

Improved Hardness of BDD and SVP Under Gap-(S)ETH

Huck Bennett ✉

Oregon State University, Corvallis, OR, USA

Chris Peikert ✉

University of Michigan, Ann Arbor, MI, USA

Yi Tang ✉

University of Michigan, Ann Arbor, MI, USA

Abstract

We show improved fine-grained hardness of two key lattice problems in the ℓ_p norm: Bounded Distance Decoding to within an α factor of the minimum distance ($\text{BDD}_{p,\alpha}$) and the (decisional) γ -approximate Shortest Vector Problem ($\text{SVP}_{p,\gamma}$), assuming variants of the Gap (Strong) Exponential Time Hypothesis (Gap-(S)ETH). Specifically, we show:

1. For all $p \in [1, \infty)$, there is no $2^{o(n)}$ -time algorithm for $\text{BDD}_{p,\alpha}$ for any constant $\alpha > \alpha_{\text{kn}}$, where $\alpha_{\text{kn}} = 2^{-c_{\text{kn}}} < 0.98491$ and c_{kn} is the ℓ_2 kissing-number constant, unless non-uniform Gap-ETH is false.
2. For all $p \in [1, \infty)$, there is no $2^{o(n)}$ -time algorithm for $\text{BDD}_{p,\alpha}$ for any constant $\alpha > \alpha_p^\dagger$, where α_p^\dagger is explicit and satisfies $\alpha_p^\dagger = 1$ for $1 \leq p \leq 2$, $\alpha_p^\dagger < 1$ for all $p > 2$, and $\alpha_p^\dagger \rightarrow 1/2$ as $p \rightarrow \infty$, unless randomized Gap-ETH is false.
3. For all $p \in [1, \infty) \setminus 2\mathbb{Z}$ and all $C > 1$, there is no $2^{n/C}$ -time algorithm for $\text{BDD}_{p,\alpha}$ for any constant $\alpha > \alpha_{p,C}^\dagger$, where $\alpha_{p,C}^\dagger$ is explicit and satisfies $\alpha_{p,C}^\dagger \rightarrow 1$ as $C \rightarrow \infty$ for any fixed $p \in [1, \infty)$, unless non-uniform Gap-SETH is false.
4. For all $p > p_0 \approx 2.1397$, $p \notin 2\mathbb{Z}$, and all $C > C_p$, there is no $2^{n/C}$ -time algorithm for $\text{SVP}_{p,\gamma}$ for some constant $\gamma > 1$, where $C_p > 1$ is explicit and satisfies $C_p \rightarrow 1$ as $p \rightarrow \infty$, unless randomized Gap-SETH is false.

Our results for $\text{BDD}_{p,\alpha}$ improve and extend work by Aggarwal and Stephens-Davidowitz (STOC, 2018) and Bennett and Peikert (CCC, 2020). Specifically, the quantities α_{kn} and α_p^\dagger (respectively, $\alpha_{p,C}^\dagger$) significantly improve upon the corresponding quantity α_p^* (respectively, $\alpha_{p,C}^*$) of Bennett and Peikert for small p (but arise from somewhat stronger assumptions). In particular, Item 1 improves the smallest value of α for which $\text{BDD}_{p,\alpha}$ is known to be exponentially hard in the Euclidean norm ($p = 2$) to an explicit constant $\alpha < 1$ for the first time under a general-purpose complexity assumption. Items 1 and 3 crucially use the recent breakthrough result of Vlăduț (Moscow Journal of Combinatorics and Number Theory, 2019), which showed an explicit exponential lower bound on the lattice kissing number. Finally, Item 4 answers a natural question left open by Aggarwal, Bennett, Golovnev, and Stephens-Davidowitz (SODA, 2021), which showed an analogous result for the Closest Vector Problem.¹

2012 ACM Subject Classification Theory of computation \rightarrow Problems, reductions and completeness; Theory of computation \rightarrow Computational geometry

Keywords and phrases lattices, lattice-based cryptography, fine-grained complexity, Bounded Distance Decoding, Shortest Vector Problem

Digital Object Identifier 10.4230/LIPIcs.ITCS.2022.19

Related Version *Full Version:* <https://arxiv.org/abs/2109.04025>

¹ We strongly encourage readers to view the full version of this paper, which contains all missing definitions, proofs, and details, at <https://arxiv.org/abs/2109.04025>. Due to space constraints, this version of the paper essentially just contains the introduction of the full version.



© Huck Bennett, Chris Peikert, and Yi Tang;

licensed under Creative Commons License CC-BY 4.0

13th Innovations in Theoretical Computer Science Conference (ITCS 2022).

Editor: Mark Braverman; Article No. 19; pp. 19:1–19:12

Leibniz International Proceedings in Informatics



LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Funding This material is based upon work supported by the National Science Foundation under Award CCF-2006857. The views expressed are those of the authors and do not necessarily reflect the official policy or position of the National Science Foundation.

Acknowledgements We thank Noah Stephens-Davidowitz for helpful comments.

1 Introduction

Lattices are geometric objects that look like regular orderings of points in real space. More formally, a lattice \mathcal{L} is the set of all integer linear combinations of some linearly independent vectors $\mathbf{b}_1, \dots, \mathbf{b}_n \in \mathbb{R}^m$. The matrix $B = (\mathbf{b}_1, \dots, \mathbf{b}_n)$ whose columns are these vectors is called a *basis* of \mathcal{L} , and we denote the lattice it generates by $\mathcal{L}(B)$, i.e., $\mathcal{L} = \mathcal{L}(B) := \{\sum_{i=1}^n a_i \mathbf{b}_i : a_1, \dots, a_n \in \mathbb{Z}\}$. The number of vectors n in a basis is an invariant of \mathcal{L} , and is called its *rank*.

In recent years, lattices have played a central role in both cryptanalysis and the design of secure cryptosystems. One very attractive quality of many lattice-based cryptosystems (e.g., [4, 5, 22, 23, 11]) is that they are secure assuming that certain key lattice problems are sufficiently hard to approximate in the *worst case*. Motivated by this and myriad other applications of lattices in computer science, many works have studied the NP-hardness of both exact and approximate lattice problems (e.g., [25, 6, 4, 18, 19, 14, 13, 15, 12, 20]). More recently, motivated especially by the need to understand the *concrete* security of lattice-based cryptosystems, a number of works [8, 3, 9, 2, 1] have studied the *fine-grained* complexity of lattice problems. That is, for a meaningful real-world security bound, it is not enough to say merely that there is no *polynomial-time* algorithm for a suitable lattice problem. Rather, a key goal is to show $2^{\Omega(n)}$ -hardness, or even 2^{Cn} -hardness for some explicit $C > 0$, of a problem under general-purpose complexity-theoretic assumptions, like variants of the (Strong) Exponential Time Hypothesis.

In this work, we extend the latter line of research by showing improved fine-grained complexity results for two key lattice problems, the Bounded Distance Decoding Problem (BDD) and the Shortest Vector Problem (SVP). To define these problems, we first recall some notation. Let $\lambda_1(\mathcal{L}) := \min_{\mathbf{v} \in \mathcal{L} \setminus \{0\}} \|\mathbf{v}\|$ denote the *minimum distance* of \mathcal{L} , i.e., the length of a shortest non-zero vector in \mathcal{L} , and let $\text{dist}(\mathbf{t}, \mathcal{L}) := \min_{\mathbf{v} \in \mathcal{L}} \|\mathbf{t} - \mathbf{v}\|$ denote the distance between a target vector \mathbf{t} and \mathcal{L} . When using the ℓ_p norm, we denote these quantities by $\lambda_1^{(p)}(\mathcal{L})$ and $\text{dist}_p(\mathbf{t}, \mathcal{L})$, respectively.

BDD and SVP

The Bounded Distance Decoding Problem in the ℓ_p norm for relative distance α , denoted $\text{BDD}_{p,\alpha}$, is the search promise problem defined as follows: given a basis B of a lattice $\mathcal{L} = \mathcal{L}(B)$ and a target vector \mathbf{t} satisfying $\text{dist}_p(\mathbf{t}, \mathcal{L}) \leq \alpha \cdot \lambda_1^{(p)}(\mathcal{L})$ as input, the goal is to find a closest lattice vector $\mathbf{v} \in \mathcal{L}$ to the target vector \mathbf{t} such that $\|\mathbf{t} - \mathbf{v}\|_p = \text{dist}_p(\mathbf{t}, \mathcal{L})$. (We note that \mathbf{v} is guaranteed to be unique when $\alpha < 1/2$, but that $\text{BDD}_{p,\alpha}$ is well-defined for any $\alpha = \alpha(n) > 0$.) The γ -approximate Shortest Vector Problem in the ℓ_p norm, denoted $\text{SVP}_{p,\gamma}$, is the decision promise problem defined as follows: given a basis B of a lattice $\mathcal{L} = \mathcal{L}(B)$ and a distance threshold $r > 0$ as input, the goal is to decide whether $\lambda_1^{(p)}(\mathcal{L}) \leq r$ (i.e., the input is a YES instance) or $\lambda_1^{(p)}(\mathcal{L}) > \gamma r$ (i.e., the input is a NO instance), with the promise that one of the two cases holds.²

² In other literature, this decision problem is often called $\text{GapSVP}_{p,\gamma}$, whereas $\text{SVP}_{p,\gamma}$ usually denotes the corresponding *search* problem (of finding a nonzero lattice vector $\mathbf{v} \in \mathcal{L}$ for which $\|\mathbf{v}\| \leq \gamma \cdot \lambda_1^{(p)}(\mathcal{L})$),

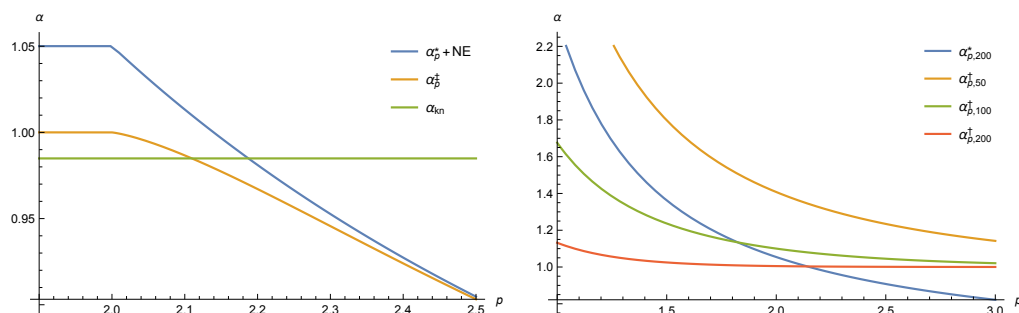


Figure 1 Plots showing the smallest relative distance α for which fine-grained hardness of $\text{BDD}_{p,\alpha}$ is known under variants of the (Strong) Exponential Time Hypothesis ((S)ETH); smaller α corresponds to stronger hardness results. The left plot shows the smallest values of α for which $2^{\Omega(n)}$ -hardness is known under variants of ETH; α_{kn} and α_p^\ddagger are from this work, and “ $\alpha_p^* + \text{NE}$ ” – α_p^* with norm embeddings – is from [9]. The right plot shows the smallest values of α for which $2^{n/C}$ -hardness is known under variants of SETH; $\alpha_{p,C}^\dagger$ is from this work and $\alpha_{p,C}^*$ is from [9]. The hardness results for the right plot only hold for $p \notin 2\mathbb{Z}$ due to a limitation in an “upstream” hardness result from [1], which in particular precludes using norm embeddings. (The curves for $\alpha_{p,50}^*$, $\alpha_{p,100}^*$, and $\alpha_{p,200}^*$ are essentially indistinguishable at the plot scale, so we include only $\alpha_{p,200}^*$.)

Although it seems far out of reach using known techniques, proving that $\text{SVP}_{p,\gamma}$ is hard for a sufficiently large polynomial approximation factor $\gamma = \gamma(n)$, or that $\text{BDD}_{p,\alpha}$ is hard for sufficiently small inverse-polynomial relative distance $\alpha = \alpha(n)$, would imply the provable security of lattice-based cryptography.³ On the other hand, most concrete security estimates for lattice-based cryptosystems are based on the runtimes of the fastest known (possibly heuristic) algorithms for exact or near-exact SVP. So, apart from its inherent theoretical interest, understanding the fine-grained complexity of (near-)exact SVP and BDD sheds light on questions of great practical importance.

2 Our Results

In this work, we show improved fine-grained hardness of $\text{BDD}_{p,\alpha}$ and $\text{SVP}_{p,\gamma}$, with an emphasis on results for smaller relative distance α and larger approximation factor γ , and on analyzing the complexity of the problems as the underlying ℓ_p norm varies. (We note that $\text{BDD}_{p,\alpha'}$ trivially reduces to $\text{BDD}_{p,\alpha}$ when $\alpha' < \alpha$, and so showing hardness results for $\text{BDD}_{p,\alpha}$ for smaller α is showing something stronger.)

At a conceptual level, our work gives very general reductions to BDD (presented in Theorem 3.4 in the full version), which reduce the task of showing hardness for BDD to analyzing properties of certain gadget lattices (described in Section 3.1). The few known hardness results for BDD (essentially just [15, 9] and this work) are all shown using this gadget lattice framework, but the previous works required separate reductions. The reductions in this work give a unified way to show hardness results using this framework.

given an arbitrary lattice \mathcal{L} .) There is a trivial reduction from the decision problem to the search problem, so any hardness of the former implies identical hardness of the latter.

³ We note that the relative distance α in $\text{BDD}_{p,\alpha}$ is not an approximation factor *per se*, but it is analogous to one in a precise sense. Namely, for $p = 2$ there is a rank-preserving reduction from $\text{BDD}_{2,\alpha}$ to $\text{SVP}_{2,\gamma}$ with $\gamma = O(1/\alpha)$ [16, 7], so sufficiently strong (fine-grained) hardness of the former problem translates to corresponding hardness for the latter problem. A similar reduction holds in reverse, but with a larger loss: $\alpha = \Omega(\sqrt{n/\log n/\gamma})$.

At a technical level, our improved results for BDD follow from improved analysis of the techniques used in [3] and [9] together with our new framework. Aggarwal and Stephens-Davidowitz [3] presented three main results on the fine-grained hardness of SVP, summarized in Items 1 to 3 in its abstract. Bennett and Peikert [9] showed new hardness results for BDD by refining and adapting the analysis used to show [3], Item 1. Analogously, in this work we obtain two of our hardness results for BDD by refining and adapting the analysis used to show [3], Items 2 and 3. Specifically, Theorem 1 corresponds to [3], Item 3 and Theorem 2 to [3], Item 2. Our third hardness result for BDD, presented in Theorem 3, uses ideas from the other reductions together with our new framework. Finally, our improved result for SVP, presented in Theorem 4, answers a natural question left open by [3, 1].

Our results assume (randomized or non-uniform) “gap” variants of the Exponential Time Hypothesis (ETH) and Strong Exponential Time Hypothesis (SETH). Recall that “plain” ETH asserts that solving the 3-SAT problem on n variables requires $2^{\Omega(n)}$ time, and “plain” SETH asserts that for every $\varepsilon > 0$ there exists $k \in \mathbb{Z}^+$ such that solving the k -SAT problem on n variables requires $2^{(1-\varepsilon)n}$ -time. The gap variants of these assumptions hypothesize that similar runtime lower bounds hold even for approximating the number of satisfiable clauses in a k -SAT formula to within some small constant approximation factor; see Section 2.5 in the full version for the precise definitions. We sometimes informally use the terminology “(Gap-)ETH-hardness” to denote $2^{\Omega(n)}$ -hardness of a problem assuming a variant of (Gap-)ETH, and “(Gap-)SETH-hardness” to denote 2^{cn} -hardness of a problem assuming a variant of (Gap-)SETH for some explicit constant $c > 0$.

2.1 Hardness for BDD

Our first result shows improved exponential hardness of $\text{BDD}_{p,\alpha}$ for all sufficiently small values of p , including the important Euclidean case of $p = 2$, assuming a variant of Gap-ETH (see the left plot in Figure 1). Indeed, it improves the smallest value of α for which exponential hardness of $\text{BDD}_{2,\alpha}$ is known under a general-purpose complexity-theoretic assumption to $\alpha < 0.98491$, showing such hardness for an explicit⁴ constant less than the $\alpha = 1$ threshold for the first time.⁵

► **Theorem 1** (Gap-ETH-hardness of BDD, first bound). *For all $p \in [1, \infty)$, there is no $2^{o(n)}$ -time algorithm for $\text{BDD}_{p,\alpha}$ for any constant $\alpha > \alpha_{\text{kn}}$, unless non-uniform Gap-ETH is false. Here $\alpha_{\text{kn}} = 2^{-c_{\text{kn}}} < 0.98491$, where c_{kn} is the ℓ_2 kissing-number constant defined in Section 3.2 in the full version.*

Our second result shows improved exponential hardness of $\text{BDD}_{p,\alpha}$ in a different regime and under a somewhat weaker assumption.

► **Theorem 2** (Gap-ETH-hardness of BDD, second bound). *For all $p \in [1, \infty)$, there is no $2^{o(n)}$ -time algorithm for $\text{BDD}_{p,\alpha}$ for any constant $\alpha > \alpha_p^\ddagger$, unless randomized Gap-ETH is false. Here α_p^\ddagger is an explicit constant, defined in Equation (20) in the full version, which satisfies $\alpha_p^\ddagger = 1$ for $1 \leq p \leq 2$, $\alpha_p^\ddagger < 1$ for all $p > 2$, and $\alpha_p^\ddagger \rightarrow 1/2$ as $p \rightarrow \infty$.*

⁴ Each of the quantities α_{kn} , α_p^\ddagger , α_p^\dagger , $\alpha_{p,C}^*$, α_p^* , and C_p described in this section is “explicit” in the sense that it is expressible via some (not necessarily closed-form) expression. These expressions are easily computed to high accuracy in practice as shown, e.g., in Figure 1. Additionally, we emphasize that these quantities are constants in that they do not depend on the rank n of the lattice in the corresponding problem.

⁵ Using the ideas in this paper and [3], showing exponential hardness of SVP essentially corresponds to showing exponential hardness of BDD with $\alpha = 1 - \varepsilon$ for some constant $\varepsilon > 0$. Additionally, using the BDD-hardness framework in this paper, it would be relatively straightforward to show exponential hardness of BDD with $\alpha = 1 + \varepsilon$ for any constant $\varepsilon > 0$. So, the $\alpha = 1$ threshold is qualitatively quite natural, and trying to show hardness for an explicit constant $\alpha < 1$ is a natural goal.

In [3], Aggarwal and Stephens-Davidowitz showed SETH-hardness of $\text{SVP}_{p,1}$ for all $p > p_0 \approx 2.1397$. To partially overcome the “ p_0 barrier,” they generalized their proof techniques to show Gap-ETH-hardness of $\text{SVP}_{p,\gamma}$ for all $p > 2$. The results in [9] adapted the former techniques of [3] to show SETH-hardness of BDD, and similarly got stuck at the p_0 barrier in the sense that they could not prove hardness of $\text{BDD}_{p,\alpha}$ with $p < p_0$ and $\alpha < 1$ simultaneously. The proof of Theorem 2 can be thought of as adapting the latter, generalized techniques of [3] to BDD, and analogously allows us to prove Gap-ETH-hardness of $\text{BDD}_{p,\alpha}$ with $\alpha < 1$ for all $p > 2$.

Compared to related quantities, α_p^\dagger is: at most “ α_p^* with norm embeddings” for all $p \in [1, \infty)$; strictly less than α_p^* for all sufficiently small p ; strictly less than α_{kn} for all sufficiently large p ; and strictly less than the minimum of α_p^* and α_{kn} for intermediate values of p . That is, α_p^\dagger improves on both α_p^* (even with norm embeddings) and α_{kn} for intermediate values of p ; again, see the left plot in Figure 1. (Recall that [9] shows exponential hardness of $\text{BDD}_{p,\alpha}$ for $\alpha > \alpha_p^*$ assuming randomized ETH, and Theorem 1 above shows such hardness for $\alpha > \alpha_{\text{kn}}$ assuming non-uniform Gap-ETH.) However, Theorem 2 relies on a somewhat stronger hardness assumption than the one used in [9], and a somewhat weaker hardness assumption than Theorem 1, so the prior and new results are formally incomparable.

Our third result shows $2^{n/C}$ -hardness of $\text{BDD}_{p,\alpha}$ for any $C > 1$ and $\alpha > \alpha_{p,C}^\dagger$, where $\alpha_{p,C}^\dagger$ is an explicit constant. For all sufficiently small $p \geq 1$ and sufficiently large $C > 1$, $\alpha_{p,C}^\dagger$ not only improves on the corresponding quantity $\alpha_{p,C}^*$ in [9], but also on $\alpha_p^* = \inf_{C>1} \alpha_{p,C}^*$. For example, we show that $\alpha_{1.5,200}^\dagger \approx 1.0247$ while [9] was only able to show $\alpha_{1.5,200}^* \approx 1.3624$ and $\alpha_p^* \approx 1.3554$ (see the right plot in Figure 1).

► **Theorem 3** (Gap-SETH-hardness of BDD). *For all $p \in [1, \infty) \setminus 2\mathbb{Z}$ and all $C > 1$, there is no $2^{n/C}$ -time algorithm for $\text{BDD}_{p,\alpha}$ for any constant $\alpha > \alpha_{p,C}^\dagger$, unless non-uniform Gap-SETH is false. Here $\alpha_{p,C}^\dagger$ is an explicit constant, defined in Equation (21) in the full version, which satisfies $\alpha_{p,C}^\dagger \rightarrow 1$ as $C \rightarrow \infty$ for any fixed $p \in [1, \infty)$.*

Theorems 1 and 3 both crucially rely on the recent breakthrough work of Vlăduț [26] showing an explicit exponential lower bound on the ℓ_2 lattice kissing number, i.e., on the maximum number of vectors $\mathbf{v} \in \mathcal{L}$ achieving $\|\mathbf{v}\| = \lambda_1(\mathcal{L})$. More specifically, [26] shows that there exists a lattice of every rank $n \in \mathbb{Z}^+$ with kissing number at least $2^{c_{\text{kn}}n - o(n)}$, where $c_{\text{kn}} \geq 0.02194$ (see Definition 3.5 and Theorem 3.6 in the full version).

Vlăduț’s specific lower bound on c_{kn} translates to the bounds on α_{kn} and $\alpha_{p,C}^\dagger$ that we obtain. Additionally, our use of “non-uniform” rather than “randomized” Gap-(S)ETH in the preceding results arises from the fact that it is not clear whether Vlăduț’s exponential kissing number lattices can be efficiently constructed uniformly (even using randomness); an affirmative answer would relax the assumptions accordingly. Indeed, our results are agnostic to Vlăduț’s specific construction, and an improved lower bound on c_{kn} would immediately imply improved upper bounds on the values α_{kn} and $\alpha_{p,C}^\dagger$. Additionally, in Section 3.4.1 in the full version we sketch an approach for removing the “gap” part of the assumption in Theorem 3, which would be a further relaxation.

2.2 Hardness for SVP

Our final result shows the same strong runtime lower bounds for $\text{SVP}_{p,\gamma}$ with some constant $\gamma > 1$ under (randomized) Gap-SETH as [3] showed for $\text{SVP}_{p,1}$ under (randomized) SETH. This answers a natural question left open by [1], which analogously showed the same runtime lower bounds for $\text{CVP}_{p,\gamma}$ with some constant $\gamma > 1$ under Gap-SETH as [8] showed for the Closest Vector Problem (CVP) under SETH.

► **Theorem 4** (Gap-SETH-hardness of SVP). *For all $p > p_0 \approx 2.1397$, $p \notin 2\mathbb{Z}$, and all $C > C_p$, there is no $2^{n/C}$ -time algorithm for $\text{SVP}_{p,\gamma}$ for some constant $\gamma > 1$, unless randomized Gap-SETH is false. Here $C_p > 1$ is an explicit constant, defined in Equation (23) in the full version, which satisfies $C_p \rightarrow 1$ as $p \rightarrow \infty$.*

The reduction used to prove Theorem 4 is itself a natural modification of the reduction used in [3] to prove SETH-hardness of exact SVP, but its analysis is more nuanced. We emphasize that simply plugging an instance of $\text{CVP}'_{p,\gamma}$ with $\gamma > 1$ rather than $\gamma = 1$ into the reduction of [3] does not yield corresponding hardness of approximation for $\text{SVP}_{p,\gamma'}$ with $\gamma' > 1$; a modified reduction is necessary. Finally, we remark that the somewhat odd-looking $p \notin 2\mathbb{Z}$ requirement in Theorems 3 and 4 is an artifact of the “upstream” hardness results we employ for $\text{CVP}'_{p,\gamma}$; see Theorem 2.18 in the full version.

3 Our Techniques

3.1 Locally Dense Lattices

As in nearly all prior work on the complexity of BDD and SVP (e.g., [19, 13, 15, 3, 9]), a key component of our results is the construction of a family of “locally dense” lattices, which are specified by a lattice \mathcal{L}^\dagger and corresponding target vector \mathbf{t}^\dagger . For our purposes, a locally dense lattice \mathcal{L}^\dagger is one with few “short” vectors, many vectors “close” to \mathbf{t}^\dagger , but few vectors “too close” to \mathbf{t}^\dagger . (Other works such as [21] define locally dense lattices in a closely related but different way, e.g., without the requirement of few “too close” vectors.)

For a discrete set S , which we will take to be a lattice or a subset of a lattice, define

$$N_p(S, r, \mathbf{t}) := |\{\mathbf{x} \in S : \|\mathbf{t} - \mathbf{x}\|_p \leq r\}| ,$$

$$N_p^o(S, r, \mathbf{t}) := |\{\mathbf{x} \in S : \|\mathbf{t} - \mathbf{x}\|_p < r\}| .$$

Somewhat more formally, we define a locally dense lattice \mathcal{L}^\dagger , \mathbf{t}^\dagger with relative distance α_G in the ℓ_p norm to be one for which

$$N_p(\mathcal{L}^\dagger, \alpha_G, \mathbf{t}^\dagger) \geq \nu^n \cdot N_p^o(\mathcal{L}^\dagger, 1, \mathbf{0}) \tag{1}$$

for some $\nu > 1$. That is, \mathcal{L}^\dagger , \mathbf{t}^\dagger is such that the number G of “close vectors” (within distance α_G of \mathbf{t}^\dagger) is an exponential factor larger than the number of short vectors (of norm at most one). Similarly, we require there to be an exponential factor more close vectors than “too close” vectors, along with some other technical conditions. We defer discussing these issues until the main body of the paper, and for the remainder of the introduction focus on the constraint in Equation (1).

A crux in showing hardness of $\text{BDD}_{p,\alpha}$ and $\text{SVP}_{p,\gamma}$ is constructing good locally dense lattices, and their parameters govern the precise hardness results that we can obtain. A family of locally dense lattices with smaller relative distance α_G and larger ν leads to stronger hardness results. To obtain ETH-type hardness results, we simply need ν to be a constant greater than 1, and then we can show $2^{\Omega(n)}$ -hardness of $\text{BDD}_{p,\alpha}$ for any constant $\alpha > \alpha_G$. For SETH-type hardness results, we get $2^{n/C}$ -hardness of $\text{BDD}_{p,\alpha}$ whenever our reduction to BDD has a multiplicative rank-increase factor of C . The value of C depends on the gap factor ν in Equation (1), so to show such hardness for explicit $C > 0$ we need an explicit lower bound on ν . Our reductions also give a tradeoff between C and α , as shown in the right plot in Figure 1. The full situation is actually a bit more complicated when taking “too close” vectors into account, but we again defer discussing this for now. The situation for SVP is similar to the situation for BDD.

3.2 Sparsification

An important technique in our work is randomized lattice sparsification, an efficient algorithm that essentially does the following. Given (a basis of) a lattice \mathcal{L} and an index $q \in \mathbb{Z}^+$ as input, the algorithm randomly samples a sublattice $\mathcal{L}' \subseteq \mathcal{L}$ such that for any fixed, finite set of lattice points $S \subseteq \mathcal{L}$ satisfying some mild conditions, $|S \cap \mathcal{L}'| \approx |S|/q$ with probability near 1. A variant of this algorithm, additionally given $\mathbf{t} \in \text{span}(\mathcal{L})$ as input, randomly samples $\mathcal{L}' \subseteq \mathcal{L}$ and \mathbf{t}' such that for any fixed, finite set of points $S \subseteq \mathcal{L} - \mathbf{t}$ satisfying some mild conditions, $|S \cap (\mathcal{L}' - \mathbf{t}')| \approx |S|/q$ with probability near 1.

Intuitively, some mild caveats aside, sparsification says that a lattice with few short vectors (and few “too close” vectors) is just as good as a lattice with *no* short non-zero vectors (and no “too close” vectors), since the latter can be efficiently obtained from the former. Indeed, sparsifying with index $q \approx N_p^o(\mathcal{L}, r, \mathbf{0})$ allows us to turn a lattice \mathcal{L} and target \mathbf{t} satisfying, say, $N_p(\mathcal{L}, \alpha r, \mathbf{t}) \geq 100 \cdot N_p^o(\mathcal{L}, r, \mathbf{0})$ into a lattice \mathcal{L}' and target \mathbf{t}' with $N_p(\mathcal{L}', \alpha r, \mathbf{t}') \geq 1$ and $N_p^o(\mathcal{L}' \setminus \{\mathbf{0}\}, r, \mathbf{0}) = 0$, so $\text{dist}_p(\mathbf{t}', \mathcal{L}') \leq \alpha r$ and $\lambda_1^{(p)}(\mathcal{L}') \geq r$. That is, the output $\mathcal{L}', \mathbf{t}'$ satisfies the BDD promise $\text{dist}_p(\mathbf{t}', \mathcal{L}') \leq \alpha \cdot \lambda_1^{(p)}(\mathcal{L}')$. See Section 2.2 in the full version for a formal description of sparsification.

3.3 A Transformation Using Locally Dense Lattices

Define $\text{CVP}'_{p,\gamma}$ to be the following variant of the decision version of the γ -approximate Closest Vector Problem: given a basis B of a rank- n lattice \mathcal{L} and a target vector \mathbf{t} as input, decide whether there exists $\mathbf{x} \in \{0, 1\}^n$ such that $\|B\mathbf{x} - \mathbf{t}\|_p \leq 1$ (i.e., the input is a YES instance), or whether $\text{dist}_p(\mathbf{t}, \mathcal{L}) > \gamma$ (i.e., the input is a NO instance), under the promise that one of the two cases holds. In other words, CVP' is the variant of CVP that asks whether there is a *binary* combination of basis vectors close to the target. Much is known about the (fine-grained) complexity of CVP' , which will be useful for us (see Theorems 2.17 and 2.18 in the full version).

Our reductions from CVP' to BDD and to SVP have the same basic form. Given a rank- n' instance B', \mathbf{t}' of $\text{CVP}'_{p,\gamma}$ for some $\gamma > 1$, we apply the following transformation with some scaling factors $s, \ell > 0$ and some locally dense lattice $\mathcal{L}^\dagger = \mathcal{L}(B^\dagger)$ of rank $n - n'$ with target \mathbf{t}^\dagger satisfying Equation (1):

$$B := \begin{pmatrix} sB' & 0 \\ I_{n'} & 0 \\ 0 & \ell B^\dagger \end{pmatrix}, \quad \mathbf{t} := \begin{pmatrix} s\mathbf{t}' \\ \frac{1}{2}\mathbf{1}_{n'} \\ \ell\mathbf{t}^\dagger \end{pmatrix}. \quad (2)$$

Essentially the same transformation appears in both [3] and [9], and similar ideas appear in a number of works before that. Our work differs in its constructions of locally dense lattice gadgets $(\mathcal{L}^\dagger, \mathbf{t}^\dagger)$, its more general reductions, and its improved analysis.

Here we give a rough analysis of the transformation using two observations. First, we observe that appending $I_{n'}$ to B' allows us to upper bound the number of short lattice vectors in $\mathcal{L}(B)$ by

$$N_p^o(\mathcal{L}(B), r', \mathbf{0}) \leq N_p^o(\mathbb{Z}^{n'} \oplus \mathcal{L}(\ell B^\dagger), r', \mathbf{0}) \quad (3)$$

for any $r' > 0$. Second, suppose that B', \mathbf{t}' is a YES instance of CVP' . Then there exists $\mathbf{x} \in \{0, 1\}^{n'}$ such that $\|B'\mathbf{x} - \mathbf{t}'\| \leq 1$, and hence for each $\mathbf{y} \in \mathbb{Z}^{n-n'}$ with $\|B^\dagger\mathbf{y} - \mathbf{t}^\dagger\|_p \leq \alpha_G$ we get that $\|B(\mathbf{x}, \mathbf{y}) - \mathbf{t}\|_p \leq r$, where $r := (s^p + n'/2^p + (\alpha_G \cdot \ell)^p)^{1/p}$. So,

$$N_p(\mathcal{L}(B), r, \mathbf{t}) \geq N_p(\mathcal{L}(B^\dagger), \alpha_G, \mathbf{t}^\dagger). \quad (4)$$

To transform a YES instance of $\text{CVP}'_{p,\gamma}$ to a valid instance of $\text{BDD}_{p,\alpha}$ for some $\alpha > 0$, it essentially suffices to set the parameters r, s, ℓ and use suitable $B^\dagger, \mathbf{t}^\dagger$ so that, say,

$$N_p(\mathcal{L}(B^\dagger), \alpha_G, \mathbf{t}^\dagger) \geq 100 \cdot N_p^o(\mathbb{Z}^{n'} \oplus \mathcal{L}(\ell B^\dagger), r/\alpha, \mathbf{0}). \quad (5)$$

Indeed, if Equation (5) holds, then by Equations (3) and (4), $N_p(\mathcal{L}(B), r, \mathbf{t}) \geq 100 \cdot N_p^o(\mathcal{L}(B), r/\alpha, \mathbf{0})$. We can then sparsify $\mathcal{L}(B)$ to obtain a lattice with no non-zero vectors of norm less than r/α , and at least one vector within distance r of \mathbf{t} , as needed.

We recall that by assumption, $N_p(\mathcal{L}(B^\dagger), \alpha_G, \mathbf{t}^\dagger) \geq \nu^{n-n'}$, which is important for satisfying Equation (5) since $N_p^o(\mathbb{Z}^{n'} \oplus \mathcal{L}(\ell B^\dagger), r/\alpha, \mathbf{0})$ will typically be exponentially large in n' . We also need that if the input CVP' instance is a NO instance, then there will be few vectors in $\mathcal{L}(B)$ that are close to \mathbf{t} , which depends on \mathcal{L}^\dagger having few vectors “too close” to \mathbf{t}^\dagger , but again we defer discussing this. See Lemma 3.2 in the full version for a precise description of the useful properties of the transformation given in Equation (2).

When reducing to $\text{SVP}_{p,\gamma'}$ instead of $\text{BDD}_{p,\alpha}$ we apply a further transformation to B, \mathbf{t} before sparsifying. Namely, we apply Kannan’s embedding, which appends the vector (\mathbf{t}, u) , for some value $u > 0$, to B to obtain a new basis:

$$B, \mathbf{t}, u \mapsto \begin{pmatrix} B & \mathbf{t} \\ 0 & u \end{pmatrix}.$$

The analysis in this case is a bit more subtle as well – we need to upper bound quantities of the form $N_p(\mathcal{L}(B), (r^p - (wu)^p)^{1/p}, w \cdot (\mathbf{t}, u))$ not just for $w = 0, 1$ (corresponding to short and “too close” vectors in the BDD case, respectively) but for all integers $w \geq 2$ too – but the idea is similar. In fact, we use a result from [3] (presented in Theorem 4.2 in the full version) that analyzes the combination of Kannan’s embedding and sparsification already, essentially reducing our task to bounding the quantities $N_p(\mathcal{L}(B), (r^p - (wu)^p)^{1/p}, w \cdot (\mathbf{t}, u))$.

3.4 Specific Locally Dense Lattices

We conclude this summary of techniques by describing the specific locally dense lattices $\mathcal{L}^\dagger, \mathbf{t}^\dagger$ that we use to instantiate Equation (2). We use two main families of locally dense lattices for our results.

3.4.1 Exponential kissing number lattices

The first family of locally dense lattices is derived from a family of “exponential kissing number” lattices $\{\mathcal{L}_n\}_{n=1}^\infty$. Here, \mathcal{L}_n is of rank n and has exponential Euclidean kissing number, i.e., $N_2(\mathcal{L}_n, \lambda_1(\mathcal{L}_n), \mathbf{0}) = 2^{\Omega(n)}$. Previously, [3] showed how to use the existence of such a family to prove $2^{\Omega(n)}$ -hardness of $\text{SVP}_{p,\gamma}$ for all $p \geq 1$ and some $\gamma > 1$ (and in particular, for $1 \leq p \leq 2$, for which the result was not already known from other techniques), assuming non-uniform Gap-ETH. However, no such family of lattices was known at the time, and in fact proving the existence of such a family was a longstanding open question.

In seminal work appearing shortly after the publication of [3], Vlăduț [26] succeeded in constructing such a family of lattices. Moreover, he proved the existence of such a family with an explicit exponential lower bound. More specifically, he showed the existence of $\{\mathcal{L}_n\}_{n=1}^\infty$ with $N_2(\mathcal{L}_n, \lambda_1(\mathcal{L}_n), \mathbf{0}) \geq 2^{c_{\text{kn}} n - o(n)}$ where $c_{\text{kn}} \geq 0.02194$ (see Theorem 3.6 in the full version).

The proofs of Theorems 1 and 3 both use these “Vlăduț lattices” to construct locally dense lattices, but in different ways. The proof of Theorem 1 constructs a locally dense lattice $\mathcal{L}^\dagger, \mathbf{t}^\dagger$ with relative distance $\alpha \approx 2^{-c_{\text{kn}}} \approx 0.98491$, but with a non-explicit lower bound

on the gap factor ν in Equation (1). The proof of Theorem 3 constructs a locally dense lattice $\mathcal{L}^\dagger, \mathbf{t}^\dagger$ with relative distance $\alpha \approx 1$ but with an explicit lower bound on ν – essentially $\nu \geq 2^{c_{kn}}$. The values $\alpha_{p,C}^\dagger$ in Theorem 3 are defined to be a certain quantity relating the maximum possible kissing number in a lattice of rank $(C-1)n'$, roughly $2^{c_{kn} \cdot (C-1)n'}$, and the number of vectors in $\mathbb{Z}^{n'}$ of norm at most r for some $r > 0$.

The proof of Theorem 3 is actually somewhat simpler than that of Theorem 1, so we first give a bit more detail on it. We note that taking $\mathcal{L}^\dagger := \mathcal{L}_n$ and $\mathbf{t}^\dagger := \mathbf{0}$ for a Vlăduț lattice \mathcal{L}_n almost yields a locally dense lattice family with $\nu^{n-o(n)}$ many close vectors for $\nu \geq 2^{c_{kn}}$ and relative distance $\alpha = 1$, but there are two issues: (1) Vlăduț lattices have exponential kissing number with respect to the ℓ_2 norm rather than general ℓ_p norms, and (2) the origin is itself a “too close” vector.

We handle issue (1) by applying norm embeddings [24] with distortion $(1 + \varepsilon)$ to $\{\mathcal{L}_n\}_{n=1}^\infty$ to obtain a family of lattices $\{\mathcal{L}'_n\}_{n=1}^\infty$ with exponentially high “handshake number” in the ℓ_p norm:

$$N_p(\mathcal{L}'_n, (1 + \varepsilon) \cdot \lambda_1^{(p)}(\mathcal{L}'_n), \mathbf{0}) \geq 2^{c_{kn}n - o(n)},$$

where applying the norm embedding is efficient for any $\varepsilon \geq 1/\text{poly}(n)$. We handle issue (2) by “sparsifying away the origin.” Specifically, for all sufficiently large n we show how to sample a sublattice $\mathcal{L}''_n \subseteq \mathcal{L}'_n$ and $\mathbf{t}'' \in \mathcal{L}'_n \setminus \mathcal{L}''_n$ satisfying

$$N_p(\mathcal{L}''_n, (1 + \varepsilon) \cdot \lambda_1^{(p)}(\mathcal{L}''_n), \mathbf{t}'') \geq N_p(\mathcal{L}'_n, (1 + \varepsilon) \cdot \lambda_1^{(p)}(\mathcal{L}'_n), \mathbf{0})/4 \geq 2^{c_{kn}n - o(n)}$$

with positive probability. In particular, this shows that such lattices exist.

For the proof of Theorem 1, we take \mathcal{L}^\dagger to be \mathcal{L}_n scaled so that $\lambda_1(\mathcal{L}_n) = 1$, and take \mathbf{t}^\dagger to be a uniformly random vector of norm δ for some appropriately chosen constant $0 < \delta < 1$. We then analyze $N_2(\mathcal{L}^\dagger, (1 - \varepsilon) \cdot \lambda_1(\mathcal{L}^\dagger), \mathbf{t}^\dagger)$ for some appropriately chosen constant $0 < \varepsilon < \delta$. Intuitively, there is a tradeoff between choosing smaller δ , which makes $N_2(\mathcal{L}^\dagger, (1 - \varepsilon) \cdot \lambda_1(\mathcal{L}^\dagger), \mathbf{t}^\dagger)$ larger but requires ε to be smaller, and larger δ , which makes $N_2(\mathcal{L}^\dagger, (1 - \varepsilon) \cdot \lambda_1(\mathcal{L}^\dagger), \mathbf{t}^\dagger)$ smaller but allows for ε to be larger. The relative distance α that our reduction achieves is essentially the smallest $\alpha = 1 - \varepsilon$ for which we can ensure that $N_2(\mathcal{L}^\dagger, (1 - \varepsilon) \cdot \lambda_1(\mathcal{L}^\dagger), \mathbf{t}^\dagger) \geq 2^{\Omega(n)}$. To translate these results to general ℓ_p norms, we again use norm embeddings. We also use additional techniques for dealing with “too close” vectors.

We note that the construction of locally dense lattices from lattices with exponential kissing number in [3] does not give explicit bounds on the relative distance α or gap factor ν achieved; the reduction there essentially just needs $\nu > 1$ and $\alpha = 1 - \varepsilon$ for non-explicit $\varepsilon > 0$. On the other hand, the construction in Theorem 1 gives an explicit bound on α but not on ν , and the construction in Theorem 3 gives an explicit bound on ν but with $\alpha > 1$. Therefore, Theorems 1 and 3 can be seen as different refinements of the corresponding analysis in [3]. A very interesting question is whether it’s possible to get a construction that simultaneously achieves explicit ν and relative distance $\alpha = 1 - \varepsilon$; our current techniques do not seem to be able to achieve this. Such a construction would lead to new (Gap-)SETH-hardness results for SVP.

3.4.2 The integer lattice \mathbb{Z}^n

The second family of locally dense lattices that we consider, used to prove Theorems 2 and 4, simply takes \mathcal{L}^\dagger to be the integer lattice \mathbb{Z}^n , and \mathbf{t}^\dagger to be the all- t s vector for some constant t (without loss of generality, $t \in [0, 1/2]$):

$$\mathcal{L}^\dagger := \mathbb{Z}^n, \quad \mathbf{t}^\dagger := t \cdot \mathbf{1}_n.$$

This family was also used in [3] and [9].

19:10 Improved Hardness of BDD and SVP Under Gap-(S)ETH

We will be especially interested in the case where $t = 1/2$. In this case $N_p(\mathbb{Z}^n, \text{dist}_p(1/2 \cdot \mathbf{1}_n, \mathbb{Z}^n), 1/2 \cdot \mathbf{1}_n) = 2^n$, where $\text{dist}_p(1/2 \cdot \mathbf{1}_n, \mathbb{Z}^n) = n^{1/p}/2$. So, for our analysis it essentially suffices to upper bound $N_p(\mathbb{Z}^n, r, \mathbf{0})$ for some $r = n^{1/p}/(2\alpha)$. We have good techniques for doing this; see Section 2.3 in the full version. (We note that the “ p_0 barrier” mentioned earlier comes from p_0 being the smallest value of p satisfying $N_p(\mathbb{Z}^n, n^{1/p}/2, \mathbf{0}) \leq 2^n$.)

The SETH-hardness result for $\text{SVP}_{1,p}$ for $p > p_0$ in [3], the hardness results for BDD in [9], and the Gap-SETH-hardness result for $\text{SVP}_{\gamma,p}$ in Theorem 4 all take $t^\dagger = 1/2 \cdot \mathbf{1}$, and analyze $N_p(\mathbb{Z}^n, n^{1/p}/2, 1/2 \cdot \mathbf{1})/N_p(\mathbb{Z}^n, n^{1/p}/(2\alpha), \mathbf{0}) = 2^n/N_p(\mathbb{Z}^n, n^{1/p}/(2\alpha), \mathbf{0})$ for some $\alpha > 0$. That is, they essentially just need to upper bound $N_p(\mathbb{Z}^n, n^{1/p}/(2\alpha), \mathbf{0})$ for some α (with $\alpha = 1$ for the SVP hardness results). As alluded to in the discussion after the statement of Theorem 2, the Gap-ETH-hardness result in [3] for $\text{SVP}_{p,\gamma}$ essentially works by proving that for every $p > 2$ there exist $t \in (0, 1/2]$ and $r > 0$ (not necessarily $t = 1/2$ or $r = n^{1/p}/2$) such that

$$\frac{N_p(\mathbb{Z}^n, r, t \cdot \mathbf{1})}{N_p(\mathbb{Z}^n, r/\alpha, \mathbf{0})} \geq 2^{\Omega(n)} \quad (6)$$

for some non-explicit $\alpha < 1$.

We do something similar, but study the more refined question of what the *minimum* value of α is such that Equation (6) holds for some t and r . This minimum value of α is essentially how we define the quantities α_p^\dagger used in Theorem 2; see Equation (20) in the full version for a precise definition. We note that, interestingly, in experiments this minimum value of α is always achieved by simply taking $t = 1/2$. That is, empirically it seems that we do not lose anything by fixing $t = 1/2$ and only varying r .⁶ We leave proving this as an interesting open question, but note that the strength of our results does not depend on its resolution either way.

4 Open Questions

One of the most interesting aspects of this and other work on the complexity of lattice problems is the interplay between geometric objects – here, lattices with exponential kissing number and locally dense lattices generally – and hardness results. Proving a better lower bound on c_{kn} would immediately translate into an improved bound on the values of α_{kn} and $\alpha_{p,C}^\dagger$, and more generally proving the existence of some family of gadgets with smaller relative distance α and at least $2^{\Omega(n)}$ close vectors would translate into a hardness result improving on both Theorems 1 and 2.

There is also the question of *constructing* locally dense lattices. The difference between existence and efficient randomized construction of locally dense lattices roughly corresponds to needing “non-uniform” versus “randomized” hardness assumptions. It is also an interesting question whether randomness is needed at all for showing hardness of BDD or SVP. In this work we crucially use randomness for sparsification in addition to using it to construct locally dense lattices. Indeed, derandomizing hardness reductions for SVP (and similarly, BDD) is a notorious, decades-old open problem.

⁶ This is especially interesting since [10] notes that $N_p(\mathbb{Z}^n, r, t \cdot \mathbf{1})$ is *not* maximized by $t = 1/2$ for some $p > 2$, including $p = 3$, and some *fixed* $r > 0$. For $1 \leq p \leq 2$, [17] and [10] note that for any fixed $r > 0$, $N_p(\mathbb{Z}^n, r, t \cdot \mathbf{1})$ is in fact *minimized* (up to a subexponential error term) by taking $t = 1/2$.

References

- 1 Divesh Aggarwal, Huck Bennett, Alexander Golovnev, and Noah Stephens-Davidowitz. Fine-grained hardness of CVP(P) — everything that we can prove (and nothing else). In *SODA*, 2021.
- 2 Divesh Aggarwal and Eldon Chung. A note on the concrete hardness of the shortest independent vector in lattices. *Inf. Process. Lett.*, 167:106065, 2021. doi:10.1016/j.ipl.2020.106065.
- 3 Divesh Aggarwal and Noah Stephens-Davidowitz. (Gap/S)ETH hardness of SVP. In *STOC*, pages 228–238, 2018.
- 4 Miklós Ajtai. The shortest vector problem in L_2 is NP-hard for randomized reductions (extended abstract). In *STOC*, pages 10–19, 1998.
- 5 Miklós Ajtai and Cynthia Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In *STOC*, pages 284–293, 1997.
- 6 Sanjeev Arora, László Babai, Jacques Stern, and Z. Sweedyk. The hardness of approximate optima in lattices, codes, and systems of linear equations. *J. Comput. Syst. Sci.*, 54(2):317–331, 1997. doi:10.1006/jcss.1997.1472.
- 7 Shi Bai, Damien Stehlé, and Weiqiang Wen. Improved reduction from the bounded distance decoding problem to the unique shortest vector problem in lattices. In *ICALP*, pages 76:1–76:12, 2016.
- 8 Huck Bennett, Alexander Golovnev, and Noah Stephens-Davidowitz. On the quantitative hardness of CVP. In *FOCS*, 2017.
- 9 Huck Bennett and Chris Peikert. Hardness of bounded distance decoding on lattices in ℓ_p norms. In *CCC*, 2020. doi:10.4230/LIPIcs.CCC.2020.36.
- 10 N. D. Elkies, A. M. Odlyzko, and J. A. Rush. On the packing densities of superballs and other bodies. *Inventiones mathematicae*, 105:613–639, December 1991.
- 11 Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *STOC*, pages 197–206, 2008.
- 12 Ishay Haviv and Oded Regev. Tensor-based hardness of the shortest vector problem to within almost polynomial factors. *Theory of Computing*, 8(1):513–531, 2012. Preliminary version in STOC 2007.
- 13 Subhash Khot. Hardness of approximating the shortest vector problem in lattices. *J. ACM*, 52(5):789–808, 2005. Preliminary version in FOCS 2004.
- 14 Subhash Khot. Hardness of approximating the shortest vector problem in high ℓ_p norms. *J. Comput. Syst. Sci.*, 72(2):206–219, 2006.
- 15 Yi-Kai Liu, Vadim Lyubashevsky, and Daniele Micciancio. On bounded distance decoding for general lattices. In *RANDOM*, pages 450–461, 2006.
- 16 Vadim Lyubashevsky and Daniele Micciancio. On bounded distance decoding, unique shortest vectors, and the minimum distance problem. In *CRYPTO*, pages 577–594, 2009.
- 17 J. E. Mazo and A. M. Odlyzko. Lattice points in high-dimensional spheres. *Monatshefte für Mathematik*, 110:47–61, March 1990.
- 18 Daniele Micciancio. The shortest vector in a lattice is hard to approximate to within some constant. *SIAM J. Comput.*, 30(6):2008–2035, 2000. Preliminary version in FOCS 1998.
- 19 Daniele Micciancio. The hardness of the closest vector problem with preprocessing. *IEEE Trans. Information Theory*, 47(3):1212–1215, 2001. doi:10.1109/18.915688.
- 20 Daniele Micciancio. Inapproximability of the shortest vector problem: Toward a deterministic reduction. *Theory of Computing*, 8(1):487–512, 2012.
- 21 Daniele Micciancio. Locally dense codes. In *CCC*, pages 90–97, 2014. doi:10.1109/CCC.2014.17.
- 22 Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on Gaussian measures. *SIAM J. Comput.*, 37(1):267–302, 2007. Preliminary version in FOCS 2004.
- 23 Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6):1–40, 2009. Preliminary version in STOC 2005.

19:12 Improved Hardness of BDD and SVP Under Gap-(S)ETH

- 24 Oded Regev and Ricky Rosen. Lattice problems and norm embeddings. In *STOC*, pages 447–456, 2006.
- 25 Peter van Emde Boas. Another NP-complete problem and the complexity of computing short vectors in a lattice. Technical Report 81-04, University of Amsterdam, 1981.
- 26 Serge Vlăduț. Lattices with exponentially large kissing numbers. *Mosc. J. Comb. Number Theory*, 8(2):163–177, 2019. doi:10.2140/moscow.2019.8.163.