the output vector defined in (18). Then $\mathbf{s} \in \mathcal{L}(\mathbf{B})$.*

**Proof:** Define the vector

$$\mathbf{w} = \sum_{i=1}^{m(n)} z_i \sum_{j=1}^{k(n)} \mathbf{w}_{i,j}.$$

[13] This is not a particularly critical part of the reduction, and using poorer rounding procedures (e.g., rounding off the coordinates of $\mathbf{x}$ with respect to basis $\mathbf{S}$ to the closest integers as done in [1]) results in substantially the same connection factors as using Babai's nearest plane algorithm.

Using the definition of $\mathbf{y}_{i,j}$ and the linearity of $\psi$, we have

$$\mathbf{s} = \sum_{i=1}^{m(n)} z_i \sum_{j=1}^{k(n)} \mathbf{y}_{i,j} = \sum_{i,j} z_i(\mathbf{v}_{i,j} - \psi(\mathbf{w}_{i,j})) = \left(\sum_{i,j} z_i \mathbf{v}_{i,j}\right) - \psi(\mathbf{w}).$$

The first term $\sum_{i,j} z_i \mathbf{v}_{i,j}$ clearly belongs to $\mathcal{L}(\mathbf{B})$ because it is an integer linear combination of lattice vectors $\mathbf{v}_{i,j} \in \mathcal{L}(\mathbf{B})$. We need to prove that also the second term $\psi(\mathbf{w})$ belongs to $\mathcal{L}(\mathbf{B})$. We show that $\mathbf{w} \in \mathcal{L}(\mathbf{M}_n)$. Since $\psi$ maps $\mathcal{L}(\mathbf{M})$ to $\mathcal{L}(\mathbf{C})$, it follows that $\psi(\mathbf{w}) \in \mathcal{L}(\mathbf{C}) \subseteq \mathcal{L}(\mathbf{B})$.

Remember that $\mathbf{z} = \mathcal{F}(\mathbf{a}) \in \Lambda(\mathbf{a})$, i.e., $\sum_i z_i a_i = 0$ (in $G_n$). Since all $\mathbf{w}_{i,j}$ belong to $\mathcal{L}(\mathbf{L})$, also $\mathbf{w}$ is a lattice point of $\mathcal{L}(\mathbf{L})$ and $[\mathbf{w}]_{\mathbf{M}_n} \in G_n$. The group element corresponding to lattice vector $\mathbf{w}$ is

$$[\mathbf{w}]_{\mathbf{M}_n} = \sum_{i=1}^{m(n)} z_i \sum_{j=1}^{k(n)} [\mathbf{w}_{i,j}]_{\mathbf{M}_n} = \sum_i z_i \sum_j a_{i,j} = \sum_i z_i a_i = 0.$$

Since $G_n$ is the quotient of $\mathcal{L}(\mathbf{L}_n)$ modulo $\mathcal{L}(\mathbf{M}_n)$, this proves that $\mathbf{w} \in \mathcal{L}(\mathbf{M}_n)$. □

## 7.3 The sampling procedure

In this subsection we define a sampling procedure to be used in the reduction of Subsection 7.2, and prove some important properties about its output distribution. The sampling procedure is illustrated in Figure 1.

**Lemma 10** *There is a sampling algorithm that on input two full rank $n$-dimensional lattices $\mathbf{L}_n$ and $\mathbf{B}$, a full rank sublattice $\mathbf{M}_n \subset \mathcal{L}(\mathbf{L}_n)$ and a non-singular linear transformation $\psi$ such that $\mathbf{C} = \psi(\mathbf{M}) \subset \mathcal{L}(\mathbf{B})$, outputs two vectors $\mathbf{v} \in \mathcal{L}(\mathbf{B})$ and $\mathbf{w} \in \mathcal{L}(\mathbf{L}_n)$ such that the following holds:*

1. *The group element $[\mathbf{v}]_{\mathbf{C}}$ is uniformly distributed over $\mathcal{L}(\mathbf{B})/\mathcal{L}(\mathbf{C})$.*
2. *$\psi^{-1}(\mathbf{v}) \in \bar{\mathcal{V}}(\mathbf{w}, \mathbf{L}_n)$, or, equivalently, $\mathbf{v} - \psi(\mathbf{w}) \in \psi(\bar{\mathcal{V}}(\mathbf{L}_n))$.*
3. *The distribution of $\mathbf{v} - \psi(\mathbf{w})$ is symmetric about the origin, and, in particular, $Exp[\mathbf{v} - \psi(\mathbf{w})] = 0$.*
4. *$\mathbf{w} \in \mathcal{P}(\mathbf{M}_n)$*

*Moreover, if lattice $\mathbf{L}_n$ is easily decodable, then the sampling procedure runs in polynomial time.*

**Proof:** We first show how to achieve the first two properties. Choose integers

$$d_1, \ldots, d_n \in \{1, \ldots, \det(\mathbf{C})/\det(\mathbf{B})\}$$

uniformly at random and let $\mathbf{v}'' = \sum_i d_i \mathbf{b}_i \in \mathcal{L}(\mathbf{B})$. By proposition 3, $[\mathbf{v}'']_{\mathbf{C}}$ is distributed uniformly at random in $\mathcal{L}(\mathbf{B})/\mathcal{L}(\mathbf{C})$. Then, compute $\mathbf{w}'' = \mathrm{CVP}_{\mathbf{L}}(\psi^{-1}(\mathbf{v}''))$. Clearly, $\psi^{-1}(\mathbf{v}'')$ belongs to the Voronoi cell $\bar{\mathcal{V}}(\mathbf{w}'', \mathbf{L}_n)$. So, the pair $(\mathbf{v}'', \mathbf{w}'')$ satisfies the first two properties.

Now, choose $b \in \{0, 1\}$ uniformly at random and set $\mathbf{v}' = (-1)^b \mathbf{v}''$ and $\mathbf{w}' = (-1)^b \mathbf{w}''$. Clearly, for any $\mathbf{v}''$ and $\mathbf{w}''$, the distribution of $\mathbf{v}' - \psi(\mathbf{w}') = (-1)^b(\mathbf{v}'' - \psi(\mathbf{w}''))$ is symmetric about the origin. So, $(\mathbf{v}', \mathbf{w}')$ satisfies the third property. We need to check that the first two properties are preserved. Since $[\mathbf{v}'']_{\mathbf{C}}$ is uniformly distributed, also $[-\mathbf{v}'']_{\mathbf{C}} = -[\mathbf{v}'']_{\mathbf{C}}$ is uniform. It follows that $[\mathbf{v}']_{\mathbf{C}}$ is uniformly distributed because $\mathbf{v}'$ is a convex combination of distributions $\mathbf{v}''$ and $-\mathbf{v}''$. Finally, since Voronoi cells of a lattice are symmetric,

$$\mathbf{v}' - \psi(\mathbf{w}') = (-1)^b(\mathbf{v}'' - \psi(\mathbf{w}'')) \in (-1)^b \bar{\mathcal{V}}(\mathbf{L}_n) = \bar{\mathcal{V}}(\mathbf{L}_n).$$

This proves that $(\mathbf{v}', \mathbf{w}')$ satisfies the first three properties.

In order to achieve also the fourth property, set $\mathbf{v} = (\mathbf{v}' - \psi(\mathbf{w}' - (\mathbf{w}' \bmod \mathbf{M}_n)))$ and $\mathbf{w} = (\mathbf{w}' \bmod \mathbf{M}_n)$. Clearly, $\mathbf{w} \in \mathcal{P}(\mathbf{M}_n)$, so, the fourth property is satisfied. We show that the first three properties are preserved. Notice that $\mathbf{v}' - \mathbf{v} \in \psi(\mathcal{L}(\mathbf{M}_n)) = \mathcal{L}(\mathbf{C})$ and $\mathbf{v} - \psi(\mathbf{w}) = \mathbf{v}' - \psi(\mathbf{w}')$. So, the first property is satisfied because $[\mathbf{v}]_{\mathbf{C}} = [\mathbf{v}']_{\mathbf{C}}$, and the other two are also satisfied because they only depend on $\mathbf{v} - \psi(\mathbf{w})$. □

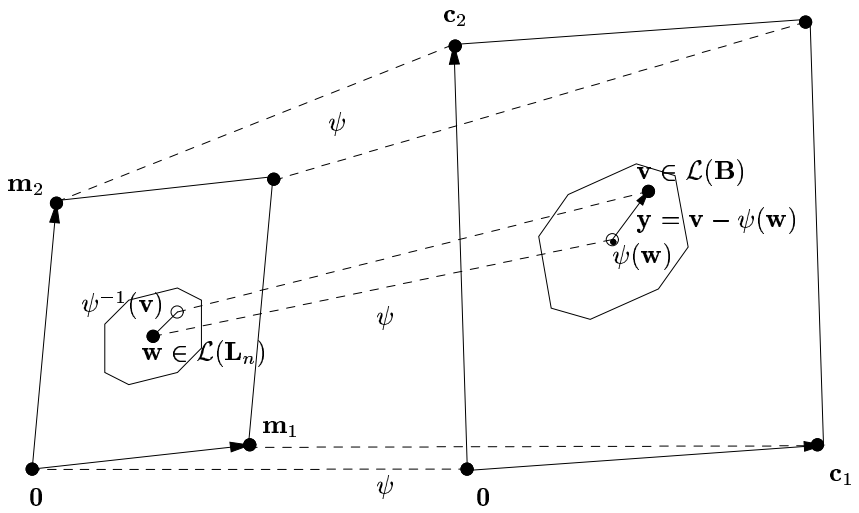


Figure 1: Sampling lattice points

The sampling procedure produces vectors $\mathbf{v} \in \mathcal{L}(\mathbf{B})$ such that $[\mathbf{v}]_{\mathbf{C}}$ is distributed uniformly at random over the group $\mathcal{L}(\mathbf{B})/\mathcal{L}(\mathbf{C})$. However, before the reduction modulo $\mathbf{C}$, vector $\mathbf{v}$ is not necessarily distributed uniformly over any set of lattice vectors. (This is due to lattice points $\mathbf{v} \in \mathcal{L}(\mathbf{B})$ such that $\psi^{-1}(\mathbf{v})$ lies on the boundary of Voronoi cells $\bar{\mathcal{V}}(\mathbf{w}, \mathbf{L}_n)$.) In the next lemma, we give simple upper and lower bounds on the probability of outputting each vector $\mathbf{v} \in \mathcal{L}(\mathbf{B})$.

**Lemma 11** *Let $(\mathbf{w}, \mathbf{v})$ be generated according to a sampling procedure of Lemma 10. Then, for any $\hat{\mathbf{v}} \in \mathcal{L}(\mathbf{B})$, $\Pr\{\mathbf{v} = \hat{\mathbf{v}}\} \leq |\det(\mathbf{B})/\det(\mathbf{C})|$. Moreover, if $\psi^{-1}(\hat{\mathbf{v}})$ belongs to the interior of a Voronoi cell $\mathcal{V}(\hat{\mathbf{w}}, \mathbf{L}_n)$ for some $\hat{\mathbf{w}} \in \mathcal{L}(\mathbf{L}_n) \cap \mathcal{P}(\mathbf{M}_n)$, then $\Pr\{\mathbf{v} = \hat{\mathbf{v}}\} = |\det(\mathbf{B})/\det(\mathbf{C})|$*

**Proof:** The upper bound is easy: for any $\hat{\mathbf{v}} \in \mathcal{L}(\mathbf{B})$,

$$\Pr\{\mathbf{v} = \hat{\mathbf{v}}\} \leq \Pr\{[\mathbf{v}]_{\mathbf{C}} = [\hat{\mathbf{v}}]_{\mathbf{C}}\} = |\det(\mathbf{B})/\det(\mathbf{C})|$$

because $[\mathbf{v}]_{\mathbf{C}}$ is uniformly distributed over a set $\mathcal{L}(\mathbf{B})/\mathcal{L}(\mathbf{C})$ of size $|\det(\mathbf{C})/\det(\mathbf{B})|$.

Now assume $\psi^{-1}(\hat{\mathbf{v}}) \in \mathcal{V}(\hat{\mathbf{w}}, \mathbf{L}_n)$ for some $\hat{\mathbf{w}} \in \mathcal{L}(\mathbf{L}_n) \cap \mathcal{P}(\mathbf{M}_n)$. We claim that if $[\mathbf{v}]_{\mathbf{C}} = [\hat{\mathbf{v}}]_{\mathbf{C}}$, then $\mathbf{v} = \hat{\mathbf{v}}$, and therefore

$$\Pr\{\mathbf{v} = \hat{\mathbf{v}}\} \geq \Pr\{[\mathbf{v}]_{\mathbf{C}} = [\hat{\mathbf{v}}]_{\mathbf{C}}\} = |\det(\mathbf{B})/\det(\mathbf{C})|.$$

Let $[\mathbf{v}]_{\mathbf{C}} = [\hat{\mathbf{v}}]_{\mathbf{C}}$, i.e., $\mathbf{v} - \hat{\mathbf{v}} \in \mathcal{L}(\mathbf{C})$. It follows that vector

$$\mathbf{y} = \psi^{-1}(\mathbf{v}) - \psi^{-1}(\hat{\mathbf{v}}) = \psi^{-1}(\mathbf{v} - \hat{\mathbf{v}})$$

belongs to lattice $\psi^{-1}(\mathcal{L}(\mathbf{C})) = \mathcal{L}(\mathbf{M}_n) \subseteq \mathcal{L}(\mathbf{L}_n)$. Since $\psi^{-1}(\hat{\mathbf{v}}) \in \mathcal{V}(\hat{\mathbf{w}}, \mathbf{L}_n)$ by assumption,

$$\psi^{-1}(\mathbf{v}) = \psi^{-1}(\hat{\mathbf{v}}) + \mathbf{y} \in \mathcal{V}(\hat{\mathbf{w}} + \mathbf{y}, \mathbf{L}_n),$$

i.e., $\psi^{-1}(\mathbf{v})$ is closer to $\hat{\mathbf{w}} + \mathbf{y}$ than to any other lattice point in $\mathcal{L}(\mathbf{L}_n)$. But we know from Lemma 10 that $\psi^{-1}(\mathbf{v})$ belongs to the Voronoi cell $\bar{\mathcal{V}}(\mathbf{w}, \mathbf{L}_n)$. Therefore, it must be $\mathbf{w} = \hat{\mathbf{w}} + \mathbf{y}$. We also know that both $\mathbf{w}$ and $\hat{\mathbf{w}}$ belong to $\mathcal{P}(\mathbf{M}_n)$, and $\mathbf{y} \in \mathcal{L}(\mathbf{M}_n)$. So, $\mathbf{w} = \hat{\mathbf{w}} + \mathbf{y}$ is possible only if $\mathbf{y} = \mathbf{0}$, which implies $\mathbf{v} = \hat{\mathbf{v}}$. □

Lemma 11 can be used to establish two important properties of the sampling algorithm of Lemma 10. The distribution $[\mathbf{v}]_{\mathbf{C}}$ produced by the sampling algorithm is uniform. However, $[\mathbf{w}]_{\mathbf{M}_n}$ is not in general uniformly distributed over $G_n$. The first property is that, provided $\|\mathbf{S}\|$ is large enough, distribution of $[\mathbf{w}]_{\mathbf{M}_n}$ is relatively close to uniform.

**Lemma 12** *Let $(\mathbf{w}, \mathbf{v})$ be generated according to the sampling procedure of Lemma 10. If $n\|\mathbf{S}\|\lambda_1(\mathbf{L}_n) \geq 6\alpha(n)\hat{\zeta}(\mathbf{B})$, then for any group element $g \in G_n$,*

$$\Pr\{[\mathbf{w}]_{\mathbf{M}_n} = g\} \approx \frac{1}{\#G_n}.$$

**Proof:** Fix group element $g$, and let $\mathbf{w}_g$ be the unique lattice point in $\mathcal{L}(\mathbf{L}_n) \cap \mathcal{P}(\mathbf{M}_n)$ such that $[\mathbf{w}_g]_{\mathbf{M}_n} = g$. Since $\mathbf{w} \in \mathcal{P}(\mathbf{M}_n)$, $[\mathbf{w}]_{\mathbf{M}_n} = g$ if and only if $\mathbf{w} = \mathbf{w}_g$. We estimate the probability that $\mathbf{w} = \mathbf{w}_g$.

Notice that if $\mathbf{v} \in \psi(\mathcal{V}(\mathbf{w}_g, \mathbf{L}_n))$, then $\mathbf{w} = \mathbf{w}_g$. Therefore,

$$\Pr\{\mathbf{w} = \mathbf{w}_g\} \geq \sum_{\mathbf{v}_g \in \psi(\mathcal{V}(\mathbf{w}_g, \mathbf{L}_n)) \cap \mathcal{L}(\mathbf{B})} \Pr\{\mathbf{v} = \mathbf{v}_g\}.$$

By Lemma 11, for any $\mathbf{v}_g \in \psi(\mathcal{V}(\mathbf{w}_g, \mathbf{L}_n)) \cap \mathcal{L}(\mathbf{B})$, $\Pr\{\mathbf{v} = \mathbf{v}_g\} = |\det(\mathbf{B})/\det(\mathbf{C})|$. So,

$$\Pr\{\mathbf{w} = \mathbf{w}_g\} \geq \frac{|\det(\mathbf{B})|}{|\det(\mathbf{C})|} \cdot \#(\psi(\mathcal{V}(\mathbf{w}_g, \mathbf{L}_n)) \cap \mathcal{L}(\mathbf{B})).$$

Similarly, if $\mathbf{w} = \mathbf{w}_g$, then $\mathbf{v} \in \psi(\bar{\mathcal{V}}(\mathbf{w}_g, \mathbf{L}_n))$. Therefore,

$$\Pr\{\mathbf{w} = \mathbf{w}_g\} \leq \sum_{\mathbf{v}_g \in \psi(\bar{\mathcal{V}}(\mathbf{w}_g, \mathbf{L}_n)) \cap \mathcal{L}(\mathbf{B})} \Pr\{\mathbf{v} = \mathbf{v}_g\} \leq \frac{|\det(\mathbf{B})|}{|\det(\mathbf{C})|} \cdot \#(\psi(\bar{\mathcal{V}}(\mathbf{w}_g, \mathbf{L}_n)) \cap \mathcal{L}(\mathbf{B})).$$

In order to complete the proof, we need to estimate the number of lattice points from $\mathcal{L}(\mathbf{B})$ that belong to $\psi(\mathcal{V}(\mathbf{w}_g, \mathbf{L}_n))$ and $\psi(\bar{\mathcal{V}}(\mathbf{w}_g, \mathbf{L}_n))$. Since $\mathcal{V}(\mathbf{w}_g, \mathbf{L}_n)$ contains an open sphere of radius $\lambda_1(\mathbf{L}_n)/2$, using (17) we get that $\psi(\mathcal{V}(\mathbf{w}_g, \mathbf{L}_n))$ (and therefore, also $\psi(\bar{\mathcal{V}}(\mathbf{w}_g, \mathbf{L}_n))$) contains a sphere of radius

$$\frac{n\|\mathbf{S}\|}{3\alpha(n)} \cdot \frac{\lambda_1(\mathbf{L}_n)}{2} \geq \hat{\zeta}(\mathbf{B}).$$

Therefore, by the definition of $\hat{\zeta}(\mathbf{B})$, the number of lattice points in $\psi(\mathcal{V}(\mathbf{w}_g, \mathbf{L}_n))$ (and $\psi(\bar{\mathcal{V}}(\mathbf{w}_g, \mathbf{L}_n))$) is approximately equal to

$$\frac{\mathrm{vol}(\psi(\mathcal{V}(\mathbf{w}_g, \mathbf{L}_n))}{|\det(\mathbf{B})|} = \frac{\mathrm{vol}(\psi(\bar{\mathcal{V}}(\mathbf{w}_g, \mathbf{L}_n))}{|\det(\mathbf{B})|}.$$

Combining this estimate with the upper and lower bounds on the probability that $\mathbf{w} = \mathbf{w}_g$, we get

$$\Pr\{[\mathbf{w}]_{\mathbf{M}_n} = g\} \approx \frac{|\det(\mathbf{B})|}{|\det(\mathbf{C})|} \cdot \frac{\mathrm{vol}(\psi(\mathcal{V}(\mathbf{w}_g, \mathbf{L}_n))}{|\det(\mathbf{B})|} = \frac{\mathrm{vol}(\psi(\mathcal{V}(\mathbf{w}_g, \mathbf{L}_n))}{|\det(\psi(\mathbf{M}_n)|} = \frac{\mathrm{vol}(\mathcal{V}(\mathbf{w}_g, \mathbf{L}_n))}{\det(\mathbf{M}_n)} = \frac{\det(\mathbf{L}_n)}{\det(\mathbf{M}_n)} = \frac{1}{\#G_n}.$$

□

If $\mathbf{v}$ and $\mathbf{w}$ are generated according to the sampling procedure of Lemma 10, then $\mathbf{v} - \psi(\mathbf{w})$ is distributed symmetrically about the origin. However, the same is not true if we consider the conditional probability of $\mathbf{v}$ given a fixed value of $\mathbf{w}$. The second property is that, provided $\|\mathbf{S}\|$ is large enough, then also this conditional distribution is roughly symmetric.

**Lemma 13** *Let $(\mathbf{w}, \mathbf{v})$ be generated according to the sampling procedure of Lemma 10. If $n\|\mathbf{S}\|\lambda_1(\mathbf{L}_n) \geq 12\alpha(n)\hat{\zeta}(\mathbf{B})$, then for any $\mathbf{h} \in \mathbb{R}^n \setminus \{\mathbf{0}\}$ and $g \in G_n$,*

$$\Pr\{\mathbf{h} \cdot (\mathbf{v} - \psi(\mathbf{w})) > 0 \mid [\mathbf{w}]_{\mathbf{M}_n} = g\} \geq \frac{1}{6}.$$

**Proof:** Fix group element $g$, and let $\mathbf{w}_g$ be the unique lattice point in $\mathcal{L}(\mathbf{L}_n) \cap \mathcal{P}(\mathbf{M}_n)$ such that $[\mathbf{w}_g]_{\mathbf{M}_n} = g$. Let $\mathcal{Q} = \{\mathbf{x} \in \mathcal{V}(\mathbf{w}_g, \mathbf{L}_n) : \mathbf{h} \cdot \psi(\mathbf{x} - \mathbf{w}_g) > 0\}$ be one of the two (open) halves of the Voronoi cell $\mathcal{V}(\mathbf{w}_g, \mathbf{L}_n)$

defined by the hyperplane orthogonal to $\mathbf{h}$ that passes through the center $\mathbf{w}_g$. (See Figure 2.) First we estimate the probability that $\mathbf{v} \in \psi(\mathcal{Q})$. Since $\mathcal{Q}$ is contained in $\mathcal{V}(\mathbf{w}_g, \mathbf{L}_n)$, by Lemma 11,

$$\Pr\{\mathbf{v} \in \psi(\mathcal{Q})\} = \sum_{\mathbf{v}_g \in \psi(\mathcal{Q}) \cap \mathcal{L}(\mathbf{B})} \Pr\{\mathbf{v} = \mathbf{v}_g\} = \frac{|\det(\mathbf{B})|}{|\det(\mathbf{C})|} \cdot \#(\psi(\mathcal{Q}) \cap \mathcal{L}(\mathbf{B})).$$

Notice that $\mathcal{Q}$ contains an open sphere of radius $\lambda_1(\mathbf{L}_n)/4$ centered in $\mathbf{w}_g - \mathbf{h} \cdot (\lambda_1(\mathbf{L}_n)/(4\|\mathbf{h}\|))$. (See figure 2.) Therefore, by (17), $\psi(\mathcal{Q})$ contains a sphere of radius

$$\frac{n\|\mathbf{S}\|}{3\alpha(n)} \cdot \frac{\lambda_1(\mathbf{L}_n)}{4} \geq \hat{\zeta}(\mathbf{B}).$$

By definition of $\hat{\zeta}(\mathbf{B})$, the number of lattice points in $\psi(\mathcal{Q})$ satisfies

$$\#(\psi(\mathcal{Q}) \cap \mathcal{L}(\mathbf{B})) \approx \frac{\mathrm{vol}(\psi(\mathcal{Q}))}{\det(\mathbf{B})} = \frac{1}{2}\frac{\mathrm{vol}(\psi(\mathcal{V}(\mathbf{w}_g, \mathbf{L}_n)))}{\det(\mathbf{B})}$$

and

$$\Pr\{\mathbf{v} \in \psi(\mathcal{Q})\} \approx \frac{1}{2}\frac{|\det(\mathbf{B})|}{|\det(\mathbf{C})|} \cdot \frac{\mathrm{vol}(\psi(\mathcal{V}(\mathbf{w}_g, \mathbf{L}_n)))}{\det(\mathbf{B})} = \frac{1}{2}\frac{\mathrm{vol}(\psi(\mathcal{V}(\mathbf{w}_g, \mathbf{L}_n)))}{\det(\psi(\mathbf{M}_n))} = \frac{1}{2}\frac{\mathrm{vol}(\mathcal{V}(\mathbf{w}_g, \mathbf{L}_n))}{\det(\mathbf{M}_n)} = \frac{1}{2 \cdot \#G_n}.$$

Notice that if $\mathbf{v} \in \psi(\mathcal{Q})$ then $\mathbf{w} = \mathbf{w}_g$ and $\mathbf{h} \cdot (\mathbf{v} - \psi(\mathbf{w}_g)) > 0$. Therefore,

$$\Pr\{[\mathbf{w}]_{\mathbf{M}_n} = g \wedge \mathbf{h} \cdot (\mathbf{v} - \psi(\mathbf{w}_g)) > 0\} \geq \Pr\{\mathbf{v} \in \psi(\mathcal{Q})\} \geq \frac{1}{4 \cdot \#G_n}.$$

We can now compute the conditional probability,

$$\begin{aligned} \Pr\{\mathbf{h} \cdot (\mathbf{v} - \psi(\mathbf{w})) > 0 \mid [\mathbf{w}]_{\mathbf{M}_n} = g\} &= \frac{\Pr\{\mathbf{h} \cdot (\mathbf{v} - \psi(\mathbf{w})) > 0 \wedge [\mathbf{w}]_{\mathbf{M}_n} = g\}}{\Pr\{[\mathbf{w}]_{\mathbf{M}_n} = g\}} \\ &\geq \frac{1}{4 \cdot \#G_n \cdot \Pr\{[\mathbf{w}]_{\mathbf{M}_n} = g\}}. \end{aligned}$$

Using Lemma 12, $\Pr\{[\mathbf{w}]_{\mathbf{M}_n} = g\} \lesssim 1/\#G_n$, i.e., $\#G_n \cdot \Pr\{[\mathbf{w}]_{\mathbf{M}_n} = g\} \leq 3/2$. Substituting in the previous inequality we get

$$\Pr\{\mathbf{h} \cdot (\mathbf{v} - \psi(\mathbf{w})) > 0 \mid [\mathbf{w}]_{\mathbf{M}_n} = g\} \geq \frac{1}{6}.$$

□

## 7.4 Some technical lemmas

In this Subsection we prove three technical lemmas that will be used to analyze the algorithm $\mathcal{A}^{\mathcal{F}}(\mathbf{B}, \mathbf{S})$ defined in Subsection 7.2. In all three lemmas, matrices $\mathbf{B}$ and $\mathbf{S}$ are the inputs to $\mathcal{A}^{\mathcal{F}}$, and $\mathbf{a}$ and $\mathbf{s}$ are the intermediate value and final output computed by $\mathcal{A}^{\mathcal{F}}$. The first lemma shows that the vector $\mathbf{z} = \mathcal{F}(\mathbf{a})$ computed during the execution of $\mathcal{A}^{\mathcal{F}}(\mathbf{B}, \mathbf{S})$ is short with high probability.

**Lemma 14** *If* $n\|\mathbf{S}\|\lambda_1(\mathbf{L}_n) \geq 6\alpha(n) \cdot \hat{\zeta}(\mathbf{B})$, *then*

$$\Pr\{\|\mathcal{F}(\mathbf{a})\| \leq \beta(n)\} = \delta(n) - \frac{1}{n^{\omega(1)}}.$$

**Proof:** We know that $\Pr\{\|\mathcal{F}(\mathbf{g})\| \leq \beta(n)\} = \delta(n)$ when $\mathbf{g} \in G_n^{m(n)}$ is chosen uniformly at random. By Corollary 1, in order to prove the proposition it is enough to evaluate the statistical distance between the distribution $\mathbf{a}$ generated by $\mathcal{A}^{\mathcal{F}}(\mathbf{B}, \mathbf{S})$ and a uniformly distributed $\mathbf{u}$, and show that $\Delta(\mathbf{a}, \mathbf{u}) = n^{-\omega(1)}$.

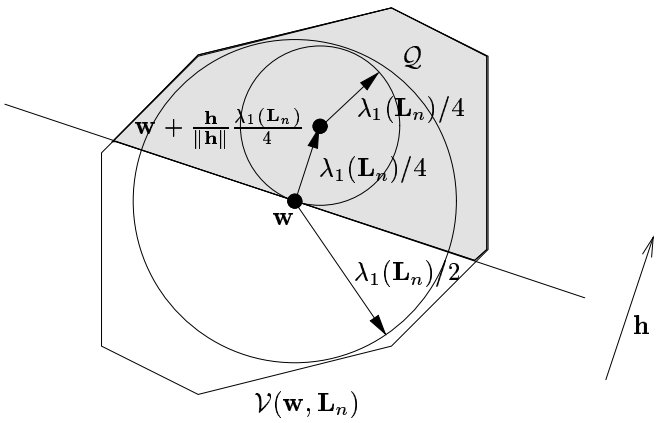


Figure 2: The conditional distribution of sampled lattice points

First consider the distribution of a single group element $a_{i,j} = [\mathbf{w}_{i,j}]_{\mathbf{M}_n}$ as output by the sampling procedure. We know from Lemma 12 that if $n\|\mathbf{S}\|\lambda_1(\mathbf{L}) \geq 6\alpha(n)\zeta(\mathbf{B})$ then for any group element $g \in G_n$,

$$\Pr\{a_{i,j} = g\} \approx \frac{1}{|G_n|}.$$

So, the probability distribution of each $a_{i,j}$ is not too far from uniform. Adding up a relatively small number of $a_{i,j}$ we get a group element $a_i = \sum_{j=1}^{k(n)} a_{i,j}$ which is almost uniformly distributed. In particular, by Proposition 9, the statistical distance between $a_i$ and a uniformly distributed $u_i \in G$ is at most

$$\Delta(a_i, u_i) \leq \frac{1}{2^{k(n)+1}}. \tag{19}$$

Since random variables $a_i$ are independent, by Proposition 6 the statistical distance between vector $\mathbf{a} = [a_1, \ldots, a_{m(n)}]^T$ and a uniformly distributed $\mathbf{u} \in G_n^{m(n)}$ is at most

$$\Delta(\mathbf{a}, \mathbf{u}) \leq \sum_{i=1}^{m(n)} \Delta(a_i, u_i) \leq \frac{m(n)}{2^{k(n)+1}} = \frac{n^{O(1)}}{n^{\omega(1)}} = n^{-\omega(1)}. \tag{20}$$

□

The next lemma shows that the probability that the output vector $\mathbf{s}$ belongs to any arbitrary $(n-1)$-dimensional hyperplane is never too high, even if conditioned on the value of the vector $\mathbf{a}$ given as input to $\mathcal{F}$.

**Lemma 15** *If $n\|\mathbf{S}\|\lambda_1(\mathbf{L}_n) \geq 12\alpha(n)\hat{\zeta}(\mathbf{B})$, then for any $\mathbf{g} \in G_n^{m(n)}$ and $(n-1)$-dimensional hyperplane $\mathcal{H}$,*

$$\Pr\{\mathbf{s} \notin \mathcal{H} \mid \mathbf{a} = \mathbf{g}\} \geq \frac{1}{6}.$$

**Proof:** We use Lemma 13 to prove that for any fixed $\mathbf{g}$, the conditional probability that $\mathbf{s} \notin \mathcal{H}$ given $\mathbf{a} = \mathbf{g}$ is at least $1/6$. Fix the values of $\mathbf{w}_{i,j} \in \mathcal{L}(\mathbf{L}_n)$ for all $i = 1, \ldots, m(n)$ and $j = 1, \ldots, k(n)$. Notice that this uniquely determines also the value of $a_{i,j} = (\mathbf{w}_{i,j} \bmod \mathbf{M}_n)$, $a_i = \sum_j a_{i,j}$ and $\mathbf{z} = \mathcal{F}(a_1, \ldots, a_n)$. Since $\mathbf{z} = \mathcal{F}(\mathbf{a}) \neq \mathbf{0}$, there exists a coordinate $i$ such that $z_i \neq 0$. Assume without loss of generality that $z_1 \neq 0$. Fix also the value of all vectors $\mathbf{y}_{i,j}$ for $(i,j) \neq (1,1)$ and let

$$\mathbf{y} = \sum_{(i,j)\neq(1,1)} z_i \cdot (\mathbf{v}_{i,j} - \psi(\mathbf{w}_{i,j})).$$

Notice that

$$\mathbf{s} = \sum_{i,j} z_i \cdot (\mathbf{v}_{i,j} - \psi(\mathbf{w}_{i,j})) = \mathbf{y} + z_1 \cdot (\mathbf{v}_{1,1} - \psi(\mathbf{w}_{1,1})).$$

We want to bound the probability that $\mathbf{s} \in \mathcal{H}$, or, equivalently,

$$\mathbf{v}_{1,1} - \psi(\mathbf{w}_{1,1}) \in (1/z_1)(\mathcal{H} - \mathbf{y}) = \mathcal{H}'.$$

Let $\mathbf{h}$ be a vector orthogonal to $\mathcal{H}'$ such that $\mathbf{h} \cdot \mathbf{x} \leq 0$ for any $\mathbf{x} \in \mathcal{H}'$. (Notice that since $\mathbf{h}$ is orthogonal to $\mathcal{H}'$, the value $\mathbf{h} \cdot \mathbf{x}$ does not depend on the specific point $\mathbf{x} \in \mathcal{H}'$ we choose.) By Lemma 13, the conditional probability that $\mathbf{h} \cdot (\mathbf{v}_{1,1} - \psi(\mathbf{w}_{1,1})) > 0$ given $\mathbf{w}_{1,1}$ is at least $1/6$. But if $\mathbf{h} \cdot (\mathbf{v}_{1,1} - \psi(\mathbf{w}_{1,1})) > 0$, then $\mathbf{v}_{1,1} - \psi(\mathbf{w}_{1,1}) \notin \mathcal{H}'$ because $\mathbf{h} \cdot x \leq 0$ for all $\mathbf{x} \in \mathcal{H}'$. □

The last lemma is the most complicated, and its proof will take the rest of this subsection.

**Lemma 16** *If $\alpha(n) = \omega(n\sqrt{k(n)}\beta(n)\rho(\mathbf{L}_n))$, then*

$$\Pr\{\|\mathcal{F}(\mathbf{a})\| \leq \beta(n) \wedge 2\|s\| > \|\mathbf{S}\|\} = o(\delta(n)).$$

**Proof:** Let $\varphi$ be the characteristic function of the set of all $\mathbf{g} \in G_n^{m(n)}$ such that $\|\mathcal{F}(\mathbf{g})\| \leq \beta(n)$:

$$\varphi(\mathbf{g}) = \begin{cases} 1 & \text{if } \|\mathcal{F}(\mathbf{g})\| \leq \beta(n) \\ 0 & \text{otherwise} \end{cases}. \tag{21}$$

We want to prove that the probability that $\varphi(\mathbf{a}) = 1$ and $2\|\mathbf{s}\| > \|\mathbf{S}\|$ is $o(\delta(n))$. Since $\varphi(\mathbf{a}) \in \{0, 1\}$ and $\|\mathbf{S}\| > 0$, events $\varphi(\mathbf{a}) = 1$ and $\|\mathbf{s}\| > \|\mathbf{S}\|/2$ are simultaneously satisfied if and only if $4\varphi(\mathbf{a})\|\mathbf{s}\|^2 > \|\mathbf{S}\|^2$. By Markov inequality, we immediately get

$$\begin{aligned} \Pr\{\|\mathcal{F}(\mathbf{a})\| \leq \beta(n) \wedge \|\mathbf{s}\| > \|\mathbf{S}\|/2\} &= \Pr\{4\varphi(\mathbf{a})\|\mathbf{s}\|^2 > \|\mathbf{S}\|^2\} \\ &\leq \frac{4\,\mathrm{Exp}[\varphi(\mathbf{a})\|\mathbf{s}\|^2]}{\|\mathbf{S}\|^2}. \end{aligned}$$

So, we need to show that the expectation $\mathrm{Exp}[\varphi(\mathbf{a})\|\mathbf{s}\|^2]$ is $o(\delta(n)\|\mathbf{S}\|^2)$. In order to bound the expectation $\mathrm{Exp}[\varphi(\mathbf{a})\|\mathbf{s}\|^2]$ we introduce some notation. For any $i, j \in \{1, \ldots, m(n)\}$, let $\varphi_{i,j}: G_n^{m(n)} \to \mathbb{Z}$ and $f_{i,j}: \mathbb{R}^n \times \mathbb{R}^n \times G_n \to \mathbb{R}$ be the functions

$$\begin{aligned} \varphi_{i,j}(\mathbf{g}) &= w_i w_j \varphi(\mathbf{g}) \qquad \text{where } \mathbf{w} = \mathcal{F}(\mathbf{g}) \\ f_{i,j}(\mathbf{v}_1, \mathbf{v}_2, \mathbf{g}) &= \langle \mathbf{v}_1, \mathbf{v}_2 \rangle \cdot \varphi_{i,j}(\mathbf{g}). \end{aligned}$$

For any $\mathbf{g} \in G_n^{m(n)}$, let $\Gamma(\mathbf{g})$ be the real random variable

$$\Gamma(\mathbf{g}) = \sum_{i,j=1}^{m(n)} \sum_{h,l=1}^{k(n)} f_{i,j}(\mathbf{y}_{i,l}, \mathbf{y}_{j,h}, \mathbf{g}). \tag{22}$$

defined by the random choice of vectors $\mathbf{y}_{i,l}, \mathbf{y}_{j,h}$ produced during the execution of $\mathcal{A}^{\mathcal{F}}(\mathbf{B}, \mathbf{S})$. These definitions are justified by the following lemma.

**Lemma 17** *If $\mathbf{a}$ and $\mathbf{s}$ are the vectors produced by $\mathcal{A}^{\mathcal{F}}$, then*

$$\Gamma(\mathbf{a}) = \|\mathbf{s}\|^2 \varphi(\mathbf{a}).$$

**Proof:** Functions $\varphi_{i,j}$ satisfy $\varphi_{i,j}(\mathbf{a}) = z_i z_j \varphi(\mathbf{a})$, where $\mathbf{z} = \mathcal{F}(\mathbf{a})$ is the output of $\mathcal{F}$ generated during the execution of $\mathcal{A}^{\mathcal{F}}(\mathbf{B}, \mathbf{S})$. Using the definition of $\mathbf{s}$ we get

$$\Gamma(\mathbf{a}) = \sum_{i,j=1}^{m(n)} \sum_{h,l=1}^{k(n)} \langle \mathbf{y}_{i,l}, \mathbf{y}_{j,h} \rangle \varphi_{i,j}(\mathbf{a})$$

$$
\begin{aligned}
&= \sum_{i,j} \left\langle \sum_l \mathbf{y}_{i,l}, \sum_h \mathbf{y}_{j,h} \right\rangle z_i z_j \varphi(\mathbf{a}) \\
&= \left\langle \sum_{i,l} z_i \mathbf{y}_{i,l}, \sum_{j,h} z_j \mathbf{y}_{j,h} \right\rangle \varphi(\mathbf{a}) \\
&= \|\mathbf{s}\|^2 \varphi(\mathbf{a}).
\end{aligned}
$$

□

Using this notation, our problem can be reformulated as computing the expectation of $\Gamma(\mathbf{a})$, where $\mathbf{a} \in G_n^{m(n)}$ is the vector produced by our sampling algorithm. Let $\mathbf{u} \in G_n^{m(n)}$ be a uniformly distributed vector. By triangle inequality,

$$\mathrm{Exp}[\Gamma(\mathbf{a})] \leq \mathrm{Exp}[\Gamma(\mathbf{u})] + |\mathrm{Exp}[\Gamma(\mathbf{a}) - \Gamma(\mathbf{u})]|.$$

We prove that both $\mathrm{Exp}[\Gamma(\mathbf{u})]$ and $|\mathrm{Exp}[\Gamma(\mathbf{a}) - \Gamma(\mathbf{u})]|$ are at most $o(\delta(n) \cdot \|\mathbf{S}\|^2)$. First, we prove a simple bound on the length of vectors $\mathbf{y}_{i,j}$. Notice that since $\psi^{-1}(\mathbf{v}_{i,j}) \in \bar{\mathcal{V}}(\mathbf{w}_{i,j}, \mathbf{L}_n)$, $\|\psi^{-1}(\mathbf{v}_{i,j}) - \mathbf{w}_{i,j}\| \leq \rho(\mathbf{L}_n)$, and, by (17), $\mathbf{y}_{i,j} = \psi(\psi^{-1}(\mathbf{v}_{i,j}) - \mathbf{w}_{i,j})$ has length at most

$$\|\mathbf{y}_{i,j}\| \leq \frac{3n\|\mathbf{S}\| \cdot \rho(\mathbf{L}_n)}{\alpha(n)}. \tag{23}$$

The following lemma bounds $\mathrm{Exp}[\Gamma(\mathbf{u})]$.

**Lemma 18** *Let $\mathbf{u} \in G^m$ be an independent and uniformly distributed random variable. If $\alpha(n)$ satisfies the hypothesis of Lemma 16, then*

$$\mathit{Exp}[\Gamma(\mathbf{u})] \leq o(\delta(n)) \cdot \|\mathbf{S}\|^2.$$

**Proof:** The key observation is that vector $\mathbf{u}$ is statistically independent from $\mathbf{y}_{i,j}, \mathbf{y}_{h,l}$. Therefore,

$$
\begin{aligned}
\mathrm{Exp}[\Gamma(\mathbf{u})] &= \sum_{i,j} \sum_{h,l} \mathrm{Exp}[\langle \mathbf{y}_{i,l}, \mathbf{y}_{j,h} \rangle \varphi_{i,j}(\mathbf{u})] \\
&= \sum_{i,j} \sum_{h,l} \mathrm{Exp}[\langle \mathbf{y}_{i,l}, \mathbf{y}_{j,h} \rangle] \cdot \mathrm{Exp}[\varphi_{i,j}(\mathbf{u})].
\end{aligned}
$$

For all $(i,l) \neq (j,h)$, random variables $\mathbf{y}_{i,l}$ and $\mathbf{y}_{j,h}$ are independent because they are generated in different runs of the sampling algorithm. It follows that

$$\mathrm{Exp}[\langle \mathbf{y}_{i,l}, \mathbf{y}_{j,h} \rangle] = \langle \mathrm{Exp}[\mathbf{y}_{i,l}], \mathrm{Exp}[\mathbf{y}_{j,h}] \rangle = 0 \tag{24}$$

because $\mathrm{Exp}[\mathbf{y}_{i,l}] = \mathrm{Exp}[\mathbf{y}_{j,h}] = 0$. On the other hand, if $(i,j) = (j,h)$ then

$$\langle \mathbf{y}_{i,l}, \mathbf{y}_{j,h} \rangle = \|\mathbf{y}_{i,l}\|^2$$

and $\varphi_{i,j}(\mathbf{u}) = \varphi_{i,i}(\mathbf{u}) \geq 0$. Substituting in the previous equation, and using (23) we get

$$
\begin{aligned}
\mathrm{Exp}[\Gamma(\mathbf{u})] &= \sum_{i=1}^{m(n)} \sum_{l=1}^{k(n)} \mathrm{Exp}[\|\mathbf{y}_{i,l}\|^2] \cdot \mathrm{Exp}[\varphi_{i,i}(\mathbf{u})] \\
&\leq \sum_{i,l} \left( \frac{3n\|\mathbf{S}\| \cdot \rho(\mathbf{L}_n)}{\alpha(n)} \right)^2 \cdot \mathrm{Exp}[\varphi_{i,i}(\mathbf{u})] \\
&= \left( \frac{4\sqrt{k(n)}n\|\mathbf{S}\| \cdot \rho(\mathbf{L}_n)}{\alpha(n)} \right)^2 \cdot \mathrm{Exp}[\sum_i \varphi_{i,i}(\mathbf{u})].
\end{aligned}
$$

Finally, we observe that for any $\mathbf{g} \in G_n^{m(n)}$,

$$\sum_{i=1}^{m(n)} \varphi_{i,i}(\mathbf{g}) = \|\mathcal{F}(\mathbf{g})\|^2 \varphi(\mathbf{g}) \leq \beta(n)^2 \cdot \varphi(\mathbf{g})$$

because $\varphi(\mathbf{g}) = 0$ whenever $\|\mathcal{F}(\mathbf{g})\| > \beta(n)$. Combining the last two equations we obtain

$$\mathrm{Exp}[\Gamma(\mathbf{u})] \leq \left(\frac{3\sqrt{k(n)}n\|\mathbf{S}\|\rho(\mathbf{L}_n)}{\alpha(n)}\right)^2 \cdot \beta(n)^2 \,\mathrm{Exp}[\varphi(\mathbf{u})] = \left(\frac{3\sqrt{k(n)}n\rho(\mathbf{L}_n)\beta(n)}{\alpha(n)}\right)^2 \cdot \|\mathbf{S}\|^2\delta(n).$$

Using $\alpha(n) = \omega(n\sqrt{k(n)}\rho(\mathbf{L}_n)\beta(n))$, we get $\mathrm{Exp}[\Gamma(\mathbf{u})] \leq o(\delta(n)) \cdot \|\mathbf{S}\|^2$. $\square$

Now consider the expectation of the difference $\mathrm{Exp}[\Gamma(\mathbf{a}) - \Gamma(\mathbf{u})]$. Notice that random variables $\Gamma(\mathbf{a})$ and $\Gamma(\mathbf{u})$ depend not only on $\mathbf{a}$ and $\mathbf{u}$, but also on the random choice of vectors $\mathbf{y}_{i,j}$. In particular, the fact that distributions $\mathbf{a}$ and $\mathbf{u}$ are statistically close does not necessarily imply that $\mathrm{Exp}[\Gamma(\mathbf{a}) - \Gamma(\mathbf{u})]$ is small, because the statistical distance between the complete distributions underlying $\Gamma(\mathbf{a})$ and $\Gamma(\mathbf{u})$ (namely $(\mathbf{y}_{1,1}, \ldots, \mathbf{y}_{m,k}, \mathbf{a})$ and $(\mathbf{y}_{1,1}, \ldots, \mathbf{y}_{m,k}, \mathbf{u})$) can be quite large. In order to bound the expectation of $\Gamma(\mathbf{a}) - \Gamma(\mathbf{u})$, we first break this expression into smaller components as follows.

$$\begin{aligned} |\mathrm{Exp}[\Gamma(\mathbf{a}) - \Gamma(\mathbf{u})]| &= \left|\sum_{i,j=1}^{m(n)} \sum_{h,l=1}^{k(n)} \mathrm{Exp}[f_{i,j}(\mathbf{y}_{i,l}, \mathbf{y}_{j,h}, \mathbf{a}) - f_{i,j}(\mathbf{y}_{i,l}, \mathbf{y}_{j,h}, \mathbf{u})]\right| \\ &\leq \sum_{i,j,h,l} |\mathrm{Exp}[f_{i,j}(\mathbf{y}_{i,l}, \mathbf{y}_{j,h}, \mathbf{a}) - f_{i,j}(\mathbf{y}_{i,l}, \mathbf{y}_{j,h}, \mathbf{u})]| \,. \end{aligned}$$

We bound each term separately and show that for any $i, j \in \{1, \ldots, m(n)\}$ and $l, h \in \{1, \ldots, k(n)\}$,

$$|\mathrm{Exp}[f_{i,j}(\mathbf{y}_{i,l}, \mathbf{y}_{j,h}, \mathbf{a}) - f_{i,j}(\mathbf{y}_{i,l}, \mathbf{y}_{j,h}, \mathbf{u})]| = n^{-\omega(1)} \cdot \|\mathbf{S}\|^2. \tag{25}$$

It follows that

$$|\,\mathrm{Exp}[\Gamma(\mathbf{a}) - \Gamma(\mathbf{u})]| \leq (m(n) \cdot k(n))^2 \cdot n^{-\omega(1)} \cdot \|\mathbf{S}\|^2 = n^{-\omega(1)} \cdot \|\mathbf{S}\|^2.$$

For any fixed value of $i, j, h, l$, define distributions

$$D_a^{i,j,l,h} = (\mathbf{y}_{i,l}, \mathbf{y}_{j,h}, \mathbf{a}) \tag{26}$$

$$D_u^{i,j,l,h} = (\mathbf{y}_{i,l}, \mathbf{y}_{j,h}, \mathbf{u}). \tag{27}$$

The next lemma shows that distributions $D_a^{i,j,l,h}$ and $D_u^{i,j,l,h}$ are statistically close.

**Lemma 19** *For any $i, j, h, l$, the statistical distance between distributions $D_a^{i,j,l,h}$ and $D_u^{i,j,l,h}$ defined in (26, 27) is at most*

$$\Delta(D_a^{i,j,l,h}, D_u^{i,j,l,h}) \leq \frac{m(n)}{2^{k(n)-1}} = n^{-\omega(n)}.$$

**Proof:**. In order to bound the statistical distance between $D_a^{i,j,l,h}$ and $D_u^{i,j,l,h}$, we define auxiliary distributions

$$\begin{aligned} \hat{D}_a^{i,j,l,h} &= (\mathbf{y}_{i,l}, \mathbf{y}_{j,h}, a_{i,l}, a_{j,h}, \hat{\mathbf{a}}) \\ \hat{D}_u^{i,j,l,h} &= (\mathbf{y}_{i,l}, \mathbf{y}_{j,h}, a_{i,l}, a_{j,h}, \hat{\mathbf{u}}) \end{aligned}$$

where

$$\hat{\mathbf{a}} = \sum_{(\hat{i},\hat{l}) \notin \{(i,l),(j,h)\}} a_{\hat{i},\hat{l}} \mathbf{e}_{\hat{i}} = \begin{cases} \mathbf{a} - a_{i,l}\mathbf{e}_i & \text{if } (i,l) = (j,h) \\ \mathbf{a} - a_{i,l}\mathbf{e}_i - a_{j,h}\mathbf{e}_j & \text{otherwise} \end{cases}$$

and

$$\hat{\mathbf{u}} = \mathbf{u} - \mathbf{a} + \hat{\mathbf{a}}.$$

Notice that $D_a^{i,j,l,h} = f_{i,j,l,h}(\hat{D}_a^{i,j,l,h})$ and $D_u^{i,j,l,h} = f_{i,j,l,h}(\hat{D}_u^{i,j,l,h})$ where $f_{i,j,l,h}$ is the function

$$f_{i,j,l,h}(\mathbf{y},\mathbf{y}',a,a',\mathbf{g}) = \begin{cases} (\mathbf{y},\mathbf{y}',\mathbf{g}+a\mathbf{e}_i) & \text{if } (i,l)=(j,h) \\ (\mathbf{y},\mathbf{y}',\mathbf{g}+a\mathbf{e}_i+a'\mathbf{e}_j) & \text{otherwise} \end{cases}$$

It follows, by Proposition 7, that

$$\Delta(D_a^{i,j,l,h}, D_u^{i,j,l,h}) = \Delta(f_{i,j,l,h}(\hat{D}_a^{i,j,l,h}), f_{i,j,l,h}(\hat{D}_u^{i,j,l,h})) \leq \Delta(\hat{D}_a^{i,j,l,h}, \hat{D}_u^{i,j,l,h}). \tag{28}$$

Notice that $\hat{\mathbf{a}} = \sum_{(\hat{i},\hat{l})\neq(i,l),(j,h)} a_{\hat{i},\hat{l}}\mathbf{e}_{\hat{i}}$ and $\hat{\mathbf{u}}$ are statistically independent from $(\mathbf{y}_{i,l}, \mathbf{y}_{j,h}, a_{i,l}, a_{j,h})$. Therefore, by Proposition 5,

$$\begin{aligned} \Delta(\hat{D}_a^{i,j,l,h}, \hat{D}_u^{i,j,l,h}) &= \Delta((\mathbf{y}_{i,l},\mathbf{y}_{j,h},a_{i,l},a_{j,h},\hat{\mathbf{a}}),(\mathbf{y}_{i,l},\mathbf{y}_{j,h},a_{i,l},a_{j,h},\hat{\mathbf{u}})) \\ &= \Delta(\hat{\mathbf{a}},\hat{\mathbf{u}}). \end{aligned}$$

The components of $\hat{\mathbf{a}}$ and $\hat{\mathbf{u}}$ are totally independent. Therefore, by Proposition 6,

$$\Delta(\hat{\mathbf{a}},\hat{\mathbf{u}}) = \sum_{t=1}^{m(n)} \Delta(\hat{a}_t, \hat{u}_t).$$

Finally, notice that each $\hat{u}_t$ is uniformly distributed over $G_n$, while each $\hat{a}_t$ is the sum of at least $k-2$ independent random variables, each satisfying the hypothesis of Proposition 9. So, the statistical distance (28) is at most

$$\frac{m(n)}{2^{k(n)-1}} = n^{-\omega(1)}.$$

□

We use Lemma 19 to bound $|\operatorname{Exp}[f_{i,j}(D_a^{i,j,l,h}) - f_{i,j}(D_u^{i,j,l,h})]|$. Notice that for any $\mathbf{g} \in G^m$,

$$|f_{i,j}(\mathbf{y}_{i,l},\mathbf{y}_{j,h},\mathbf{g})| \leq \|\mathbf{y}_{i,l}\| \cdot \|\mathbf{y}_{j,h}\| \cdot |\varphi_{i,j}(\mathbf{g})| \leq \left(\frac{4n\|\mathbf{S}\|\rho(\mathbf{L}_n)\beta(n)}{\alpha(n)}\right)^2 = \frac{\|\mathbf{S}\|^2}{\omega(k(n))}.$$

Therefore, by Proposition 8

$$|\operatorname{Exp}[f_{i,j}(D_a^{i,j,l,h}) - f_{i,j}(D_u^{i,j,l,h})]| = |\operatorname{Exp}[f_{i,j}(D_a^{i,j,l,h})] - \operatorname{Exp}[f_{i,j}(D_u^{i,j,l,h})]| \leq \frac{\|\mathbf{S}\|^2}{\omega(k(n))} \cdot \Delta(D_a^{i,j,l,h}, D_u^{i,j,l,h}). = \frac{\|\mathbf{S}\|^2}{n^{\omega(1)}}.$$

This proves (25) and completes the proof of the Lemma 16. □

## 7.5 Analysis of the reduction

In this subsection we prove Lemma 7. We first prove the lemma under the simplifying assumption that procedure $\mathcal{F}$ is deterministic and it always outputs a nonzero lattice vector.

**Lemma 20** *Let $\{\mathbf{L}_n\}$ a family of easily decodable $\tau(n)$-perfect lattices, $\gamma(n) = \beta(n)\tau(n) \cdot \omega(\sqrt{\log n})$ and $\alpha(n) = n\lambda_1(\mathbf{L}_n)\gamma(n)/12$. Assume there exists a deterministic polynomial time procedure $\mathcal{F}$ that on input a vector $\mathbf{g} \in G_n^{m(n)}$, produces a nonzero lattice vector $\mathcal{F}(\mathbf{g}) \in \Lambda(\mathbf{g}) \setminus \{\mathbf{0}\}$ such that $\|\mathcal{F}(\mathbf{g})\| \leq \beta(n)$ for a non-negligible fraction $\delta(n) = 1/n^{O(1)}$ of the inputs. Then, there exists a probabilistic polynomial time algorithm $\mathcal{A}^{\mathcal{F}}(\cdot,\cdot)$ that on input any $n$-dimensional lattice basis $\mathbf{B}$ and a set of linearly independent lattice vectors $\mathbf{S} \subset \mathcal{L}(\mathbf{B})$ such that $\|\mathbf{S}\| > \gamma(n) \cdot \hat{\zeta}(\mathbf{B})$, outputs a lattice vector $\mathbf{s} = \mathcal{A}^{\mathcal{F}}(\mathbf{B},\mathbf{S}) \in \mathcal{L}(\mathbf{B})$ such that*

$$\Pr\{\mathbf{s} \notin \mathit{span}\{\mathbf{s}_i \mid 2\|\mathbf{s}_i\| < \|\mathbf{s}\|\} = \Omega(\delta(n)).$$

**Proof:** Let $\mathcal{A}$ be the algorithm described in Subsection 7.2 with

$$k(n) = \frac{\gamma(n) \cdot \sqrt{\log n}}{\beta(n) \cdot \tau(n)} = \omega(\log n).$$

Notice that

$$\alpha(n) = \frac{n\lambda_1(\mathbf{L}_n)}{12} \frac{k(n)\beta(n)\tau(n)}{\sqrt{\log n}} \geq \frac{\beta(n)\rho(\mathbf{L}_n)n}{6} \frac{k(n)}{o(\sqrt{k(n)})} = \omega(n\sqrt{k(n)}\beta(n)\rho(\mathbf{L}_n)),$$

so, (11) and the hypothesis of Lemma 16 are satisfied. From the definition of $\alpha(n)$ and the assumption that $\|\mathbf{S}\| > \gamma(n)\hat{\zeta}(\mathbf{B})$, we get

$$12\alpha(n)\hat{\zeta}(\mathbf{B}) = n\lambda_1(\mathbf{L}_n)\gamma(n)\hat{\zeta}(\mathbf{B}) < n\lambda_1(\mathbf{L}_n)\|\mathbf{S}\|.$$

So, also the hypotheses of Lemmas 14 and 15 are satisfied.

We already proved in Lemma 9 that $\mathbf{s} \in \mathcal{L}(\mathbf{B})$. We use Lemmas 14, 15 and 16 to prove that

$$\Pr\{\mathbf{s} \notin \text{span}\{\mathbf{s}_i : \|\mathbf{s}_i\| < 2\|\mathbf{s}\|\}\} = \Omega(\delta(n)).$$

Let $\mathbf{s}_j$ be any vector of length $\|\mathbf{s}_j\| = \|\mathbf{S}\|$, and consider the hyperplane $\mathcal{H} = \text{span}\{\mathbf{s}_i : i \neq j\}$. Notice that if $\|\mathbf{S}\| \geq 2\|\mathbf{s}\|$ then $\text{span}\{\mathbf{s}_i : \|\mathbf{s}_i\| < 2\|\mathbf{s}\|\} \subseteq \mathcal{H}$. Therefore if $\|\mathbf{S}\| \geq 2\|\mathbf{s}\|$ and $\mathbf{s} \notin \mathcal{H}$, then $\mathbf{s} \notin \text{span}\{\mathbf{s}_i : \|\mathbf{s}_i\| < 2\|\mathbf{s}\|\}$, and

$$\Pr\{\mathbf{s} \notin \text{span}\{\mathbf{s}_i : \|\mathbf{s}_i\| < 2\|\mathbf{s}\|\}\} \geq \Pr\{\mathbf{s} \notin \mathcal{H} \wedge 2\|\mathbf{s}\| \leq \|\mathbf{S}\|\}.$$

We know from Lemmas 14, 15 and 16 that $\Pr\{\|\mathcal{F}(\mathbf{a})\| \leq \beta(n)\} = \delta(n) - n^{-\omega(1)}$, $\Pr\{\mathbf{s} \notin \mathcal{H} \mid \mathbf{a} = \mathbf{g}\} \geq 1/6$ and $\Pr\{\|\mathcal{F}(\mathbf{a})\| \leq \beta(n) \wedge 2\|\mathbf{s}\| > \|\mathbf{S}\|\} = o(\delta(n))$. Therefore the probability that $\Pr\{\mathbf{s} \notin \text{span}\{\mathbf{s}_i : \|\mathbf{s}_i\| < 2\|\mathbf{s}\|\}$ is at least

$$\begin{aligned}
&\Pr\{\mathbf{s} \notin \mathcal{H} \wedge 2\|\mathbf{s}\| \leq \|\mathbf{S}\|\} \geq \\
&\quad \geq \Pr\{\mathbf{s} \notin \mathcal{H} \wedge 2\|\mathbf{s}\| \leq \|\mathbf{S}\| \wedge \|\mathcal{F}(\mathbf{a})\| \leq \beta(n)\} \\
&\quad \geq \Pr\{\|\mathcal{F}(\mathbf{a})\| \leq \beta(n) \wedge \mathbf{s} \notin \mathcal{H}\} - \Pr\{\|\mathcal{F}(\mathbf{a})\| \leq \beta(n) \wedge 2\|\mathbf{s}\| > \|\mathbf{S}\|\} \\
&\quad = \sum_{\mathbf{g}:\|\mathcal{F}(\mathbf{g})\| \leq \beta(n)} \Pr\{\mathbf{a} = \mathbf{g}\} \cdot \Pr\{\mathbf{s} \notin \mathcal{H} \mid \mathbf{a} = \mathbf{g}\} - \Pr\{\|\mathcal{F}(\mathbf{a})\| \leq \beta(n) \wedge 2\|\mathbf{s}\| > \|\mathbf{S}\|\} \\
&\quad \geq \Pr\{\|\mathcal{F}(\mathbf{a})\| \leq \beta(n)\} \cdot \frac{1}{6} - o(\delta(n)) \\
&\quad \geq (\delta(n) - n^{-\omega(1)}) \cdot \frac{1}{6} - o(\delta(n)) = \Omega(\delta(n)).
\end{aligned}$$

□

We combine Lemma 8 with Lemma 20 to get a proof of Lemma 7.

**Proof:** Let $\mathcal{F}$ a probabilistic polynomial time procedure such that if $\mathbf{g} \in G_n^{m(n)}$ is chosen uniformly at random, then $\mathcal{F}(\mathbf{g}) \in \Lambda(\mathbf{g}) \setminus \{\mathbf{0}\}$ and $\|\mathcal{F}(\mathbf{g})\| \leq \beta(n)$. On input $(\mathbf{B}, \mathbf{S})$, algorithm $\mathcal{A}^{\mathcal{F}}(\mathbf{B}, \mathbf{S})$ first transforms $\mathcal{F}$ into a deterministic procedure $\mathcal{F}'$ using Lemma 8. We know that $\mathcal{F}'(\mathbf{g}) \in \Lambda(\mathbf{g}) \setminus \{\mathbf{0}\}$ for all $\mathbf{g} \in G_n^{m(n)}$. Moreover, with probability at least $1 - 2/e$ (probability over the randomness of the transformation from $\mathcal{F}$ to $\mathcal{F}'$), $\|\mathcal{F}'(\mathbf{g})\| \leq \beta(n)$ for at least a non-negligible fraction $\delta(n)/4$ of the inputs $\mathbf{g} \in G_n^{m(n)}$. Finally, $\mathcal{A}$ applies Lemma 20 to $\mathcal{F}'$ to get an algorithm $\mathcal{A}'$, computes lattice vector $\mathbf{s} = \mathcal{A}'(\mathbf{B}, \mathbf{S}) \in \mathcal{L}(\mathbf{B})$ and outputs $\mathbf{s}$.

If $\|\mathcal{F}'(\mathbf{g})\| \leq \beta(n)$ for a non-negligible fraction $\delta(n)/4$ of the inputs, then the conditional probability that $\mathbf{s} \notin \{\mathbf{s}_i \mid 2\|\mathbf{s}_i\| < \|\mathbf{s}\|\}$ (given $\Pr_{\mathbf{g}}\{\|\mathcal{F}'(\mathbf{g})\| \leq \beta(n)\} \geq \delta(n)/4$) is $\Omega(\delta(n)/4) = \Omega(\delta(n))$. Since $\Pr_{\mathbf{g}}\{\|\mathcal{F}'(\mathbf{g})\| \leq \beta(n)\} \geq \delta(n)/4$ with probability (over the randomness in the construction of $\mathcal{F}'$ from $\mathcal{F}$) at least $1 - 2/e$, the overall probability that $\mathbf{s} \notin \{\mathbf{s}_i \mid 2\|\mathbf{s}_i\| < \|\mathbf{s}\|\}$ is at least $(1 - 2/e) \cdot \Omega(\delta(n)) = \Omega(\delta(n))$. □

# 8 Applications

In this section we show how Theorem 5 immediately implies strong connections between the average case and worst case complexity of various lattice approximation problems. We also show how to build provably secure cryptographic (collision resistant) hash functions based on worst-case complexity assumptions.

**Corollary 2** *Let $\tau(n) \leq \sqrt{n}$ be a function such that there exists a family of $\tau(n)$-perfect easily decodable lattices. For every polynomially bounded functions $\mu(m) = m^{O(1)}$, $m(n) = \Theta(n \log n)$, and superlogarithmic function $\omega(\log n)$, there exists a sequence of groups $\{G_n\}$ such that the following is true. If there is a probabilistic polynomial time algorithm that on input a uniformly random $\mathbf{g} \in G_n^{m(n)}$, outputs with non-negligible probability a nonzero lattice vector $\mathbf{s} \in \Lambda(\mathbf{g}) \setminus \{\mathbf{0}\}$ within a factor $\mu(m(n))$ from Minkowski's bound*

$$\|\mathbf{s}\| \leq \mu(m(n)) \cdot \sqrt{m(n)} \cdot \det(\Lambda(\mathbf{g}))^{1/m(n)},$$

*then there is a probabilistic polynomial time algorithm that on input any $n$-dimensional lattice $\mathbf{B}$ solves, with probability exponentially close to 1, any of the following problems*

1. [SIVP] *Find a set $\mathbf{S} \subseteq \mathcal{L}(\mathbf{B})$ of $n$ linearly independent vectors such that*

$$\|\mathbf{S}\| \leq \mu(m(n)) \cdot n^2 \cdot \tau(n) \cdot \omega(\log n) \cdot \lambda_n(\mathbf{B}).$$

2. [SVP] *Compute an approximation $\hat{\lambda}_1$ such that*

$$\frac{\lambda_1(\mathbf{B})}{\mu(m(n)) \cdot n^{2.5} \cdot \tau(n) \cdot \omega(\log n)} \leq \hat{\lambda}_1 \leq \lambda_1(\mathbf{B}).$$

3. [CRP] *Compute an approximation $\hat{\rho}$ such that*

$$\rho(\mathbf{B}) \leq \hat{\rho} \leq \mu(m(n)) \cdot n^2 \cdot \tau(n) \cdot \omega(\log n) \cdot \rho(\mathbf{B}).$$

4. [BDD$^\rho$] *Given also a target vector $\mathbf{t} \in span(\mathbf{B})$, find a lattice vector $\mathbf{v} \in \mathcal{L}(\mathbf{B})$ such that*

$$\|\mathbf{v} - \mathbf{t}\| \leq \mu(m(n)) \cdot n^2 \cdot \tau(n) \cdot \omega(\log n) \cdot \rho(\mathbf{B}).$$

**Proof:** Let $\mathcal{F}(\cdot)$ be a probabilistic polynomial time algorithm that finds nonzero vectors within a factor $\mu(m)$ from Minkowski's bound. We claim that $\mathcal{F}(\cdot)$ also satisfies the hypothesis of Theorem 5 with

$$\beta(n) = \sqrt{n\omega(\log n)}\mu(m(n)) = \omega(\sqrt{m(n)}\mu(m(n))),$$

and

$$\gamma(n) = \beta(n)\tau(n)\sqrt{\omega(\log n)} = \sqrt{n}\mu(m(n))\tau(n)\omega(\log n).$$

Let $\alpha(n)$ and $G_n$ be as defined in Theorem 5. We know that with non-negligible probability $\mathcal{F}(\mathbf{g})$ returns a nonzero lattice vector of length at most

$$\|\mathcal{F}(\mathbf{g})\| \leq \mu(m(n))\sqrt{m(n)}\det(\Lambda(\mathbf{g}))^{1/m(n)}.$$

Using the bound on $|\det(\Lambda(\mathbf{g}))| \leq \#G$ from Lemma 5, we get

$$\begin{aligned}
\|\mathcal{F}(\mathbf{g})\| &\leq \mu(m(n))\sqrt{m(n)}\left(\frac{3}{2}\frac{\alpha(n)\sqrt{n}}{\lambda_1(\mathbf{L}_n)}\right)^{n/m(n)} \\
&= \mu(m(n))\sqrt{m(n)}\left(\frac{n^{1.5}\gamma(n)}{8}\right)^{n/m(n)} \\
&= O(\mu(m(n))\sqrt{m(n)} \\
&= o(\beta(n)),
\end{aligned}$$

because $n^{1.5}\gamma(n)/8 = n^{O(1)} = 2^{O(\log n)}$ and $n/m(n) = 1/\Omega(\log n)$. Therefore, $\|\mathcal{F}(\mathbf{g})\| \leq \beta(n)$ with non-negligible probability.

By Theorem 5, there exists a polynomial time algorithm $\mathcal{S}(\cdot)$ that on input any $n$-dimensional lattice basis $\mathbf{B}$, finds (with probability exponentially close to 1) a set of $n$ linearly independent vectors $\mathbf{S} = \mathcal{S}(\mathbf{B})$ such that $\|\mathbf{S}\| \leq \gamma(n) \cdot \hat{\zeta}(\mathbf{B})$. We show how to use this algorithm to solve all the problems in the conclusion of the theorem.

1. [SIVP] Just run $\mathbf{S} = \mathcal{S}(\mathbf{B})$ and output $\mathbf{S}$. By (9)

$$\|\mathbf{S}\| \leq \gamma(n) \cdot \hat{\zeta}(\mathbf{B}) \leq \frac{3}{2} n^{1.5} \cdot \gamma(n) \cdot \lambda_n(\mathbf{B}) = \frac{3}{2} n^2 \tau(n) \mu(m(n)) \omega(\log n) \lambda_n(\mathbf{B}).$$

2. [SVP] On input basis $\mathbf{B}$, run $\mathbf{S} = \mathcal{S}(\mathbf{B}^*)$ where $\mathbf{B}^*$ is the basis of the dual lattice, and output $1/\|\mathbf{S}\|$. By (4),

$$\|\mathbf{S}\| \geq \lambda(\mathbf{B}^*) \geq \frac{1}{\lambda_1(\mathbf{B})}.$$

   Also, by (10),

$$\|\mathbf{S}\| \leq \gamma(n) \cdot \hat{\zeta}(\mathbf{B}^*) \leq \frac{3}{2} n^2 \cdot \gamma(n)/\lambda_1(\mathbf{B}) = \frac{3}{2} n^{2.5} \tau(n) \mu(m(n)) \omega(\log n)/\lambda_1(\mathbf{B}).$$

3. [CRP] This time, we run $\mathbf{S} = \mathcal{S}(\mathbf{B}^*)$ and output $\sqrt{n}\|\mathbf{S}\|/2$. By (2),

$$\sqrt{n}\|\mathbf{S}\|/2 \geq (\sqrt{n}/2)\lambda_n(\mathbf{B}) \geq \rho(\mathbf{B}).$$

   Moreover, by Theorem 1,

$$\sqrt{n}\|\mathbf{S}\|/2 \leq \frac{3}{2} n^{1.5} \cdot \gamma(n) \cdot \rho(\mathbf{B}) = \frac{3}{2} n^2 \tau(n) \mu(m(n)) \omega(\log n) \cdot \rho(\mathbf{B}).$$

4. [BDD$^\rho$] In order to find a lattice point close to target $\mathbf{t}$, we first run $\mathbf{S} = \mathcal{S}(\mathbf{B}^*)$ and then execute Babai's nearest plane algorithm using sublattice $\mathbf{S}$ and target $\mathbf{t}$. The result is a point within distance $\sqrt{n}\|\mathbf{S}\|/2$ from the target. As in the proof for the covering radius problem, this bound satisfies

$$\sqrt{n}\|\mathbf{S}\|/2 \leq \frac{3}{2} n^2 \tau(n) \mu(m(n)) \omega(\log n) \cdot \rho(\mathbf{B}).$$

□

Notice that in the proof of Corollary 2, the definition of group $G_n$ implicitly depends on function $m(n)$. This is because in Theorem 5 the definition of group $G_n$ depends on the value of $\alpha(n)$, which in turns, depends on the value of $\beta(n)$. Moreover, the definition of $\beta(n)$ in the proof of Corollary 2 depends on $\mu(m(n))$. So, unless $\mu(\cdot)$ is a constant function, group $G_n$ can be selected only after the value of $m(n)$ has been chosen. The following corollary immediately follows from Corollary 2 by setting $\mu(m) = 1$, and observing that the definition of group $G_n$ does not depend on $m(n)$ when $\mu(m)$ is constant.

**Corollary 3** *Let $\tau(n) \leq \sqrt{n}$ be a function such that there exists a family of $\tau(n)$-perfect easily decodable lattices. For every superlogarithmic function $\omega(\log n)$, there exists a sequence of groups $\{G_n\}$ such that for any $m(n) = \Theta(n \log n)$, the following is true. If there is a probabilistic polynomial time algorithm $\mathcal{F}(\cdot)$ that on input a uniformly random $\mathbf{g} \in G_n^{m(n)}$, outputs with non-negligible probability a shortest nonzero lattice vector $\mathbf{s} \in \Lambda(\mathbf{g}) \setminus \{\mathbf{0}\}$ (or, even, just a vector satisfying Minkowski's bound $\|\mathbf{s}\| \leq \sqrt{m(n)} \cdot \det(\Lambda(\mathbf{g}))^{1/m(n)}$,) then there is a probabilistic polynomial time algorithm that on input any $n$-dimensional lattice $\mathbf{B}$ solves, with probability exponentially close to 1, any of the following problems*

1. [SIVP] *Find a maximal set of linearly independent vectors within $n^2 \cdot \tau(n) \cdot \omega(\log n)$ from the shortest.*
2. [SVP] *Approximate $\lambda_1(\mathbf{B})$ within a factor $n^{2.5} \cdot \tau(n) \cdot \omega(\log n)$.*

3. [CRP] *Approximate* $\rho(\mathbf{B})$ *within a factor* $n^2 \cdot \tau(n) \cdot \omega(\log n)$.

4. [BDD$^\rho$] *Given also a target vector* $\mathbf{t} \in span(\mathbf{B})$, *find a lattice vector* $\mathbf{v} \in \mathcal{L}(\mathbf{B})$ *within distance* $n^2 \cdot \tau(n) \cdot \omega(\log n) \cdot \rho(\mathbf{B})$ *from* $\mathbf{t}$.

We now turn to the construction of collision resistant hash functions. Following [15], for any $\mathbf{g} \in G_n^{m(n)}$, define function $h_{\mathbf{g}}: \{0,1\}^{m(n)} \to G_n$ by

$$h_{\mathbf{g}}(\mathbf{x}) = \sum_{i=1}^{n} g_i x_i.$$

Notice that function $h_{\mathbf{g}}$ maps $m(n)$ bits to $\log_2 \#G$ bits. If $m(n) > c \cdot \log_2 \#G$, then the function compresses the size of input $\mathbf{x}$ by a factor $c$, and collisions $h_{\mathbf{g}}(\mathbf{x}) = h_{\mathbf{g}}(\mathbf{y})$ (for $\mathbf{x} \neq \mathbf{y}$) are guaranteed to exist by the pigeon hole principle. We prove that, if the key $\mathbf{g}$ is chosen at random, then these collisions are computationally hard to find.

**Corollary 4** *Assume no probabilistic polynomial time algorithm solves problems* SIVP, SVP, CRP *or* BDD$^\rho$ *with probability exponentially close to* 1 *within the factors specified in Corollary 3. Then for any* $c > 1$ *and* $m(n) = \max(c \cdot \log_2 \#G_n, n \log_2 n)$, *there exist no probabilistic polynomial time algorithm that on input a random key* $\mathbf{g} \in G_n^{m(n)}$, *outputs with non-negligible probability a collision to function* $h_{\mathbf{g}}$, *i.e., two binary strings* $\mathbf{x} \neq \mathbf{y}$ *such that* $h_{\mathbf{g}}(\mathbf{x}) = h_{\mathbf{g}}(\mathbf{y})$.

**Proof:** Notice that $m(n) \geq c \cdot \log_2 \#G_n$, so function $h_{\mathbf{g}}$ is a hash function with compression ratio $c$. Assume $\mathcal{F}(\mathbf{g}) = (\mathbf{x}, \mathbf{y})$ be a collision finder algorithm, and notice that if $\mathcal{F}$ is successful, then $\mathbf{x} - \mathbf{y} \in \Lambda(\mathbf{g}) \setminus \{\mathbf{0}\}$ is a lattice vector of length at most

$$\|\mathbf{x} - \mathbf{y}\| \leq \sqrt{m(n)}.$$

Since $\Lambda(\mathbf{g})$ is a sublattice of $\mathbb{Z}^n$,

$$|\det(\Lambda(\mathbf{g}))| \geq \det(\mathbb{Z}^n) = 1.$$

So, lattice vector $\mathbf{x} - \mathbf{y} \in \Lambda(\mathbf{g})$ satisfies Minkowski's bound

$$\|\mathbf{x} - \mathbf{y}\| \leq \sqrt{m(n)} \leq \sqrt{m(n)} \det(\Lambda(\mathbf{g}))^{1/m(n)}.$$

Therefore, collision finder $\mathcal{F}$ can be easily transformed in a short vector algorithms satisfying the conditions in Corollary 3. By Lemma 5, the size of $G_n$ is at most

$$\#G_n \leq \left(\frac{3\alpha(n)\sqrt{n}}{2\lambda_1(\mathbf{L}_n)}\right)^n = \left(\frac{n^{1.5}\gamma(n)}{8}\right)^n = 2^{O(n \log n)}.$$

Therefore $m(n) = \max(c \cdot \log_2 \#G_n, n \log_2 n) = \Theta(n \log n)$, and we can invoke Corollary 3 to get an algorithm to approximately solve SIVP, SVP, CRP and BDD$^\rho$. This contradicts the assumption that some of SIVP, SVP, CRP and BDD$^\rho$ cannot be efficiently approximated. □

# 9 Conclusion and open problems

We related the computational complexity of finding shortest lattice vectors on the average (in appropriately defined random classes of lattices) to the worst-case complexity of approximating various lattice problems. As in [1], the random class of lattices is quite natural: lattices are defined as the set of solutions to a uniformly random homogeneous linear equation over a suitably chosen Abelian group. The worst-case approximation factors achieved depend on the class of easily decodable lattices used in the definition of the group. In particular, if $\tau(n)$-perfect easily decodable lattices are used, then finding shortest vectors in random lattices is at least as hard as approximating the length of the shortest vector in any lattice within a factor $\gamma(n) = n^{2.5}\tau(n)\omega(\log n)$. Even for $\tau(n) = \sqrt{n}$ (which correspond as a special case to Ajtai's random class of lattices) this improves previously known best connection factor from $n^{4+\epsilon}$ [8] to $n^3\omega(\log n)$. We also showed that finding shortest vectors in random lattices is at least as hard as approximating within a factor $n^2\tau(n)\omega(\log n)$ any of the following problems:

- [SIVP] Computing a maximal set of shortest linearly independent vectors
- [CRP] Computing the covering radius
- [BDD$^\rho$] Computing a lattice vector within distance $\max_{\mathbf{x}} \mathrm{dist}(\mathbf{x}, \mathcal{L}(\mathbf{B}))$ from a given target,

improving [8] in the case of SIVP, and connecting the average case complexity of the shortest vector problem to two new computational problems on lattices that might be of independent interest.

We also gave polynomial time constructions of easily decodable $\tau(n)$-perfect lattices with $\tau(n) = o(\sqrt{n})$. These constructions allow to achieve connection factors $n^{2.5}\omega(\sqrt{\log n \log\log n})$ (for SIVP, CRP and BDD$^\rho$) and $n^3\omega(\sqrt{\log n \log\log n})$ (for SVP). While this improvement over $\tau(n) = \sqrt{n}$ is not substantial, it suggests that further investigation of almost perfect lattices might allow to find easily decodable $\tau(n)$-perfect lattices with much smaller $\tau(n)$, e.g., $\tau(n) = n^\epsilon$ or even $\tau(n) = O(1)$. This would immediately reduce the connection factor for all the above problems by about $\sqrt{n}$.

Another possible source of improvement are better bounds relating the fundamental constants associated to a lattice. Our main theorem (Theorem 5) shows that finding short vectors on the average is at least as hard as finding vectors that are not much longer than a new lattice quantity we call the generalized uniform radius. All other results are obtained by first relating the generalized uniform radius to the covering radius (Theorem 1), and then bounding the covering radius in terms of other lattice constants using standard transference theorems and other well known bounds (Proposition 2). In particular, (9) and (10) show that the generalized uniform radius is at most $O(n^{1.5})$ times $\lambda_n(\mathbf{B})$ or at most $O(n^2)$ times $1/\lambda_1(\mathbf{B}^*)$. It would be interesting to improve (9) and (10) to show, for example, that

$$\hat{\zeta}(\mathbf{B}) \leq O(n)\lambda_n(\mathbf{B}). \tag{29}$$

and

$$\hat{\zeta}(\mathbf{B}) \leq O(n)/\lambda_1(\mathbf{B}^*). \tag{30}$$

Whether these bounds hold true is a natural geometric question, and proving them would be of independent interest. Moreover, it would allow to reduce the connection factors for SIVP and SVP by $O(\sqrt{n})$ and $O(n)$, respectively. Together with the construction of almost perfect easily decodable lattices, this would immediately improve the connection factors for both SVP and SIVP to just $n^{1.5}\omega(\log n)$. Connections with such small approximation factors are currently known only for restrictions of the (worst-case) shortest vector problem to lattices with special structure where the shortest vector is unique is some technical sense [34].

Notice that by (4), bound (30) would also imply (29). Also, (30), if correct, would be asymptotically optimal because Conway and Thompson (see [32]) showed that there exist self dual lattices such that $\rho(\mathbf{B}) \cdot \lambda_1^*(\mathbf{B}) \geq O(n)$, and by Proposition 10 $\rho(\mathbf{B}) \leq \zeta(\mathbf{B}) \leq \hat{\zeta}(\mathbf{B})$. We conjecture that (30) holds true, and that there exist random lattices such that finding shortest vectors on the average (with non-negligible probability) is at least as hard as approximating the length of the shortest nonzero vector (or finding a maximal set of shortest linearly independent vectors) in any $n$-dimensional lattice within a factor $n^{1.5}\omega(\log n)$.

# 10 Acknowledgments

The author would like to thank Ravi Kannan and Alex Vardy for interesting discussions and pointers to relevant references.

# References

[1] M. Ajtai. Generating hard instances of lattice problems (extended abstract). In *Proceedings of the twenty-eighth annual ACM symposium on the theory of computing - STOC '96*, pages 99–108, Philadelphia, Pennsylvania, USA, May 1996. ACM.

[2] M. Ajtai and C. Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In *Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing - STOC '97*, pages 284–293, El Paso, Texas, USA, May 1997. ACM.

[3] M. Ajtai, R. Kumar, and D. Sivakumar. A sieve algorithm for the shortest lattice vector problem. In *Proceedings on 33rd annual acm symposium on theory of computing, stoc 2001*, pages 266–275, Heraklion, Crete, Greece., 2001. ACM.

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

[5] J. Blömer and J.-P. Seifert. On the complexity of computing short linearly independent vectors and short bases in a lattice. In *Proceedings of the thirty-first Annual ACM Symposium on Theory of Computing - STOC '99*, pages 711–720, Atlanta, Georgia, USA, May 1999. ACM.

[6] J. Bruck and M. Naor. The hardness of decoding linear codes with preprocessing. *IEEE Transactions on Information Theory*, 36(2):381–385, Mar. 1990.

[7] G. J. Butler. Simultaneous packing and covering in euclidean space. *Proc. London Math. Soc.*, 25:721–735, 1972.

[8] J.-Y. Cai and A. P. Nerurkar. An improved worst-case to average-case connection for lattice problems (extended abstract). In *38th annual symposium on foundations of computer science – FOCS'97*, pages 468–477, Miami Beach, Florida, 20 Oct. 1997. IEEE.

[9] J. H. Conway and N. J. A. Sloane. *Sphere packings, lattices and groups.* Springer Verlag, 3rd edition, 1998.

[10] I. Dinur, G. Kindler, R. Raz, and S. Safra. An improved lower bound for approximating CVP. *Combinatorica.* To appear.

[11] M. Dyer, A. Frieze, and R. Kannan. A random polynomial-time algorithm for approximating the volume of convex bodies. *Journal of the Association for Computing Machinery*, 38(1):1–17, Jan. 1991.

[12] U. Feige and D. Micciancio. The inapproximability of lattice and coding problems with preprocessing. *Journal of Computer and System Sciences*, 2003. (To appear. Preliminary version in CCC 2002.).

[13] O. Goldreich. *Foundation of Cryptography - Basic Tools.* Cambridge Unievrsity Press, 2001.

[14] O. Goldreich and S. Goldwasser. On the limits of nonapproximability of lattice problems. *Journal of Computer and System Sciences*, 60(3):540–563, 2000. Preliminary version in STOC'98.

[15] O. Goldreich, S. Goldwasser, and S. Halevi. Collision-free hashing from lattice problems. Technical Report TR96-056, Electronic Colloquium on Computational Complexity (ECCC), 1996.

[16] O. Goldreich, D. Micciancio, S. Safra, and J.-P. Seifert. Approximating shortest lattice vectors is not harder than approximating closest lattice vectors. *Information Processing Letters*, 71(2):55–61, 1999.

[17] I. Honkala and A. Tietäväinen. *Handbook of Coding Theory*, volume 2, chapter 13, Codes and Number Theory, pages 1141–1194. Elsevier, 1998.

[18] R. Kannan. *Annual reviews of computer science*, volume 2, chapter Algorithmic Geometry of numbers, pages 231–267. Annual Review Inc., Palo Alto, California, 1987.

[19] R. Kannan. Minkowski's convex body theorem and integer programming. *Mathematics of operation research*, 12(3):415–440, Aug. 1987.

[20] R. Kannan. Lattice translates of a polytope and the Frobenius problem. *Combinatorica*, 12(2):161–177, 1992.

[21] R. Kannan and S. Vempala. Sampling lattice points. In *Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing - STOC '97*, pages 696–700, El Paso, Texas, USA, May 1997. ACM.

[22] J. C. Lagarias, H. W. Lenstra, Jr., and C.-P. Schnorr. Korkine-Zolotarev bases and successive minima of a lattice and its reciprocal lattice. *Combinatorica*, 10(4):333–348, 1990.

[23] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261:513–534, 1982.

[24] A. Lobstein. The hardness of solving subset sum with preprocessing. *IEEE Transactions on Information Theory*, 36(4):943–946, July 1990.

[25] J. E. Mazo and A. M. Odlyzko. Lattice points in high dimensional spheres. *Monatsh. Math.*, 110:47–61, 1990.

[26] A. M. McLoughlin. The complexity of computing the covering radius of a code. *IEEE Transactions on Information Theory*, 30:800–804, Nov. 1984.

[27] D. Micciancio. The hardness of the closest vector problem with preprocessing. *IEEE Transactions on Information Theory*, 47(3):1212–1215, Mar. 2001.

[28] D. Micciancio. Improving lattice based cryptosystems using the Hermite normal form. In J. Silverman, editor, *Cryptography and lattices conference — CaLC'01*, volume 2146 of *Lecture Notes in Computer Science*, pages 126–145, Providence, Rhode Island, 29–30Mar. 2001. Springer-Verlag.

[29] D. Micciancio. The shortest vector problem is NP-hard to approximate to within some constant. *SIAM Journal on Computing*, 30(6):2008–2035, Mar. 2001. Preliminary version in FOCS 1998.

[30] D. Micciancio. Improved cryptographic hash functions with worst-case/average-case connection. In *Proceedings of the thirty-fourth Annual ACM Symposium on Theory of Computing - STOC 2002*, pages 609–618, Montréal, Québec, Canada, May 2002. ACM.

[31] 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, Massachusetts, Mar. 2002.

[32] J. Milnor and D. Husemoller. *Simmetric Bilinear Forms*. Springer-Verlag, 1973.

[33] O. Regev. Improved Inapproximability of Lattice and Coding Problems with Preprocessing. In *Proceedings of the IEEE Conference on Computational Complexity*, Århus, Denmark, 7 July 2003. IEEE. To appear.

[34] O. Regev. New lattice based cryptographic constructions. In *Proceedings of the thirty-fifth annual ACM symposium on theory of computing - STOC 2003*, pages 407–426, San Diego, CA, USA, June 2003. ACM.

[35] C. A. Rogers. A note on coverings and packings. *Journal of the London Mathematical Society*, 25:327–331, 1950.

[36] C.-P. Schnorr. A hierarchy of polynomial time lattice basis reduction algorithms. *Theoretical Computer Science*, 53(2–3):201–224, 1987.

[37] A. Vardy. Algorithmic complexity in coding theory and the minimum distance problem. In *Proceedings of the twenty-ninth annual acm symposium on theory of computing, stoc'97*, pages 92–109, El Paso, Texas, May 4–6 1997. ACM, ACM.



ECCC ISSN 1433-8092
http://www.eccc.uni-trier.de/eccc
ftp://ftp.eccc.uni-trier.de/pub/eccc
ftpmail@ftp.eccc.uni-trier.de, subject 'help eccc'