Improved Reduction from the Bounded Distance Decoding Problem to the Unique Shortest Vector Problem in Lattices*†

Shi Bai[1], Damien Stehlé[2], and Weiqiang Wen[3]

1 **ENS de Lyon, Laboratoire LIP (U. Lyon, CNRS, ENSL, INRIA, UCBL), Lyon, France**
shi.bai@ens-lyon.fr
2 **ENS de Lyon, Laboratoire LIP (U. Lyon, CNRS, ENSL, INRIA, UCBL), Lyon, France**
damien.stehle@ens-lyon.fr
3 **ENS de Lyon, Laboratoire LIP (U. Lyon, CNRS, ENSL, INRIA, UCBL), Lyon, France**
weiqiang.wen@ens-lyon.fr

Abstract

We present a probabilistic polynomial-time reduction from the lattice Bounded Distance Decoding (BDD) problem with parameter $1/(\sqrt{2}\cdot\gamma)$ to the unique Shortest Vector Problem (uSVP) with parameter γ for any $\gamma > 1$ that is polynomial in the lattice dimension n. It improves the BDD to uSVP reductions of [Lyubashevsky and Micciancio, CRYPTO, 2009] and [Liu, Wang, Xu and Zheng, Inf. Process. Lett., 2014], which rely on Kannan's embedding technique. The main ingredient to the improvement is the use of Khot's lattice sparsification [Khot, FOCS, 2003] before resorting to Kannan's embedding, in order to boost the uSVP parameter.

1998 ACM Subject Classification F.2.1 Numerical Algorithms and Problems

Keywords and phrases Lattices, Bounded Distance Decoding Problem, Unique Shortest Vector Problem, Sparsification

Digital Object Identifier 10.4230/LIPIcs.ICALP.2016.76

1 Introduction

A (full-rank) lattice $\mathcal{L}$ in dimension n is the set of all integer linear relations of n linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{Q}^n$. The minimum $\lambda_1(\mathcal{L})$ quantifies the discreteness of $\mathcal{L}$: the smallest Euclidean distance between two distinct lattice vectors is $\lambda_1(\mathcal{L})$. A standard computational problem on lattices is the so-called Bounded Distance Decoding problem (BDD_α): Given as inputs a basis $\mathbf{B} = (\mathbf{b}_i)_i$ of a lattice $\mathcal{L}$ and a vector $\mathbf{t} \in \mathbb{Q}^n$ (called target vector) within distance $\alpha \cdot \lambda_1(\mathcal{L})$ of $\mathcal{L}$, the goal is to find a vector $\mathbf{b} \in \mathcal{L}$ closest to $\mathbf{t}$. Here $\alpha > 0$ is a problem parameter, which may be a function of the lattice dimension n. The hardness of BDD was initially studied in the context of linear codes by Vardy in [22], and later in the context of lattices by Liu *et al.* in [14].

In communications theory, BDD models the task of decoding in the context of continuous channels with white Gaussian noise [6]. The information to be transmitted is stored in a

* A full version of the paper is available at http://eprint.iacr.org/2016/753.
† This work has been supported by ERC Starting Grant ERC-2013-StG-335086-LATTAC.

43rd International Colloquium on Automata, Languages, and Programming (ICALP 2016).
Editors: Ioannis Chatzigiannakis, Michael Mitzenmacher, Yuval Rabani, and Davide Sangiorgi;
Article No. 76; pp. 76:1–76:12
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

lattice vector, and the receiver should recover this vector from a noisy version thereof. The knowledge of the signal-to-noise ratio implies a bound on the distance from the noisy vector to the lattice. Decoding a white Gaussian noise channel can be seen as a version of BDD in which the distance to the lattice follows a prescribed distribution.

In cryptography, BDD is closely related to the Learning With Errors problem (LWE) [19], which serves as a security foundation for numerous cryptographic primitives. When the number of requested LWE samples is bounded (which is most often the case in cryptographic constructions), LWE may be viewed as a variant of BDD in which the offset from $\mathbf{t}$ to $\mathcal{L}$ is Gaussian (like in the decoding context), and $\mathcal{L}$ is randomly sampled.

A common approach to solve BDD is via Kannan's embedding technique [9, Se. 6]. The principle is to map the offset between $\mathbf{t}$ and a closest lattice vector to $\mathbf{t}$, to a shortest non-zero vector in an $(n+1)$-dimensional lattice. Lattice reduction [12, 20] and short lattice vector enumeration [8, 7] may then be used to find shortest non-zero vectors in the $(n+1)$-dimensional lattice. Formally, Kannan's embedding technique is a reduction from BDD to a variant of the Shortest Vector Problem (SVP) in which the pair of shortest non-zero vectors in the lattice under scope are known to be much shorter than any other lattice vector not parallel to them. For a lattice $\mathcal{L}$, we define the second minimum $\lambda_2(\mathcal{L})$ as the minimal radius of a zero-centered ball that contains two or more linearly independent vectors from $\mathcal{L}$. The unique Shortest Vector Problem (uSVP_γ) of parameter $\gamma \geq 1$ consists in finding a shortest non-zero vector in a lattice $\mathcal{L}$ described by an input basis $\mathbf{B} = (\mathbf{b}_i)_i$, under the promise that $\lambda_2(\mathcal{L}) \geq \gamma \cdot \lambda_1(\mathcal{L})$. This reduction was analyzed by Lyubashevsky and Micciancio in [15], who showed that $\text{BDD}_{1/(2\gamma)}$ reduces to uSVP_γ for any $\gamma \geq 1$. Later, Liu *et al.* [13] refined the analysis of Lyubashevsky and Micciancio and proved that BDD_{1/γ_1} reduces to uSVP_γ with $\gamma_1 = \sqrt{3/(4-\gamma^2)}\gamma + 1$, for any $\gamma \in (1, 1.9318)$. It is folklore [3, 17] that the analysis can be tightened even more, resulting in a proof that BDD_{1/γ_1} reduces to uSVP_γ with $\gamma_1 = (2\gamma^2 + 2\lfloor\gamma\rfloor\lfloor\gamma+1\rfloor)/(2\lfloor\gamma\rfloor+1)$, for any $\gamma \geq 1$. For the sake of completeness, we give a proof in Appendix A.1 of the full version. Note that in the case of $\gamma = 1$ (and in fact all integral γ), all three results are identical: $\text{BDD}_{1/2}$ reduces to uSVP_1.

Our result. We give a probabilistic polynomial-time reduction from $\text{BDD}_{1/(\sqrt{2}\gamma)}$ to uSVP_γ, for any $\gamma \geq 1$ that is polynomially bounded as a function of n. As clearly visible in Figure 1, this reduction supersedes all prior results with respect to the BDD problem parameter. In particular, we reduce $\text{BDD}_{1/\sqrt{2}}$ to uSVP_1. Our improvement comes with two weaknesses: the reduction is probabilistic and restricted to polynomially bounded γ. Like prior reductions, the dimension of the uSVP instance is only one more than the dimension of the BDD instance.

Technical overview. We illustrate our improvement with the case of $\text{BDD}_{1/2}$. Given the $\text{BDD}_{1/2}$ instance $(\mathbf{B}, \mathbf{t})$, Kannan's embedding consists in constructing the following uSVP_1 instance:

$$\mathbf{B}' = \begin{pmatrix} \mathbf{B} & \mathbf{t} \\ \mathbf{0} & d \end{pmatrix} \in \mathbb{Q}^{n+1},$$

with $d = \text{dist}(\mathbf{t}, \mathcal{L}) \leq \lambda_1(\mathcal{L})/2$, where $\mathcal{L}$ is the lattice spanned by $\mathbf{B}$ (in fact, the reduction does not know d, but this is a mere technical problem which can be handled easily, as explained in Section 2). If $\mathbf{c}$ denotes a closest vector to $\mathbf{t}$ in $\mathcal{L}$ then it may be proved that the vector $\mathbf{s}' = ((\mathbf{c}-\mathbf{t})^{\mathrm{T}}, -d)^{\mathrm{T}}$ is a shortest non-zero vector of lattice $\mathcal{L}'$ of basis $\mathbf{B}'$. Now, let $\mathbf{s}$ denote a shortest non-zero vector in $\mathcal{L}$ and assume that $\mathbf{t}$ is exactly halfway between $\mathbf{c}$ and $\mathbf{c}+\mathbf{s}$. Then both $\mathbf{s}'$ and $\mathbf{s}' + (\mathbf{s}^{\mathrm{T}}, 0)^{\mathrm{T}}$ in $\mathcal{L}'$ have norm $\sqrt{2} \cdot d$ but are linearly independent.

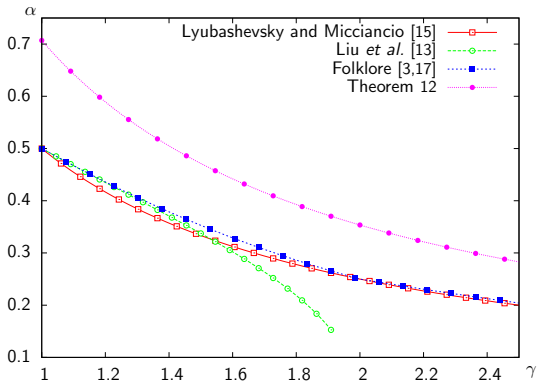

Figure 1 Comparison between prior reductions from BDD_α to uSVP_γ, and ours.

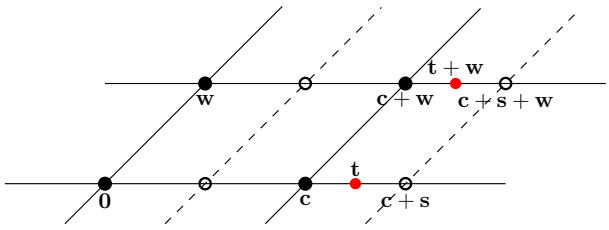

Figure 2 An example of sparsification for $\mathrm{BDD}_{1/2}$ (here $\mathbf{w} \in \mathcal{L}_{p,\mathbf{z}}/\mathcal{L}$).

This shows that we can have $\lambda_2(\mathcal{L}') = \lambda_1(\mathcal{L}')$ and obtain a uSVP_γ instance with $\gamma = 1$. This is a limitation of Kannan's embedding and hence of its analyzes.

We modify the reduction to increase the ratio $\lambda_2(\mathcal{L}')/\lambda_1(\mathcal{L}')$. To achieve this, we use lattice sparsification on $\mathcal{L}$. It provides a full-rank sublattice $\mathcal{L}_{\mathrm{sparse}} \subseteq \mathcal{L}$ that still contains a closest vector $\mathbf{c} \in \mathcal{L}$ to $\mathbf{t}$, but no other close-by vector. We consider the vectors of $\mathcal{L}$ whose coordinates with respect to a basis $\mathbf{B}$ satisfy a linear equation modulo some prime integer p: $\mathcal{L}_{\mathrm{sparse}} = \mathcal{L}_{p,\mathbf{z}} = \{\mathbf{b} \in \mathcal{L} : \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{b} \rangle = 0 \bmod p\}$, for some vector $\mathbf{z} \in \mathbb{Z}_p^n$. This technique was first introduced by Khot in [10, 11]. To guarantee that vectors in $\mathcal{L}$ remain in the sparsified set with probability close to $1/p$, a uniform coset of $\mathcal{L}_{p,\mathbf{z}}$ (modulo $\mathcal{L}$) was considered in [4, 5]. Technically, we use the formulation from [21] of the latter variant.

The aim of sparsification in our context is to keep a closest vector $\mathbf{c} \in \mathcal{L}$ to $\mathbf{t}$, and remove as many as nearby vectors of $\mathcal{L}$ as possible. After sparsification, vector $\mathbf{c}$ remains in the sparse lattice (with non-negligible probability), and all other remaining vectors are much further away from $\mathbf{t}$. For $\mathrm{BDD}_{1/2}$, a simple example of sparsification is shown in Figure 2: there are two points simultaneously closest to the target point; then sparsification is used to remove one of the closest points (either is fine); in the sparse lattice, the closest vector is much closer than any other lattice vector. In Figure 2, after sparsification, all the lattice vectors labelled with filled dots are kept, e.g., vector $\mathbf{c} + \mathbf{w}$, and other vectors labelled with hollow dots are removed, e.g., vector $\mathbf{c} + \mathbf{s} + \mathbf{w}$.

The probability of keeping a vector of $\mathcal{L}$ in the sparsified set is essentially $1/p$. As we want the probability of keeping $\mathbf{c}$ to be non-negligible, we are hence restricted to taking $p \leq \mathrm{poly}(n)$. As a result, we cannot remove more than polynomially many close-by vectors, because each

one individually is removed with probability $\approx 1 - 1/p$ (a precise statement is given in Lemma 8). To assess the limitation of our reduction, we are hence interested in the largest value of α such that for any lattice $\mathcal{L}$ and any vector $\mathbf{t}$, there are at most $\mathrm{poly}(n)$ vectors within distance $\alpha \cdot \lambda_1(\mathcal{L})$ from $\mathbf{t}$. The quantity $\alpha \cdot \lambda_1(\mathcal{L})$ can be viewed as the worst-case list-decoding radius. Interestingly, this problem was studied by Ajtai [1] and Micciancio [16] in the context of proving hardness of SVP. Proofs of the following two statements may be found in [18, Chap. 5]:

- For any lattice $\mathcal{L}$ and vector $\mathbf{t}$, there are $\leq 2n$ vectors of $\mathcal{L}$ within distance $\lambda_1(\mathcal{L})/\sqrt{2}$ from $\mathbf{t}$.
- For any $\alpha > 1/\sqrt{2}$, there exists $\varepsilon > 0$ such that for any sufficiently large n we can find an n-dimensional lattice $\mathcal{L}$ and a vector $\mathbf{t}$ such that there are $\geq 2^{n^\varepsilon}$ vectors of $\mathcal{L}$ within distance $\alpha \cdot \lambda_1(\mathcal{L})$ from $\mathbf{t}$.

The overall reduction consists in first sparsifying $\mathcal{L}$ to $\mathcal{L}_{p,\mathbf{z}}$ and shifting $\mathbf{t}$ (as we use a coset of $\mathcal{L}_{p,\mathbf{z}}$), and then resorting to Kannan's embedding. To increase the ratio $\lambda_2(\mathcal{L}')/\lambda_1(\mathcal{L}')$, we decrease the bottom-right entry in $\mathbf{B}'$ from d to $k \cdot d$ for some $k < 1$. Geometrically, this has the effect of limiting the contribution of the extra dimension. This idea was already used in [13], but we decrease k even further, to $1/\mathrm{poly}(n)$. An additional difficulty, related to this decrease of k, is that short vectors in $\mathcal{L}'$ may be obtained by using multiples of $\mathbf{t}$. Let $m \geq 2$ and $\mathbf{d} \in \mathcal{L}$ closest to $m\mathbf{t}$. Then, vector $((\mathbf{d} - m\mathbf{t})^{\mathrm{T}}, mkd)^{\mathrm{T}}$ may be very short (if very unlucky, it has norm mkd). We remove such annoying vectors with sparsification.

Open problems. In [15], Lyubashevsky and Micciancio considered the relative hardness of BDD and uSVP. They obtained a reduction from $\mathrm{BDD}_{1/(2\gamma)}$ to uSVP_γ, and a reduction from uSVP_γ to $\mathrm{BDD}_{1/\gamma}$ (for all $\gamma \geq 1$). This led them to conjecture that it may be possibly to show that (i)- $\mathrm{uSVP}_{\gamma/2}$ reduces to $\mathrm{BDD}_{1/\gamma}$, or (ii)- $\mathrm{BDD}_{1/\gamma}$ reduces to uSVP_γ, or (iii)- uSVP_γ reduces to $\mathrm{BDD}_{1/(\sqrt{2}\gamma)}$ and $\mathrm{BDD}_{1/(\sqrt{2}\gamma)}$ reduces to uSVP_γ. By showing the second half of (iii), (i) becomes very unlikely.

Independently, it would be interesting to make our reduction deterministic and let it work even for parameters γ that are not $\leq \mathrm{poly}(n)$.

Notation. For a lattice $\mathcal{L}$, a point $\mathbf{t}$, a radius r, we define $\mathcal{B}(\mathbf{t}, r) = \{\mathbf{x} : \|\mathbf{x} - \mathbf{t}\| \leq r\}$. We let $\mathrm{dist}(\mathbf{t}, \mathcal{L}(\mathbf{B}))$ denote the distance between $\mathbf{t}$ and lattice $\mathcal{L}(\mathbf{B})$. We always represent the basis of lattice in column form. If S is a finite set, we let $\#S$ denote its cardinality.

2 Reminders

In this section, we recall basic facts on lattices and lattice problems. We then consider lattice sparsification and its use in the context of BDD instances.

2.1 Lattice problems

We refer the reader to [18] for an introduction to the computational aspects of lattices.

▶ **Definition 1** (Lattice). An n-dimensional lattice $\mathcal{L} \subseteq \mathbb{Q}^m$ $(m \geq n)$ is a discrete additive subgroup of $\mathbb{R}^m$. The lattice $\mathcal{L}$ is the set of all integral linear combinations of n linearly independent basis vectors $\mathbf{B} = \{\mathbf{b}_1, \cdots, \mathbf{b}_n\} \subseteq \mathbb{Q}^m$. In other words, we have

$$\mathcal{L}(\mathbf{B}) = \left\{ \sum_{i \in [n]} u_i \mathbf{b}_i : \ \mathbf{u} \in \mathbb{Z}^n \right\}.$$

▶ **Definition 2** (Successive minima)**.** For any lattice $\mathcal{L}$, the i-th minimum $\lambda_i(\mathcal{L})$ is the radius of the smallest ball with center $\mathbf{0}$ and containing i linearly independent lattice vectors:

$$\lambda_i(\mathcal{L}) = \inf\{r : \dim(\mathrm{span}(\mathcal{L} \cap \mathcal{B}(\mathbf{0}, r))) \geq i\}.$$

In this work, we investigate the respective hardness of uSVP_γ and BDD_α defined below, when the lattice dimension n goes to infinity. The problem parameters γ and α can be functions of n.

▶ **Definition 3** (Unique Shortest Vector Problem (uSVP_γ))**.** Let $\gamma \geq 1$. Given as input a lattice basis $\mathbf{B}$ such that $\lambda_2(\mathbf{B}) \geq \gamma \cdot \lambda_1(\mathbf{B})$, the goal is to find a non-zero vector $\mathbf{v} \in \mathcal{L}(\mathbf{B})$ of norm $\lambda_1(\mathcal{L}(\mathbf{B}))$. The Shortest Vector Problem (SVP) corresponds to $\gamma = 1$.

In the literature (in [15], for example), uSVP is sometimes be defined with a strict lower bound on $\lambda_2(\mathbf{B})$. We allow equality (as in [13]), as it is more convenient in our proofs. Note that Lemma 5 below implies that these two variants are equivalent.

▶ **Definition 4** (Bounded Distance Decoding (BDD_α))**.** Let $\alpha > 0$. Given as inputs a lattice basis $\mathbf{B}$ and a vector $\mathbf{t}$ such that $\mathrm{dist}(\mathbf{t}, \mathcal{L}(\mathbf{B})) \leq \alpha \cdot \lambda_1(\mathbf{B})$, the goal is to find a lattice vector $\mathbf{v} \in \mathcal{L}(\mathbf{B})$ closest to $\mathbf{t}$.

Note that in some works, the range of α is restricted to $(0, 1/2)$. This is to guarantee that there is exactly one element of $\mathcal{L}$ in the ball of radius $\alpha \cdot \lambda_1(\mathcal{L})$ centered on $\mathbf{t}$. The problem is well-defined even for large α, and in this work we actually consider $\alpha \geq 1/2$.

In the next lemma, it is stated that BDD_α is equivalently hard for any parameter α' that is within a factor $(1 - 1/n)^c$ of α, for any constant c.

▶ **Lemma 5** ([15, Cor. 2])**.** *For any $\alpha > 0$, any constant $c > 0$, there is a polynomial-time reduction from BDD_α to $\mathrm{BDD}_{\alpha(1-1/n)^c}$.*

2.2 Approximation results

Given as input an n-dimensional lattice basis $\mathbf{B} \in \mathbb{Q}^{n \times n}$, it is possible to find a non-zero vector that has norm at most $2^{n/2} \cdot \lambda_1(\mathcal{L}(\mathbf{B}))$ in time polynomial in n and also the bit-sizes of the entries of $\mathbf{B}$, by using the LLL algorithm [12]. Further, by using the Babai round-off algorithm [2] with inputs an n-dimensional lattice basis $\mathbf{B} \in \mathbb{Q}^{n \times n}$ and a target vector $\mathbf{t} \in \mathbb{Q}^n$, one obtains an approximation of the distance between $\mathbf{t}$ and $\mathcal{L}(\mathbf{B})$ within a factor $2^{n/2}$ in time polynomial in n and also the bit-sizes of the entries of $\mathbf{B}$ and $\mathbf{t}$.

▶ **Lemma 6** ([12, Prop. 1.6])**.** *There exists a polynomial-time algorithm that, given as input an n-dimensional lattice basis $\mathbf{B} \in \mathbb{Q}^{n \times n}$, outputs $\ell \in \lambda_1(\mathcal{L}) \cdot [1, 2^{n/2})$.*

▶ **Lemma 7** ([2, Thm. 3.1])**.** *There exists a polynomial-time algorithm that, given as input an n-dimensional lattice basis $\mathbf{B} \in \mathbb{Q}^{n \times n}$ and a target vector $\mathbf{t} \in \mathbb{Q}^n$, outputs $d \in \mathrm{dist}(\mathbf{t}, \mathcal{L}(\mathbf{B})) \cdot [1, 2^{n/2})$.*

We will rely on much tighter approximations to $\lambda_1(\mathcal{L}(\mathbf{B}))$ (resp. $\mathrm{dist}(\mathbf{t}, \mathcal{L}(\mathbf{B}))$) than provided by Lemmata 6 and 7. We explain here why we may assume that we know $\ell \in \lambda_1(\mathcal{L}(\mathbf{B})) \cdot [1, 1/(1 - 1/n))$ (resp. $d \in \mathrm{dist}(\mathbf{t}, \mathcal{L}(\mathbf{B})) \in [1, 1/(1 - 1/n))$).

Our reduction is from BDD, whose candidate solutions can be compared in polynomial time. Assume the reduction finds the optimal solution in one case among polynomially many, but that we do not know which one. Then we may call the reduction this polynomially many times, and keep a best solution among the returned ones. Concretely, our reduction will be

proved correct if we know a tight approximation to $\lambda_1(\mathcal{L}(\mathbf{B}))$ and $\mathrm{dist}(\mathbf{t}, \mathcal{L}(\mathbf{B}))$, where $(\mathbf{B}, \mathbf{t})$ is the BDD instance. We can assume without loss of generality that we have these tight approximations, as the interval $[1, 2^{n/2})$ may be covered by polynomially many intervals of the form $x \cdot [1, 1/(1-1/n))$ for well-chosen rational x's.

2.3 Lattice sparsification

Our techniques rely on lattice sparsification, and, more concretely, on the following lemma.

▶ **Lemma 8** ([21, Cor. 2.16]). *For any prime p, collection of vectors $\mathbf{v}_1, \cdots, \mathbf{v}_N \in \mathbb{Z}_p^n \setminus \{\mathbf{0}\}$, and $\mathbf{x} \notin \{\mathbf{v}_i\}_{i \le N}$, we have*

$$\frac{1}{p} - \frac{N}{p^2} - \frac{N}{p^{n-1}} \le \Pr_{\mathbf{z},\mathbf{u} \hookleftarrow U(\mathbb{Z}_q^n)} \left[\begin{array}{ll} \forall i, & \langle \mathbf{z}, \mathbf{v}_i + \mathbf{u} \rangle \neq 0 \bmod p \\ & \langle \mathbf{z}, \mathbf{x} + \mathbf{u} \rangle = 0 \bmod p \end{array} \right] \le \frac{1}{p} + \frac{1}{p^n}.$$

The upper bound in Lemma 8 is not used in this work, but we keep it to show that the difference between the upper and lower bound is small, and thus that the lower bounds is almost tight. Lemma 8 leads to the definition of a sublattice that will be used in our reduction from BDD to uSVP. The lemma below explains that we can efficiently compute a basis of the sublattice.

▶ **Lemma 9.** *There exists a polynomial-time algorithm which, given as inputs a basis $\mathbf{B} \in \mathbb{Q}^{n \times n}$ of an n-dimensional lattice $\mathcal{L}$, an integer p and a vector $\mathbf{z} \in \mathbb{Z}_p^n$, outputs a basis $\mathbf{B}_{p,\mathbf{z}}$ of the lattice $\mathcal{L}_{p,\mathbf{z}} = \{\mathbf{x} \in \mathcal{L} \mid \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{x} \rangle = 0 \bmod p\}$.*

Proof. According to the definition of the lattice $\mathcal{L}_{p,\mathbf{z}}$, we have

$$\langle \mathbf{z}, \mathbf{y} \rangle = 0 \bmod p,$$

where $\mathbf{y} = \mathbf{B}^{-1}\mathbf{x}$ and $\mathbf{x} \in \mathcal{L}_{p,\mathbf{z}}$. We can obtain a basis $\mathbf{S}$ of the kernel $\mathbf{y}$ over $\mathbb{Z}^n$. We compute the column Hermite normal form of $\begin{bmatrix} \mathbf{S} & p\mathbf{I}_n \end{bmatrix} \in \mathbb{Z}^{n \times 2n}$; and obtain the nonzero columns $\mathbf{S}' \in \mathbb{Z}^{n \times n}$. The columns of $\mathbf{S}'$ generate the lattice orthogonal to $\mathbf{z} \pmod p$. In the end, we compute $\mathbf{B}_{p,\mathbf{z}} = \mathbf{B}\mathbf{S}'$, which is a basis for the lattice $\mathcal{L}_{p,\mathbf{z}}$. ◀

Below, we state that for any two lattice vectors in $\mathcal{L}$ with distance smaller than $p \cdot \lambda_1(\mathcal{L})$ where p is an integer, the coordinates of these two lattice vectors differ modulo p.

▶ **Lemma 10.** *For any basis $\mathbf{B}$, any integer p and any pair of lattice vectors $\mathbf{x} \neq \mathbf{v}$ with $\|\mathbf{x} - \mathbf{v}\| < p \cdot \lambda_1(\mathcal{L}(\mathbf{B}))$, we have that $\mathbf{B}^{-1}\mathbf{x} \neq \mathbf{B}^{-1}\mathbf{v} \bmod p$.*

Proof. For all lattice vector $\mathbf{a}$, we let $\widetilde{\mathbf{a}}$ denote its coordinate vector under the basis $\mathbf{B}$. Assume by contradiction that $\widetilde{\mathbf{x}} = \widetilde{\mathbf{v}} \bmod p$. Equivalently, we have $\mathbf{x} - \mathbf{v} \in p \cdot \mathcal{L}(\mathbf{B})$.

Combined with $\mathbf{x} \neq \mathbf{v}$, we have $\|\mathbf{x} - \mathbf{v}\| \ge p \cdot \lambda_1(\mathcal{L})$, which is in contradiction with $\|\mathbf{x} - \mathbf{v}\| < p \cdot \lambda_1(\mathcal{L})$. As a result, we have $\widetilde{\mathbf{x}} \neq \widetilde{\mathbf{v}} \bmod p$. ◀

The proof from [18] of the lemma below is by induction. It goes fast over a subtle counting argument when reducing the problem in dimension $n+1$ to dimension n. We briefly recall the proof and give more explanations on the counting argument in Appendix A.2 of the full version.

▶ **Lemma 11** ([18, Thm. 5.2]). *For any n-dimensional lattice $\mathcal{L}$ and any vector $\mathbf{t} \in \mathbb{Q}^n$, we have $\#\mathcal{L} \cap \mathcal{B}(\mathbf{t}, \lambda_1(\mathcal{L})/\sqrt{2}) \le 2n$.*

We will use the above three lemmas in the following way to tackle BDD. Consider the coordinate vectors (with respect to some arbitrary basis) of all lattice vectors in $\mathcal{B}(\mathbf{t}, r)$ with $r = \lambda_1(\mathcal{L})/\sqrt{2}$ and some arbitrary target vector $\mathbf{t}$. First, according to Lemma 10 with $p > 2\sqrt{2}$, we can obtain that one of the coordinate vectors differs from all the others modulo p. Further, by Lemma 8, a uniformly chosen vector $\mathbf{z}$ over $\mathbb{Z}_p$ is orthogonal to exactly one of the coordinate vectors (shifted by another uniformly chosen vector $\mathbf{u}$) with non-negligible probability. Assume that this orthogonal coordinates vector is the coordinates vector of a closest lattice vector to $\mathbf{t}$: this occurs with non-negligible probability as $\#\mathcal{L} \cap \mathcal{B}(\mathbf{t}, r) \leq 2n$. We can consider the sublattice $\mathcal{L}_{p,\mathbf{z}}$, which contains just this BDD solution and none of the other vectors of $\mathcal{L} \cap \mathcal{B}(\mathbf{t}, r)$. This will help us ensuring a large gap between the first two minima of the uSVP lattice in the BDD to uSVP reduction.

Note that $\mathbf{u}$ is necessary, as otherwise some superfluous vectors (including vector $\mathbf{0}$) could be multiples of the solution vector and hence always stay in $\mathcal{L}_{p,\mathbf{z}}$ if the solution vector does.

3 Reducing $\mathrm{BDD}_{1/(\sqrt{2}\gamma)}$ to u$\mathrm{SVP}_{\gamma(1+\varepsilon)}$

In this section, we use a $\mathrm{uSVP}_{\gamma(1+\varepsilon)}$ solver with $\varepsilon = \Omega(1/n)$ to solve $\mathrm{BDD}_{1/(\sqrt{2}\gamma)}$.

▶ **Theorem 12.** *Let $\gamma(n) \leq \mathrm{poly}(n)$. There is a probabilistic polynomial-time reduction from $\mathrm{BDD}_{1/(\sqrt{2}\gamma)}$ to $\mathrm{uSVP}_{\gamma(1+\varepsilon)}$, where $\varepsilon = \Omega(1/n)$.*

Thanks to Lemma 5, it suffices to reduce $\mathrm{BDD}_{(1-1/n)/(\sqrt{2}\gamma)}$ to $\mathrm{uSVP}_{\gamma(1+\varepsilon)}$. Let us first describe the reduction.

Algorithm 1. The $\mathrm{BDD}_{(1-1/n)/(\sqrt{2}\gamma)}$ to $\mathrm{uSVP}_{\gamma(1+\varepsilon)}$ reduction.

Input: a basis $\mathbf{B} = \{\mathbf{b}_i\}_{i\in[n]}$ of an n-dimensional lattice $\mathcal{L} \subseteq \mathbb{Q}^n$, and a target point $\mathbf{t} \in \mathbb{Q}^n$.

Output: a lattice point $\mathbf{c}$ such that $\|\mathbf{c} - \mathbf{t}\| = \mathrm{dist}(\mathbf{t}, \mathcal{L})$.

0. Guess $d_0 \in [d, d/(1-1/n))$ and $\ell_0 \in [\ell, \ell/(1-1/n))$, where $d = \mathrm{dist}(\mathbf{t}, \mathcal{L})$ and $\ell = \lambda_1(\mathcal{L})$ (see Section 2.2).

1. Compute p the smallest prime greater than $4\gamma n^2$.
Sample $\mathbf{z}, \mathbf{u}$ uniformly and independently in $\mathbb{Z}_p^n$.
Compute $\mathbf{w} = \mathbf{B}\bar{\mathbf{u}} \in \mathcal{L}$, such that $\bar{\mathbf{u}} = \mathbf{u} \bmod p$ and $\|\mathbf{t} + \mathbf{w}\| \geq (n+1)\ell_0/\sqrt{2}$.
Use the algorithm of Lemma 9 to compute a basis $\mathbf{B}_{p,\mathbf{z}}$ of $\mathcal{L}_{p,\mathbf{z}} = \{\mathbf{b} \in \mathcal{L} : \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{b}\rangle = 0 \bmod p\}$.

2. Set $k = 1/(n-1)$. Define

$$\mathbf{B}' = \begin{pmatrix} \mathbf{B}_{p,\mathbf{z}} & \mathbf{t}+\mathbf{w} \\ \mathbf{0} & kd_0 \end{pmatrix}.$$

3. Run the $\mathrm{uSVP}_{\gamma(1+\varepsilon)}$ solver on input $\mathbf{B}'$. Let $\mathbf{s}' = ((\mathbf{s}'_1)^{\mathrm{T}}, s'_2)^{\mathrm{T}}$ be its output. Output $\mathbf{s}'_1 + \mathbf{t}$.

It may be checked that the above algorithm runs in polynomial time. The rest of the section is devoted to proving its correctness.

In this reduction, we are given a $\mathrm{BDD}_{(1-1/n)/(\sqrt{2}\gamma)}$ instance $(\mathbf{B}, \mathbf{t})$. Let $\mathbf{c} \in \mathcal{L}$ be a closest vector to $\mathbf{t}$. In order to construct a uSVP instance, our strategy is to use lattice sparsification to keep only one closest vector $\mathbf{c} + \mathbf{w}$ for some lattice shift $\mathbf{w}$ closest to $\mathbf{t} + \mathbf{w}$ (the shift vector $\mathbf{w}$ comes from Lemma 8). As the sparsification results in a lattice, we not only keep $\mathbf{c} + \mathbf{w}$, but also the $m \cdot (\mathbf{c} + \mathbf{w})$'s for all $m \leq \gamma n$. Simultaneously, all other vectors inside the balls with centers $\{m \cdot (\mathbf{t} + \mathbf{w})\}_{m\leq\gamma n}$ and radius $\lambda_1(\mathcal{L})/\sqrt{2}$ are regarded

as superfluous vectors and removed through sparsification. For the first γ balls, we have $m \cdot (\mathbf{c}+\mathbf{w}) \in \mathcal{B}(m \cdot (\mathbf{t}+\mathbf{w}), \lambda_1(\mathcal{L})/\sqrt{2})$. We can keep exactly one vector inside every ball with sparsification over these balls. However, for $m > \gamma$, all closest points to $\mathbf{t}$ may fall out of the corresponding ball, but may end up in another relevant ball: vector $i \cdot (\mathbf{c}+\mathbf{w})$ may belong to $\mathcal{B}(j \cdot (\mathbf{t}+\mathbf{w}), \lambda_1(\mathcal{L})/\sqrt{2})$ for some $j \neq i$. As a consequence, there can be more than one lattice vector inside a ball, which may result in no gap between first two minima of the uSVP oracle input lattice. In order to avoid this, we make every two balls far away from each other by choosing $\mathbf{w}$ such that $\mathbf{t}+\mathbf{w}$ is long.

▶ **Lemma 13.** *Consider a basis $\mathbf{B}$ of an n-dimensional lattice $\mathcal{L}$, a vector $\mathbf{c} \in \mathcal{L}$ and a vector $\mathbf{t} \in \mathbb{R}^n$ such that $\|\mathbf{c}-\mathbf{t}\| \leq r = \lambda_1(\mathcal{L})/(\sqrt{2}\gamma)$ for some $\gamma > 0$. Let p prime with $p \geq n+1$. For any $\mathbf{z} \in \mathbb{Z}_p^n$, We have*

$$\Pr_{\mathbf{u},\mathbf{z} \hookleftarrow U(\mathbb{Z}_p^n)} \left[\begin{array}{ccc} \mathbf{c}+\mathbf{w} & \in & \mathcal{L}_{p,\mathbf{z}} \cap \mathcal{B}(\mathbf{t}+\mathbf{w}, \gamma \cdot r) \\ \mathbb{Z} \cdot (\mathbf{c}+\mathbf{w}) & \supseteq & \mathcal{L}_{p,\mathbf{z}} \cap \bigcup\limits_{i \leq \gamma n} \mathcal{B}(i \cdot (\mathbf{t}+\mathbf{w}), \gamma \cdot r) \end{array} \right] \geq \frac{1}{p} - \frac{N}{p^2} - \frac{N}{p^{n-1}},$$

where $\mathbf{w}$ is arbitrary such that $\mathbf{B}^{-1}\mathbf{w} = \mathbf{u} \bmod p$ and $N = \#\mathcal{L} \cap \cup_{i \leq \gamma n} \mathcal{B}(i \cdot (\mathbf{t}+\mathbf{w}), \gamma \cdot r)$.

Further, if $\mathbf{w}$ is chosen such that $\|\mathbf{t}+\mathbf{w}\| > \gamma(n+1)r$, we have, for all $i \in [\gamma n]$,

$$i \cdot (\mathbf{c}+\mathbf{w}) \notin \bigcup_{j \neq i, j \in [\gamma n]} \mathcal{B}\left(j \cdot (\mathbf{t}+\mathbf{w}), \gamma \cdot r\right).$$

Proof. For $i \in [\gamma n]$, we define $N_i = \#\mathcal{L} \cap \mathcal{B}(i \cdot \mathbf{t}, \gamma \cdot r) \setminus \{i \cdot \mathbf{c}\}$ and $\{\mathbf{v}_{ij}\}_{j \in [N_i]} = (\mathcal{L} \cap \mathcal{B}(i \cdot \mathbf{t}, \gamma \cdot r)) \setminus \{i \cdot \mathbf{c}\}$. For any $\mathbf{v} \in \mathcal{L}$, we use $\widetilde{\mathbf{v}}$ to denote the coordinate of $\mathbf{v}$ under the basis $\mathbf{B}$. We claim that, with probability $\geq 1/p - N/p^2 - N/p^{n-1}$, the vector $\mathbf{z}$ is orthogonal (modulo p) to $\widetilde{\mathbf{c}}$, and at the same time not orthogonal to any $\widetilde{\mathbf{v}}_{ij}$ for $i \in [\gamma n]$ and $j \in [N_i]$.

We have, for all $i \in [\gamma n]$ and $j \in [N_i]$,

$$\|i \cdot \mathbf{c} - \mathbf{v}_{ij}\| \leq i \cdot \|\mathbf{c}-\mathbf{t}\| + \|i \cdot \mathbf{t} - \mathbf{v}_{ij}\| \leq (n+1)(\gamma r) = \frac{n+1}{\sqrt{2}} \cdot \lambda_1(\mathcal{L}).$$

By choice of p, this is smaller than $p \cdot \lambda_1(\mathcal{L})$. Thanks to Lemma 10, we have $i \cdot \widetilde{\mathbf{c}} \neq \widetilde{\mathbf{v}}_{ij} \bmod p$. Moreover, as p is prime and $p \geq \gamma n + 1 > i$, we have $\widetilde{\mathbf{c}} \neq \frac{1}{i} \cdot \widetilde{\mathbf{v}}_{ij} \bmod p$.

Now we apply Lemma 8 with $\widetilde{\mathbf{c}}$ and $\{\frac{1}{i} \cdot \widetilde{\mathbf{v}}_{ij}\}_{i \in [\gamma n], j \in [N_i]}$. We have

$$\Pr_{\mathbf{z},\mathbf{u} \hookleftarrow U(\mathbb{Z}_p^n)} \left[\begin{array}{lcl} \forall i,j: & \langle \mathbf{z}, \frac{1}{i} \cdot \widetilde{\mathbf{v}}_{ij} + \mathbf{u} \rangle & \neq 0 \bmod p \\ & \langle \mathbf{z}, \widetilde{\mathbf{c}} + \mathbf{u} \rangle & = 0 \bmod p \end{array} \right] \geq \frac{1}{p} - \frac{N}{p^2} - \frac{N}{p^{n-1}}.$$

As p is prime and sufficiently large, the inequality $\langle \mathbf{z}, \frac{1}{i} \cdot \widetilde{\mathbf{v}}_{ij} + \mathbf{u} \rangle \neq 0 \bmod p$ is equivalent to $\langle \mathbf{z}, \widetilde{\mathbf{v}}_{ij} + i \cdot \mathbf{u} \rangle \neq 0 \bmod p$. Therefore

$$\Pr_{\mathbf{z},\mathbf{u} \hookleftarrow U(\mathbb{Z}_p^n)} \left[\begin{array}{lcl} \forall i,j: & \langle \mathbf{z}, \widetilde{\mathbf{v}}_{ij} + i \cdot \mathbf{u} \rangle & \neq 0 \bmod p \\ & \langle \mathbf{z}, \widetilde{\mathbf{c}} + \mathbf{u} \rangle & = 0 \bmod p \end{array} \right] \geq \frac{1}{p} - \frac{N}{p^2} - \frac{N}{p^{n-1}}.$$

This proves the first claim of the lemma.

Let $i \neq j \leq \gamma n$. Then, by the triangle inequality and the assumption on $\mathbf{w}$, we have:

$$\|i \cdot (\mathbf{c}+\mathbf{w}) - j \cdot (\mathbf{t}+\mathbf{w})\| \geq |j-i| \cdot \|\mathbf{t}+\mathbf{w}\| - i\|\mathbf{c}-\mathbf{t}\| > \gamma(n+1)r - (\gamma n)r = \gamma r.$$

This completes the proof of the lemma. ◀

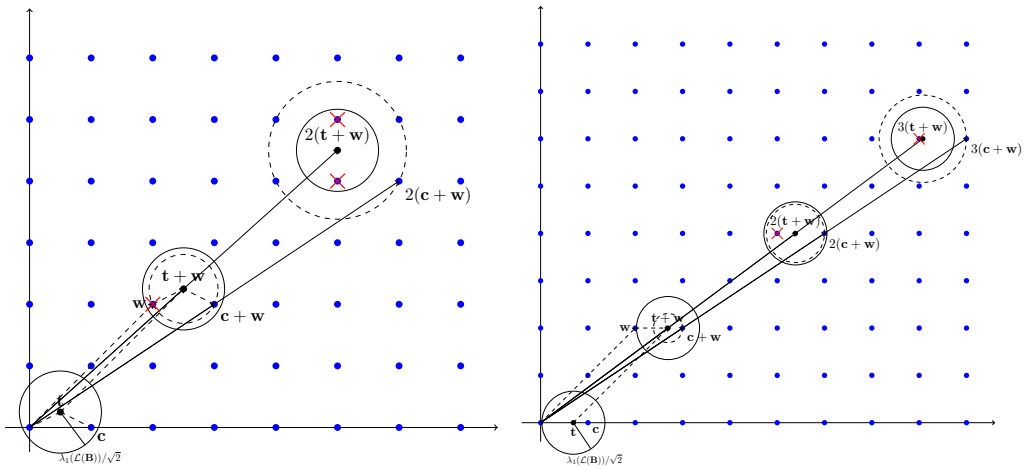

Figure 3 Sparsification for a $\mathrm{BDD}_{1/\sqrt{2}}$ instance (left) and for a $\mathrm{BDD}_{1/(2\sqrt{2})}$ instance (right).

As we have $p > 4\gamma n^2 \geq 2N$ (thanks to Lemma 11), with non-negligible probability, none of the vectors of $\mathcal{L}$ belonging to the γn balls is in the sparser lattice $\mathcal{L}_{p,\mathbf{z}}$, except possibly those in $\{i \cdot (\mathbf{c}+\mathbf{w})\}_{i\in[\gamma n]}$. In the rest of the reduction analysis, we assume that we are in this situation and do not repeatedly state that this occurs with non-negligible probability.

As an illustration of Lemma 13, we include Figure 3. In the case of $\gamma = 1$ (left subfigure), there are several plain balls with radius $\lambda_1(\mathcal{L})$, centered in $\mathbf{t}$, $\mathbf{t}+\mathbf{w}$ and $2(\mathbf{t}+\mathbf{w})$. The dashed balls illustrate the distance between $i \cdot (\mathbf{c}+\mathbf{w})$ and $i \cdot (\mathbf{t}+\mathbf{w})$ for all $i \in [\gamma n]$. We can see that $\mathbf{c}+\mathbf{w}$ (within the dashed ball) is inside the plain ball, and $2 \cdot (\mathbf{c}+\mathbf{w})$ (within the dashed ball) is outside of its corresponding plain ball. Similarly, in the case of $\gamma = 2$ (right subfigure), vector $i \cdot (\mathbf{c}+\mathbf{w})$ is outside of its corresponding plain ball only when $i > 2$. Note in particular that in the case of $\gamma = 2$, vector $\mathbf{0}$ is not the closest point to the target vector, but belongs to the plain ball with center $\mathbf{t}$. Thus vector $\mathbf{0}$ should be removed via sparsification. As it is kept in any sparsified lattice, this is impossible to achieve. This illustrates why center $\mathbf{t}$ is shifted to a new point $\mathbf{t}+\mathbf{w}$ (then the shift $\mathbf{w}$ of $\mathbf{0}$ may be removed via sparsification). In both figures, the red crosses denote the points that are removed from the lattice via sparsification.

In Step 2 of the reduction, we construct a basis $\mathbf{B}'$ of an $(n+1)$-dimensional lattice $\mathcal{L}'$ by using Kannan's embedding technique. In Step 3, we call the $\mathrm{uSVP}_{\gamma(1+\varepsilon)}$ oracle with input basis $\mathbf{B}'$. The correctness of the reduction is provided by Lemmata 14, 15 and 16.

Any vector in lattice $\mathcal{L}'$ can be written as $\mathbf{b}' = ((\mathbf{b}+m(\mathbf{t}+\mathbf{w}))^{\mathrm{T}}, mkd_0)^{\mathrm{T}}$ with $\mathbf{b} \in \mathcal{L}_{p,\mathbf{z}}$ and $m \in \mathbb{Z}$. We claim that the vector $\mathbf{s}' = (((\mathbf{c}+\mathbf{w})-(\mathbf{t}+\mathbf{w}))^{\mathrm{T}}, -kd_0)^{\mathrm{T}} = ((\mathbf{c}-\mathbf{t})^{\mathrm{T}}, -kd_0)^{\mathrm{T}}$ is a shortest non-zero vector in $\mathcal{L}'$ and also that $\lambda_2(\mathcal{L}')/\lambda_1(\mathcal{L}') = \gamma(1+\Omega(1/n))$. Thus $\pm\mathbf{s}'$ will be output by the $\mathrm{uSVP}_{\gamma(1+\varepsilon)}$ oracle. We can then obtain the vector $\mathbf{c} = (\mathbf{c}+\mathbf{w})-(\mathbf{t}+\mathbf{w})+\mathbf{t} \in \mathcal{L}$. In the following, we give lower bounds for the norm of $\mathbf{b}' = ((\mathbf{b}+m(\mathbf{t}+\mathbf{w}))^{\mathrm{T}}, mkd_0)^{\mathrm{T}}$ not parallel to $\mathbf{s}'$, which depend on the value of m. Without loss of generality, we restrict ourselves to $m \geq 0$.

The following lemma is analogous to the '$m = 0$ case' of the Lyubashevsky-Micciancio reduction [15]. Note that the lower bound in the statement is essentially $2\gamma^2$.

▶ **Lemma 14.** *If $m = 0$ and $\mathbf{b}' \neq \mathbf{0}$, then $\|\mathbf{b}'\|^2/\|\mathbf{s}'\|^2 \geq 2\gamma^2/(1+1/(n-1)^2)$.*

Proof. As $m = 0$ and $\mathbf{b}' \neq \mathbf{0}$, we must have $\mathbf{b} \neq \mathbf{0}$. As a result, we have

$$\|\mathbf{b}'\|^2 \;=\; \|\mathbf{b}\|^2 \;\geq\; \lambda_1^2(\mathcal{L}) \;\geq\; \frac{2\gamma^2 d^2}{(1-\frac{1}{n})^2} \;\geq\; 2\gamma^2 d_0^2.$$

Thus, in this case, we have the gap

$$\frac{\|\mathbf{b}'\|^2}{\|\mathbf{s}'\|^2} \geq \frac{2\gamma^2 d_0^2}{d^2 + d_0^2 k^2} \geq \frac{2\gamma^2}{1+k^2} = \frac{2\gamma^2}{1+\frac{1}{(n-1)^2}}.$$

◀

The second lemma bounds the gap for small m's. It is where our improvement over prior reductions stems from. Note that the lower bound in the statement is essentially γ^2.

▶ **Lemma 15.** *If $m \leq \gamma n$ and $\mathbf{b}'$ is linearly independent with $\mathbf{s}'$, then $\|\mathbf{b}'\|^2/\|\mathbf{s}'\|^2 \geq (\gamma^2 + 1/n^2)/((1-1/n)^2 + 1/(n-1)^2)$.*

Proof. By Lemma 13, we have

$$\mathbf{c} + \mathbf{w} \;\in\; \mathcal{L}_{p,\mathbf{z}} \bigcap \bigcup_{i \leq \gamma n} \mathcal{B}\left(i \cdot (\mathbf{t}+\mathbf{w}), \frac{\lambda_1(\mathcal{L})}{\sqrt{2}}\right) \;\subseteq\; \mathbb{Z} \cdot (\mathbf{c}+\mathbf{w}).$$

Thus, as $\mathbf{b} \notin \mathbb{Z} \cdot (\mathbf{c}+\mathbf{w})$ (by assumption), we have

$$\|\mathbf{b}'\|^2 = \|\mathbf{b} - m \cdot (\mathbf{t}+\mathbf{w})\|^2 + m^2 d_0^2 k^2 \geq \frac{\lambda_1^2(\mathcal{L})}{2} + m^2 d_0^2 k^2 \geq \left(\frac{d\gamma}{1-\frac{1}{n}}\right)^2 + m^2 d_0^2 k^2.$$

Thus, in this case, we have the gap

$$\frac{\|\mathbf{b}'\|^2}{\|\mathbf{s}'\|^2} \geq \frac{(\frac{d\gamma}{1-\frac{1}{n}})^2 + m^2 d_0^2 k^2}{d^2 + d_0^2 k^2} \geq \frac{(\frac{d\gamma}{1-\frac{1}{n}})^2 + m^2 d^2 k^2}{d^2 + (\frac{d}{1-\frac{1}{n}})^2 k^2} = \frac{\gamma^2 + \frac{m^2}{n^2}}{(1-\frac{1}{n})^2 + \frac{1}{(n-1)^2}}.$$

The gap is an increasing function in m and hence it suffices to consider $m = 1$. ◀

The third lemma bounds the gap for larger m's. This corresponds to the 'large m case' of the Lyubashevsky-Micciancio reduction. As in the previous case, the lower bound in the statement is essentially γ^2.

▶ **Lemma 16.** *If $m > \gamma n$, then $\|\mathbf{b}'\|^2/\|\mathbf{s}'\|^2 \geq \gamma^2/((1-1/n)^2 + 1/(n-1)^2)$.*

Proof. For any $\mathbf{b} \in \mathcal{L}$, we have $\|\mathbf{b}'\|^2 \geq m^2 k^2 d_0^2$. Thus, in this case, we have the gap

$$\frac{\|\mathbf{b}'\|^2}{\|\mathbf{s}'\|^2} \geq \frac{m^2 k^2 d_0^2}{d^2 + k^2 d_0^2} \geq \frac{m^2 k^2 d^2}{d^2 + (\frac{d}{1-\frac{1}{n}})^2 k^2} = \frac{m^2}{(n-1)^2 + \frac{n}{(n-1)^2}}.$$

The gap is an increasing function in m and hence it suffices to consider the $m = \gamma n$. ◀

Now, we complete the proof of Theorem 12. According to Lemmata 14, 15 and 16, the uSVP gap satisfies, for large enough n

$$\frac{\lambda_2^2(\mathcal{L}')}{\lambda_1^2(\mathcal{L}')} \geq \min\left(\frac{2\gamma^2}{1+\frac{1}{(n-1)^2}}, \frac{\gamma^2+\frac{1}{n^2}}{(1-\frac{1}{n})^2+\frac{1}{(n-1)^2}}, \frac{\gamma^2}{(1-\frac{1}{n})^2+\frac{1}{(n-1)^2}}\right) \geq \gamma^2\left(1 + \Omega\left(\frac{1}{n}\right)\right).$$

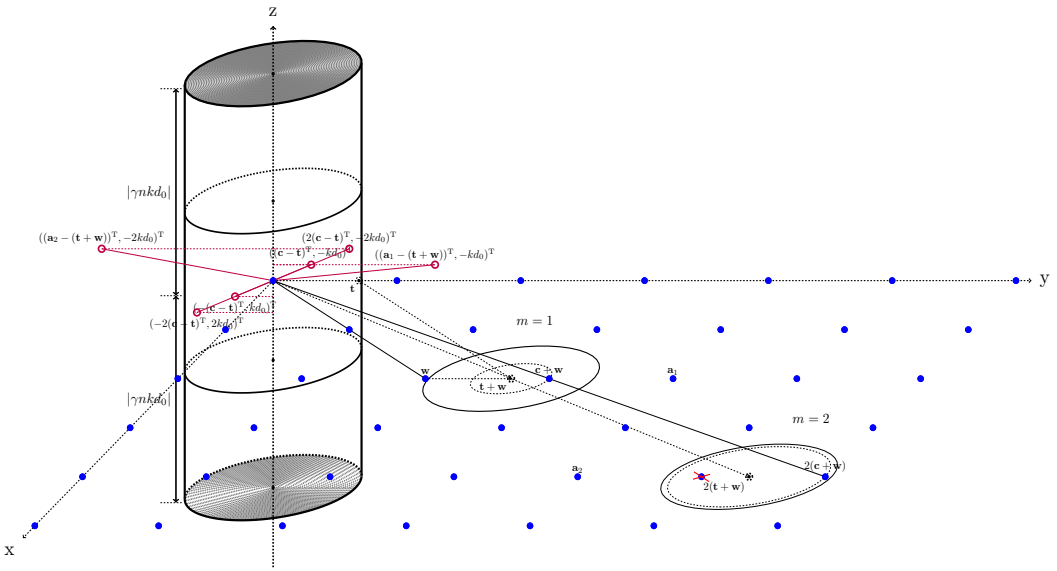

Figure 4 Geometric illustration of the reduction.

We include Figure 4 to geometrically illustrate the overall reduction. For convenience, we take $k = -1/(n-1)$ in the figure. We use filled dots to label points of 2-dimensional lattice $\mathcal{L}$, and hollow dots to label points of 3-dimensional lattice $\mathcal{L}'$ that are not in $\mathcal{L}$ (recall that $\mathcal{L} \subseteq \mathcal{L}'$). With Kannan's embedding technique, the offset between the vectors of $\mathcal{L}$ (e.g., $\mathbf{c}+\mathbf{w}$) and the shifted target $\mathbf{t}+\mathbf{w}$ are mapped to $\mathcal{L}'$ (e.g., $((\mathbf{c}-\mathbf{t})^{\mathrm{T}}, -kd_0)^{\mathrm{T}}$). Thanks to sparsification, all the points of $\mathcal{L}'$ belonging to the drawn cylinder (of height $|2\gamma nkd_0|$) are multiples of the shortest non-zero vector $\mathbf{s}' = ((\mathbf{c}-\mathbf{t})^{\mathrm{T}}, -kd_0)^{\mathrm{T}}$, e.g., $\pm((\mathbf{c}-\mathbf{t})^{\mathrm{T}}, -kd_0)^{\mathrm{T}}$ and $\pm(2(\mathbf{c}-\mathbf{t})^{\mathrm{T}}, -2kd_0)^{\mathrm{T}}$. All other points in $\mathcal{L}'$ that are linearly independent from $\mathbf{s}'$ lie outside of the cylinder, e.g., $((\mathbf{a}_1-(\mathbf{t}+\mathbf{w}))^{\mathrm{T}}, -kd_0)^{\mathrm{T}}$ and $((\mathbf{a}_2-(\mathbf{t}+\mathbf{w}))^{\mathrm{T}}, -2kd_0)^{\mathrm{T}}$. This cylinder forces the second minimum $\lambda_2(\mathcal{L}')$ to be large, and, more concretely, larger than $\gamma\lambda_1(\mathcal{L}')$. This corresponds to Lemma 15 (Lemma 14 handles the points of $\mathcal{L}$ and Lemma 16 handles the points of $\mathcal{L}'$ whose z-component is large).

Acknowledgments. We thank Steven Galbraith, Daniele Micciancio and Jinming Wen for helpful discussions.

References

1 M. Ajtai. The shortest vector problem in l_2 is NP-hard for randomized reductions (extended abstract). In *Proc. of STOC*, pages 284–293. ACM, 1998.
2 L. Babai. On Lovász lattice reduction and the nearest lattice point problem. *Combinatorica*, 6:1–13, 1986.
3 S. Bai and S. Galbraith. Private communication, 2015.
4 D. Dadush and G. Kun. Lattice sparsification and the approximate closest vector problem. In *Proc. of SODA*, pages 1088–1102. SIAM, 2013.
5 D. Dadush, O. Regev, and N. Stephens-Davidowitz. On the closest vector problem with a distance guarantee. In *Proc. of CCC*, pages 98–109. IEEE Computer Society Press, 2014.
6 R. de Buda. The upper error bound of a new near-optimal code. *IEEE Trans. on Information Theory*, 21(4):441–445, 1975.

7 U. Fincke and M. Pohst. A procedure for determining algebraic integers of given norm. In *Proc. of EUROCAL*, volume 162 of *LNCS*, pages 194–202, 1983.

8 R. Kannan. Improved algorithms for integer programming and related lattice problems. In *Proc. of STOC*, pages 99–108. ACM, 1983.

9 R. Kannan. Minkowski's convex body theorem and integer programming. *Math. Oper. Res.*, 12(3):415–440, 1987.

10 S. Khot. Hardness of approximating the shortest vector problem in high L_p norms. In *Proc. of FOCS*, pages 290–297. IEEE Computer Society Press, 2003.

11 S. Khot. Hardness of approximating the shortest vector problem in lattices. *J. ACM*, 52(5):789–808, 2005.

12 A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann*, 261:515–534, 1982.

13 M. Liu, X. Wang, G. Xu, and X. Zheng. A note on BDD problems with λ_2-gap. *Inf. Process. Lett.*, 114(1-2):9–12, January 2014.

14 Y. K. Liu, V. Lyubashevsky, and D. Micciancio. On bounded distance decoding for general lattices. In *Proc. of RANDOM*, volume 4110 of *LNCS*, pages 450–461. Springer, 2006.

15 V. Lyubashevsky and D. Micciancio. On bounded distance decoding, unique shortest vectors, and the minimum distance problem. In *Proc. of CRYPTO*, pages 577–594, 2009.

16 D. Micciancio. The shortest vector problem is NP-hard to approximate to within some constant. *SIAM J. Comput*, 30(6):2008–2035, 2001.

17 D. Micciancio. Private communication, 2015.

18 D. Micciancio and S. Goldwasser. *Complexity of Lattice problem: A Cryptography Perspective*. Kluwer, 2009.

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

20 C. P. Schnorr. A hierarchy of polynomial lattice basis reduction algorithms. *Theor. Comput. Science*, 53:201–224, 1987.

21 N. Stephens-Davidowitz. Discrete Gaussian sampling reduces to CVP and SVP. In *Proc. of SODA*, pages 1748–1764. SIAM, 2016.

22 A. Vardy. Algorithmic complexity in coding theory and the minimum distance problem. In *Proc. of STOC*, pages 92–109. ACM, 1997.