

# Tensor-based Hardness of the Shortest Vector Problem to within Almost Polynomial Factors

Ishay Haviv\*

Oded Regev†

March 12, 2007

## Abstract

We show that unless  $\text{NP} \subseteq \text{RTIME}(2^{\text{poly}(\log n)})$ , for any  $\varepsilon > 0$  there is no polynomial-time algorithm approximating the Shortest Vector Problem (SVP) on  $n$ -dimensional lattices in the  $\ell_p$  norm ( $1 \leq p < \infty$ ) to within a factor of  $2^{(\log n)^{1-\varepsilon}}$ . This improves the previous best factor of  $2^{(\log n)^{1/2-\varepsilon}}$  under the same complexity assumption due to Khot [18]. Under the stronger assumption  $\text{NP} \not\subseteq \text{RSUBEXP}$ , we obtain a hardness factor of  $n^{c/\log \log n}$  for some  $c > 0$ .

Our proof starts with SVP instances from [18] that are hard to approximate to within some constant. To boost the hardness factor we simply apply the standard tensor product of lattices. The main novel part is in the analysis, where we show that the lattices of [18] behave nicely under tensorization. At the heart of the analysis is a certain matrix inequality which was first used in the context of lattices by de Shalit and Parzanchevski [12].

## 1 Introduction

A *lattice* is a periodic geometric object defined as all integer combinations of some linearly independent vectors in  $\mathbb{R}^n$ . The interesting combinatorial structure of lattices was investigated by mathematicians over the last two centuries, and in the last two decades it was also studied from a computational point of view. Roughly speaking, most fundamental problems on lattices are not known to be efficiently solvable. Moreover, there are hardness results showing that such problems cannot be solved by polynomial-time algorithms unless the polynomial-hierarchy collapses. One of the main motivations for research on the hardness of lattice problems is their applications in cryptography, as was demonstrated by Ajtai [3], who came up with a construction of cryptographic primitives whose security relies on the worst-case hardness of certain lattice problems.

Two main computational problems associated with lattices are the Shortest Vector Problem (SVP) and the Closest Vector Problem (CVP). In the former, for a lattice given by *some* basis we are supposed to find (the length of) a shortest nonzero vector in the lattice. The problem CVP is an inhomogeneous variant of SVP, in which given a lattice and some target point one has to find (the distance from) the closest lattice

---

\*Department of Computer Science, Tel-Aviv University, Tel-Aviv 69978, Israel.

†Department of Computer Science, Tel-Aviv University, Tel-Aviv 69978, Israel. Supported by an Alon Fellowship, by the Binational Science Foundation, by the Israel Science Foundation, and by the European Commission under the Integrated Project QAP funded by the IST directorate as Contract Number 015848.

point. The hardness of lattice problems partly comes from the fact that there are many possible bases for the same lattice.

In this paper we improve the best hardness result known for SVP. Before presenting our results let us start with an overview of related work.

## 1.1 Related Work

In the early 1980s, Lenstra, Lenstra and Lovász (LLL) presented the first polynomial-time approximation algorithm for SVP [19]. Their algorithm achieves an approximation factor of  $2^{O(n)}$ , where  $n$  is the dimension of the lattice. Using their algorithm, Babai gave an approximation algorithm for CVP achieving the same approximation factor [7]. A few years later, improved algorithms were presented for both problems, obtaining a slightly sub-exponential approximation factor, namely  $2^{O(n(\log \log n)^2 / \log n)}$  [25], and this has since been improved slightly [4]. The best algorithm known for solving SVP *exactly* requires exponential running time in  $n$  [17, 4]. All the above results hold with respect to any  $\ell_p$  norm.

On the hardness side, it was proven in 1981 by van Emde Boas that it is NP-hard to solve SVP exactly in the  $\ell_\infty$  norm [26]. The question of extending this result to other norms, and in particular to the Euclidean norm  $\ell_2$ , remained open till the breakthrough result by Ajtai showing that exact SVP in the  $\ell_2$  norm is NP-hard under randomized reductions [2]. Then, Cai and Nerurkar obtained hardness of approximation to within  $1 + n^{-\varepsilon}$  for some  $\varepsilon > 0$  [10]. The first inapproximability result of SVP to within some constant bounded away from 1 is that of Micciancio, who showed that under randomized reductions SVP in the  $\ell_p$  norm is NP-hard to approximate to within any factor smaller than  $\sqrt[p]{2}$  [20]. For the  $\ell_\infty$  norm, a considerably stronger result is known: Dinur [13] showed that SVP is NP-hard to approximate in the  $\ell_\infty$  norm to within a factor of  $n^{c/\log \log n}$  for some constant  $c > 0$ .

To date, the strongest hardness result known for SVP in the  $\ell_p$  norm is due to Khot [18] who showed NP-hardness of approximation to within arbitrarily large constants under randomized reductions for any  $1 < p < \infty$ . Furthermore, under quasi-polynomial randomized reductions (i.e., reductions that run in time  $2^{\text{poly}(\log n)}$ ), the hardness factor becomes  $2^{(\log n)^{1/2-\varepsilon}}$  for any  $\varepsilon > 0$ . Khot speculated there that it might be possible to improve this to  $2^{(\log n)^{1-\varepsilon}}$ , as this is the hardness factor known for the analogous problem in linear codes [15].

Khot's proof does not work for the  $\ell_1$  norm. However, a recent result [24] shows that for lattice problems, the  $\ell_2$  norm is the easiest in the following sense: for any  $1 \leq p \leq \infty$ , there exists a randomized reduction from lattice problems such as SVP and CVP in the  $\ell_2$  norm to the respective problem in the  $\ell_p$  norm. In particular, this implies that Khot's results also hold for the  $\ell_1$  norm.

Finally, we mention that a considerably stronger result is known for CVP, namely that for any  $1 \leq p \leq \infty$ , it is NP-hard to approximate CVP in the  $\ell_p$  norm to within  $n^{c/\log \log n}$  for some constant  $c > 0$  [14]. We also mention that in contrast to the above hardness results, it is known that SVP and CVP are unlikely to be NP-hard to approximate to within  $\sqrt{n/\log n}$ , as this would imply the collapse of the polynomial-time hierarchy [16, 1].

## 1.2 Our Results

The main result of this paper improves the best NP-hardness factor known for SVP under randomized quasi-polynomial reductions. This and two additional hardness results are stated in the following theorem.

**Theorem 1.1.** *For any  $1 \leq p \leq \infty$  the following holds.*

1. For any  $c \geq 1$ , there is no polynomial-time algorithm that approximates SVP in the  $\ell_p$  norm to within  $c$  unless  $\text{NP} \subseteq \text{RP}$ .
2. For any  $\varepsilon > 0$ , there is no polynomial-time algorithm that approximates SVP on  $n$ -dimensional lattices in the  $\ell_p$  norm to within a factor of  $2^{(\log n)^{1-\varepsilon}}$  unless  $\text{NP} \subseteq \text{RTIME}(2^{\text{poly}(\log n)})$ .
3. There exists a  $c > 0$  such that there is no polynomial-time algorithm that approximates SVP on  $n$ -dimensional lattices in the  $\ell_p$  norm to within a factor of  $n^{c/\log \log n}$  unless  $\text{NP} \subseteq \text{RSUBEXP} = \bigcap_{\delta > 0} \text{RTIME}(2^{n^\delta})$ .

Theorem 1.1 improves on the best known hardness result for any  $p < \infty$ . For  $p = \infty$ , a better hardness result is already known, namely that for some  $c > 0$ , approximating to within  $n^{c/\log \log n}$  is NP-hard [13]. Moreover, Item 1 was already proved by Khot [18] and we provide an alternative proof. As we will show later, Theorem 1.1 follows easily from the following theorem.

**Theorem 1.2.** *There exist  $c, c' > 0$ , such that for any  $1 \leq p \leq \infty$ , there exists a  $c' > 0$  such that for any  $k = k(N)$ , there is no polynomial-time algorithm that approximates SVP in the  $\ell_p$  norm on  $N^{c'k}$ -dimensional lattices to within a factor of  $2^{c'k}$  unless SAT is in  $\text{RTIME}(n^{O(k(n^c))})$ .*

### 1.3 Techniques

A standard method to prove hardness of approximation for large constant or super-constant factors is to first prove hardness for some fixed constant factor, and then *amplify* the constant using some polynomial-time (or quasi-polynomial time) transformation. For example, the *tensor product* of linear codes is used to amplify the NP-hardness of approximating the minimum distance in a linear code of block length  $n$  to arbitrarily large constants under polynomial-time reductions and to  $2^{(\log n)^{1-\varepsilon}}$  (for any  $\varepsilon > 0$ ) under quasi-polynomial-time reductions [15]. This example motivates one to use the tensor product of lattices to increase the hardness factor known for approximating SVP. However, whereas the minimum distance of the  $k$ -fold tensor product of a code  $\mathcal{C}$  is simply the  $k$ th power of the minimum distance of  $\mathcal{C}$ , the behavior of the length of a shortest nonzero vector in a tensor product of lattices is more complicated and not so well understood.

Khot's approach in [18] was to prove a constant hardness factor for SVP instances that have some 'code-like' properties. The rationale is that such lattices might behave in a more predictable way under the tensor product. The construction of these 'basic' SVP instances is ingenious, and is based on BCH codes as well as a restriction into a random sublattice. However, even for these code-like lattices, the behavior of the tensor product was not clear. To resolve this issue, Khot introduced a variant of the tensor product, which he called *augmented tensor product*, and using it he showed the hardness factor of  $2^{(\log n)^{1/2-\varepsilon}}$ . This unusual hardness factor can be seen as a result of the augmented tensor product. In more detail, for the augmented tensor product to work, Khot's basic SVP instances must depend on the number of times  $k$  that we intend to apply the augmented tensor product, and their dimension grows like  $n^{O(k)}$ . After applying the augmented tensor product, the dimension grows to  $n^{O(k^2)}$  and the hardness factor becomes  $2^{O(k)}$ . This limits the hardness factor as a function of the dimension  $n$  to  $2^{(\log n)^{1/2-\varepsilon}}$ .

Our main contribution is showing that Khot's basic SVP instances *do* behave well under the (standard) tensor product. The proof of this fact uses a new method to analyze vectors in the tensor product of lattices, and is related to a technique used by de Shalit and Parzanchevski [12]. Theorem 1.2 now follows easily: we start with (a minor modification of) Khot's basic SVP instances, which are known to be hard to approximate

to within some constant. We then apply the  $k$ -fold tensor product and obtain instances of dimension  $n^{O(k)}$  with hardness  $2^{O(k)}$ .

## 1.4 Open Questions

Some open problems remain. The most obvious is proving that SVP is hard to approximate for factors greater than  $n^{c/\log \log n}$  under some plausible complexity assumption. Such a result, however, is not known for CVP nor for the minimum distance problem in linear codes, and most likely proving it there first would be easier. An alternative goal is to improve on the  $\sqrt{n/\log n}$  upper bound beyond which SVP is not believed to be NP-hard [16, 1].

A second open question is whether our complexity assumptions can be weakened. For instance, our  $n^{c/\log \log n}$  hardness result is based on the assumption that  $\text{NP} \not\subseteq \text{RSUBEXP}$ . For CVP, such a hardness factor is known based solely on  $\text{P} \neq \text{NP}$  [14]. Showing something similar for SVP would be very interesting. In fact, all known hardness proofs for SVP in  $\ell_p$  norms,  $p < \infty$ , are shown through randomized reductions (but see [20] for a possible exception). Finding a deterministic reduction would thus be interesting.

## 1.5 Outline

The rest of the paper is organized as follows. In Section 2 we gather some background on lattices and on the central tool in this paper – the tensor product of lattices. In Section 3 we prove Theorems 1.1 and 1.2. For the sake of completeness, Appendix A provides a brief summary of Khot’s work [18] together with the minor modifications that we need to introduce.

# 2 Preliminaries

## 2.1 Lattices

A *lattice* is a discrete additive subgroup of  $\mathbb{R}^n$ . Equivalently, it is the set of all integer combinations

$$\mathcal{L}(b_1, \dots, b_m) = \left\{ \sum_{i=1}^m x_i b_i : x_i \in \mathbb{Z} \text{ for all } 1 \leq i \leq m \right\}$$

of  $m$  linearly independent vectors  $b_1, \dots, b_m$  in  $\mathbb{R}^n$  ( $n \geq m$ ). If the rank  $m$  equals the dimension  $n$ , then we say that the lattice is *full-rank*. The set  $\{b_1, \dots, b_m\}$  is called a *basis* of the lattice. Note that a lattice has many possible bases. We often represent a basis by an  $n \times m$  matrix  $B$  having the basis vectors as columns, and we say that the basis  $B$  *generates* the lattice  $\mathcal{L}$ . In such case we write  $\mathcal{L} = \mathcal{L}(B)$ . It is well-known and easy to verify that two bases  $B_1$  and  $B_2$  generate the same lattice if and only if  $B_1 = B_2 U$  for some *unimodular* matrix  $U \in \mathbb{Z}^{m \times m}$  (i.e., a matrix whose entries are all integers and its determinant is  $\pm 1$ ). The *determinant* of a lattice generated by a basis  $B$  is  $\det(\mathcal{L}(B)) = \sqrt{\det(B^T B)}$ . It is easy to show that the determinant of a lattice is independent of the choice of basis and is thus well-defined. A *sub-lattice* of  $\mathcal{L}$  is a lattice  $\mathcal{L}(S) \subseteq \mathcal{L}$  generated by some linearly independent lattice vectors  $S = \{s_1, \dots, s_r\} \subseteq \mathcal{L}$ . It is known that any integer matrix  $B$  can be written as  $[H \ 0]U$  where  $H$  has full column rank and  $U$  is unimodular. One way to achieve this is by using the Hermite Normal Form (see, e.g., [11, Page 67]).

For any  $1 \leq p < \infty$ , the  $\ell_p$  norm of a vector  $x \in \mathbb{R}^n$  is defined as  $\|x\|_p = \sqrt[p]{\sum_i |x_i|^p}$  and its  $\ell_\infty$  norm is  $\|x\|_\infty = \max_i |x_i|$ . One basic parameter of a lattice  $\mathcal{L}$ , denoted by  $\lambda_1^{(p)}(\mathcal{L})$ , is the  $\ell_p$  norm of a shortest

nonzero vector in it. Equivalently,  $\lambda_1^{(p)}(\mathcal{L})$  is the minimum  $\ell_p$  distance between two distinct points in the lattice  $\mathcal{L}$ . This definition can be generalized to define the  $i$ th *successive minimum* as the smallest  $r$  such that  $\mathcal{B}_p(r)$  contains  $i$  linearly independent lattice points, where  $\mathcal{B}_p(r)$  denotes the  $\ell_p$  ball of radius  $r$  centered at the origin. More formally, for any  $1 \leq p \leq \infty$ , we define

$$\lambda_i^{(p)}(\mathcal{L}) = \min\{r : \dim(\text{span}(\mathcal{L} \cap \mathcal{B}_p(r))) \geq i\}.$$

We often omit the superscript in  $\lambda_i^{(p)}$  when  $p = 2$ .

In 1896, Hermann Minkowski [23] proved the following two classical results, known as Minkowski's first and second theorems. Note that Minkowski's second theorem is a strengthening of the first one. We consider here the  $\ell_2$  norm although these results have easy extensions to other norms. For simple proofs the reader is referred to [21, Chapter 1, Section 1.3].

**Theorem 2.1** (Minkowski's First Theorem). *For any rank  $r$  lattice  $\mathcal{L}$ ,*

$$\det(\mathcal{L}) \geq \left( \frac{\lambda_1(\mathcal{L})}{\sqrt{r}} \right)^r.$$

**Theorem 2.2** (Minkowski's Second Theorem). *For any rank  $r$  lattice  $\mathcal{L}$ ,*

$$\det(\mathcal{L}) \geq \frac{\prod_{i=1}^r \lambda_i(\mathcal{L})}{r^{r/2}}.$$

Our hardness of approximation results will be shown through the promise version  $\text{GapSVP}_\gamma^p$ , defined for any  $1 \leq p \leq \infty$  and for any approximation factor  $\gamma \leq 1$  as follows.

**Definition 2.3** (Shortest Vector Problem). *An instance of  $\text{GapSVP}_\gamma^p$  is a pair  $(B, s)$  where  $B$  is a lattice basis and  $s$  is a number. In YES instances  $\lambda_1^{(p)}(\mathcal{L}(B)) \leq \gamma \cdot s$  and in NO instances  $\lambda_1^{(p)}(\mathcal{L}(B)) > s$ .*

## 2.2 Tensor Product of Lattices

A central tool in the proof of our results is the *tensor product* of lattices. Let us first recall some basic definitions. For two column vectors  $u$  and  $v$  of dimensions  $n_1$  and  $n_2$  respectively, we define their tensor product  $u \otimes v$  as the  $n_1 n_2$ -dimensional column vector

$$\begin{pmatrix} u_1 v \\ \vdots \\ u_{n_1} v \end{pmatrix}.$$

If we think of the coordinates of  $u \otimes v$  as arranged in an  $n_1 \times n_2$  matrix, we obtain the equivalent description of  $u \otimes v$  as the matrix  $u \cdot v^T$ . More generally, any  $n_1 n_2$ -dimensional vector  $w$  can be written as an  $n_1 \times n_2$  matrix  $W$ . To illustrate the use of this notation, notice that if  $W$  is the matrix corresponding to  $w$  then

$$\|w\|_2^2 = \text{tr}(WW^T). \quad (1)$$

Finally, for an  $n_1 \times m_1$  matrix  $A$  and an  $n_2 \times m_2$  matrix  $B$ , one defines their tensor product  $A \otimes B$  as the  $n_1 n_2 \times m_1 m_2$  matrix

$$\begin{pmatrix} A_{11}B & \cdots & A_{1m_1}B \\ \vdots & & \vdots \\ A_{n_1 1}B & \cdots & A_{n_1 m_1}B \end{pmatrix}.$$

Let  $\mathcal{L}_1$  be a lattice generated by the  $n_1 \times m_1$  matrix  $B_1$  and  $\mathcal{L}_2$  be a lattice generated by the  $n_2 \times m_2$  matrix  $B_2$ . Then the tensor product of  $\mathcal{L}_1$  and  $\mathcal{L}_2$  is defined as the  $n_1 n_2$ -dimensional lattice generated by the  $n_1 n_2 \times m_1 m_2$  matrix  $B_1 \otimes B_2$  and is denoted by  $\mathcal{L} = \mathcal{L}_1 \otimes \mathcal{L}_2$ . Equivalently,  $\mathcal{L}$  is generated by the  $m_1 m_2$  vectors obtained by taking the tensor of two column vectors, one from  $B_1$  and one from  $B_2$ . If we think of the vectors in  $\mathcal{L}$  as  $n_1 \times n_2$  matrices then we can also define it as

$$\mathcal{L} = \mathcal{L}_1 \otimes \mathcal{L}_2 = \{B_1 X B_2^T : X \in \mathbb{Z}^{m_1 \times m_2}\},$$

with each entry in  $X$  corresponding to one of the  $m_1 m_2$  generating vectors. We will mainly use this definition in the proof of the main result.

As alluded to before, in the present paper we are interested in the behavior of the shortest vector in a tensor product of lattices. It is easy to see that for any  $1 \leq p \leq \infty$  and any two lattices  $\mathcal{L}_1$  and  $\mathcal{L}_2$ , we have

$$\lambda_1^{(p)}(\mathcal{L}_1 \otimes \mathcal{L}_2) \leq \lambda_1^{(p)}(\mathcal{L}_1) \cdot \lambda_1^{(p)}(\mathcal{L}_2). \quad (2)$$

Indeed, any two vectors  $v_1$  and  $v_2$  satisfy  $\|v_1 \otimes v_2\|_p = \|v_1\|_p \cdot \|v_2\|_p$ . Applying this to shortest nonzero vectors of  $\mathcal{L}_1$  and  $\mathcal{L}_2$  implies Inequality (2).

Inequality (2) has an analogue for linear codes, with  $\lambda_1^{(p)}$  replaced by the minimum distance of the code under the Hamming metric. There, it is not too hard to show that the inequality is in fact an equality: the minimal distance of the tensor product of two linear codes always equals to the product of their minimal distances. However, contrary to what one might expect, there exist lattices for which Inequality (2) is *strict*. More precisely, for any large enough  $n$  there exist  $n$ -dimensional lattices  $\mathcal{L}_1$  and  $\mathcal{L}_2$  satisfying

$$\lambda_1(\mathcal{L}_1 \otimes \mathcal{L}_2) < \lambda_1(\mathcal{L}_1) \cdot \lambda_1(\mathcal{L}_2).$$

The following lemma due to Steinberg shows this fact. Although we do not use this fact later on, the proof is instructive and helps motivate the need for a careful analysis of tensor products. To present this proof we need the notion of a *dual lattice*. For a full-rank lattice  $\mathcal{L} \subseteq \mathbb{R}^n$  its *dual lattice*  $\mathcal{L}^*$  is defined as

$$\mathcal{L}^* = \{x \in \mathbb{R}^n : \langle x, y \rangle \in \mathbb{Z} \text{ for all } y \in \mathcal{L}\},$$

and a *self-dual* lattice is one that satisfies  $\mathcal{L} = \mathcal{L}^*$ . It can be seen that for a full-rank lattice  $\mathcal{L}$  generated by a basis  $B$ , the basis  $(B^{-1})^T$  generates the lattice  $\mathcal{L}^*$ .

**Lemma 2.4** ([22, Page 48]). *For any large enough  $n$  there exists an  $n$ -dimensional self-dual lattice  $\mathcal{L}$  satisfying  $\lambda_1(\mathcal{L} \otimes \mathcal{L}^*) \leq \sqrt{n}$  and  $\lambda_1(\mathcal{L}) = \lambda_1(\mathcal{L}^*) = \Omega(\sqrt{n})$ .*

**Proof:** We first show that for any full-rank  $n$ -dimensional lattice  $\mathcal{L}$ ,  $\lambda_1(\mathcal{L} \otimes \mathcal{L}^*) \leq \sqrt{n}$ . Let  $\mathcal{L}$  be a lattice generated by a basis  $B = \{b_1, \dots, b_n\}$ . Let  $(B^{-1})^T = \{\tilde{b}_1, \dots, \tilde{b}_n\}$  be the basis generating its dual lattice  $\mathcal{L}^*$ . Now consider the vector  $e = \sum_{i=1}^n b_i \otimes \tilde{b}_i \in \mathcal{L} \otimes \mathcal{L}^*$ . Using our matrix notation, this vector can be written as

$$B I_n ((B^{-1})^T)^T = B B^{-1} = I_n,$$

and clearly has  $\ell_2$  norm  $\sqrt{n}$ . To complete the proof, we need to use the (non-trivial) fact that for large enough  $n$  there exist full-rank,  $n$ -dimensional and self-dual lattices with nonzero shortest vector of norm  $\Omega(\sqrt{n})$ . This fact is due to Conway and Thompson; see [22, Page 46] for details. ■

### 3 Proof of Results

In this section we present the proof of Theorem 1.2 and conclude Theorem 1.1. We only consider the  $\ell_2$  norm. The general case will follow from the following theorem of [24].

**Theorem 3.1** ([24]). *For any  $\varepsilon > 0$ ,  $\gamma < 1$  and  $1 \leq p \leq \infty$  there exists a randomized polynomial-time reduction from  $\text{GapSVP}_{\gamma'}^2$  to  $\text{GapSVP}_{\gamma}^p$  where  $\gamma' = (1 - \varepsilon)\gamma$ .*

To prove our results we first describe a variant of SVP similar to the one that was proved to be NP-hard to approximate to within some constant under randomized reductions by Khot [18]. Then we use the tensor product of lattices and a technique of [12] to boost the hardness factor to an almost polynomial factor in the  $\ell_2$  norm. We note that our results can be shown directly for any  $1 < p < \infty$  without using Theorem 3.1 by essentially the same proof.

#### 3.1 Basic SVP

As already mentioned, our reduction is crucially based on a hardness result of a variant of SVP stemming from Khot's work [18]. Instances of this variant have properties that make it possible to amplify the gap using the tensor product. The following theorem summarizes the hardness result which our proof is based on. For a brief summary indicating how this theorem follows from Khot's work [18] the reader is referred to Appendix A.

**Theorem 3.2** ([18]). *There are a constant  $\gamma < 1$  and a polynomial-time randomized reduction from SAT to SVP outputting a lattice basis  $B$ , satisfying  $\mathcal{L}(B) \subseteq \mathbb{Z}^n$  for some integer  $n$ , and an integer  $d$  that with probability  $9/10$  have the following properties:*

1. *If the SAT instance is a YES instance, then  $\lambda_1(\mathcal{L}(B)) \leq \gamma \cdot \sqrt{d}$ .*
2. *If the SAT instance is a NO instance, then every nonzero vector  $v \in \mathcal{L}(B)$* 
  - *either has at least  $d$  nonzero coordinates,*
  - *or has all coordinates even and at least  $d/4$  of them are nonzero,*
  - *or has all coordinates even and  $\|v\|_2 \geq d$ ,*
  - *or has a coordinate with absolute value at least  $Q := d^{4d}$ .*

*In particular,  $\lambda_1(\mathcal{L}(B)) \geq \sqrt{d}$ .*

#### 3.2 Boosting the SVP Hardness Factor

As mentioned before, we boost the hardness factor using the standard tensor product of lattices. For a lattice  $\mathcal{L}$  we denote by  $\mathcal{L}^{\otimes k}$  the  $k$ -fold tensor product of  $\mathcal{L}$ . An immediate corollary of Inequality (2) is that if  $(B, d)$  is a YES instance of the SVP variant in Theorem 3.2, and  $\mathcal{L} = \mathcal{L}(B)$  then

$$\lambda_1(\mathcal{L}^{\otimes k}) \leq \gamma^k d^{k/2}. \quad (3)$$

For the case in which  $(B, d)$  is a NO instance we will show that any nonzero vector of  $\mathcal{L}^{\otimes k}$  has norm at least  $d^{k/2}$ , i.e.,

$$\lambda_1(\mathcal{L}^{\otimes k}) \geq d^{k/2}. \quad (4)$$

This yields a gap of  $\gamma^k$  between the two cases. Inequality (4) easily follows by induction from the central lemma below, which shows that NO instances ‘tensor nicely’.

**Lemma 3.3.** *Let  $(B, d)$  be a NO instance of the SVP variant given in Theorem 3.2, and denote by  $\mathcal{L}_1$  the lattice generated by the basis  $B$ . Then for any lattice  $\mathcal{L}_2$ ,*

$$\lambda_1(\mathcal{L}_1 \otimes \mathcal{L}_2) \geq \sqrt{d} \cdot \lambda_1(\mathcal{L}_2).$$

The proof of this lemma is based on some properties of sub-lattices of NO instances which are established in the following claim.

**Claim 3.4.** *Let  $(B, d)$  be a NO instance of the SVP variant given in Theorem 3.2, and let  $\mathcal{L} \subseteq \mathcal{L}(B)$  be some rank  $r > 0$  sub-lattice of  $\mathcal{L}(B)$ . Then at least one of the following properties holds:*

1. *Every basis matrix of  $\mathcal{L}$  has at least  $d$  nonzero rows.*
2. *Every basis matrix of  $\mathcal{L}$  contains only even entries and has at least  $\frac{d}{4}$  nonzero rows.*
3.  *$\det(\mathcal{L}) \geq d^{r/2}$ .*

**Proof:** Let  $\mathcal{L} \subseteq \mathcal{L}(B)$  be a rank  $r > 0$  sub-lattice of the integer lattice  $\mathcal{L}(B)$ . The pair  $(B, d)$  is a NO instance of the SVP variant from Theorem 3.2. Hence, every nonzero vector  $v \in \mathcal{L} \subseteq \mathcal{L}(B)$  either has at least  $d$  nonzero coordinates, or has all coordinates even and at least  $d/4$  of them are nonzero, or has all coordinates even and  $\|v\|_2 \geq d$ , or has a coordinate with absolute value at least  $Q = d^{4d}$ .

Assume that the first two properties are not satisfied. Our goal is to show that the third property holds. Since the first property does not hold, we have  $r < d$  and also that any vector in  $\mathcal{L}$  has less than  $d$  nonzero coordinates. We now consider two cases, depending on whether  $\mathcal{L} \subseteq 2 \cdot \mathbb{Z}^n$ .

First assume that  $\mathcal{L} \subseteq 2 \cdot \mathbb{Z}^n$ . By the assumption that the second property does not hold, there must exist a basis of  $\mathcal{L}$  that has less than  $\frac{d}{4}$  nonzero rows. Therefore, all nonzero vectors in  $\mathcal{L}$  have less than  $\frac{d}{4}$  nonzero coordinates, and hence either contain a coordinate with absolute value at least  $d^{4d}$  or have norm at least  $d$ . In particular,  $\lambda_1(\mathcal{L}) \geq d$ , and by Minkowski’s First Theorem (Theorem 2.1) and  $r < d$  we have

$$\det(\mathcal{L}) \geq \left( \frac{\lambda_1(\mathcal{L})}{\sqrt{r}} \right)^r \geq d^{r/2}.$$

Now consider the case  $\mathcal{L} \not\subseteq 2 \cdot \mathbb{Z}^n$ . In this case, any basis of  $\mathcal{L}$  must contain a vector with an odd coordinate, and this vector must have a coordinate of absolute value at least  $d^{4d}$ . Thus, we see that any basis of  $\mathcal{L}$  must contain a vector of length at least  $d^{4d}$ . We claim that this implies that  $\lambda_r(\mathcal{L}) \geq d^{4d}/\sqrt{r}$ . Indeed, it is known that in any lattice  $\mathcal{L}'$  with rank  $r'$  there exists a basis all of whose vectors are of length at most  $\sqrt{r'} \cdot \lambda_{r'}(\mathcal{L}')$  (see [21, Page 129] for details). Using Minkowski’s Second Theorem (Theorem 2.2), we conclude that

$$\det(\mathcal{L}) \geq \frac{\lambda_r(\mathcal{L})}{r^{r/2}} \geq d^{r/2},$$

where we used the fact that since  $\mathcal{L}$  is an integer lattice, every nonzero vector in it has norm at least 1. ■

**Proof of Lemma 3.3:** Let  $v$  be an arbitrary nonzero vector in  $\mathcal{L}_1 \otimes \mathcal{L}_2$ . Our goal is to show that  $\|v\|_2 \geq \sqrt{d} \cdot \lambda_1(\mathcal{L}_2)$ . We can write  $v$  in matrix notation as  $B_1 X B_2^T$  where the integer matrix  $B_1$  is a basis of  $\mathcal{L}_1$ ,  $B_2$  is a basis of  $\mathcal{L}_2$ , and  $X$  is an integer matrix of coefficients. Let  $U$  be a unimodular matrix for which

$X = [H \ 0]U$  where  $H$  is a full column rank matrix. Thus, the vector  $v$  can be written as  $B_1[H \ 0](B_2U^T)^T$ . Since  $U^T$  is also unimodular, the matrices  $B_2$  and  $B_2U^T$  generate the same lattice. Now remove from  $B_2U^T$  the columns corresponding to the zero columns in  $[H \ 0]$  and denote it by  $B'_2$ . Furthermore, denote the matrix  $B_1H$  by  $B'_1$ . Observe that both the matrices  $B'_1$  and  $B'_2$  are bases of the lattices they generate, i.e., have full column rank. The vector  $v$  equals to  $B'_1B'_2{}^T$  where  $\mathcal{L}'_1 := \mathcal{L}(B'_1) \subseteq \mathcal{L}_1$  and  $\mathcal{L}'_2 := \mathcal{L}(B'_2) \subseteq \mathcal{L}_2$ .

Claim 3.4 guarantees that the lattice  $\mathcal{L}'_1$  defined above satisfies at least one of the three properties mentioned in the claim. We show that  $\|v\|_2 \geq \sqrt{d} \cdot \lambda_1(\mathcal{L}'_2)$  in each of these three cases. Then, by the fact that  $\lambda_1(\mathcal{L}'_2) \geq \lambda_1(\mathcal{L}_2)$  the lemma will follow.

**Case 1:** Assume that at least  $d$  of the rows in the basis matrix  $B'_1$  are nonzero. Thus, at least  $d$  of the rows of  $B'_1B'_2{}^T$  are nonzero lattice points from  $\mathcal{L}'_2$  and thus

$$\|v\|_2 \geq \sqrt{d} \cdot \lambda_1(\mathcal{L}'_2).$$

**Case 2:** Assume that the basis matrix  $B'_1$  contains only even entries and has at least  $\frac{d}{4}$  nonzero rows. Hence at least  $\frac{d}{4}$  of the rows of  $B'_1B'_2{}^T$  are even multiples of nonzero lattice vectors from  $\mathcal{L}'_2$ . Therefore every such row has  $\ell_2$  norm at least  $2 \cdot \lambda_1(\mathcal{L}'_2)$  and it follows that

$$\|v\|_2 \geq \sqrt{\frac{d}{4}} \cdot 2 \cdot \lambda_1(\mathcal{L}'_2) = \sqrt{d} \cdot \lambda_1(\mathcal{L}'_2).$$

The third case is based on the following central claim, which is similar to Proposition 1.1 in [12]. The proof is based on an elementary matrix inequality relating the trace and the determinant of a symmetric positive semidefinite matrix (see, e.g., [9, Page 47]).

**Claim 3.5.** *Let  $\mathcal{L}_1$  and  $\mathcal{L}_2$  be two rank  $r$  lattices generated by the bases  $U = \{u_1, \dots, u_r\}$  and  $W = \{w_1, \dots, w_r\}$  respectively. Consider the vector  $v = \sum_{i=1}^r u_i \otimes w_i$  in  $\mathcal{L}_1 \otimes \mathcal{L}_2$ , which can be written as  $UI_rW^T = UW^T$  in matrix notation. Then,*

$$\|v\|_2 \geq \sqrt{r} \cdot (\det(\mathcal{L}_1) \cdot \det(\mathcal{L}_2))^{1/r}.$$

**Proof:** Define the two  $r \times r$  symmetric positive definite matrices  $G_1 = U^TU$  and  $G_2 = W^TW$  (known as the Gram matrices of  $U$  and  $W$ ). By the fact that  $\text{tr}(AB) = \text{tr}(BA)$  for any matrices  $A$  and  $B$  and by Equation (1),

$$\|v\|_2^2 = \text{tr}((UW^T)(UW^T)^T) = \text{tr}(G_1G_2) = \text{tr}(G_1G_2^{1/2}G_2^{1/2}) = \text{tr}(G_2^{1/2}G_1G_2^{1/2}),$$

where  $G_2^{1/2}$  is the positive square root of  $G_2$ . The matrix  $G = G_2^{1/2}G_1G_2^{1/2}$  is also symmetric and positive definite, and as such it has  $r$  real and positive eigenvalues. We can thus apply the geometric-arithmetic means inequality on these eigenvalues to get

$$\|v\|_2^2 = \text{tr}(G) \geq r \det(G)^{1/r} = r \cdot (\det(G_1) \cdot \det(G_2))^{1/r}.$$

Taking the square root of the above completes the proof. ■

Equipped with Claim 3.5 we turn to deal with the third case. In order to bound from below the norm of  $v$ , we apply the claim to its matrix notation  $B'_1B'_2{}^T$  with the lattices  $\mathcal{L}'_1$  and  $\mathcal{L}'_2$  as above.

**Case 3:** Assume that the lattice  $\mathcal{L}'_1$  satisfies  $\det(\mathcal{L}'_1) \geq d^{r/2}$ , where  $r$  denotes its rank. Combining Claim 3.5 and Minkowski's First Theorem we have that

$$\|v\|_2 \geq \sqrt{r} \cdot (\det(\mathcal{L}'_1) \cdot \det(\mathcal{L}'_2))^{1/r} \geq \sqrt{r} \cdot (d^{r/2})^{1/r} \cdot \frac{\lambda_1(\mathcal{L}'_2)}{\sqrt{r}} = \sqrt{d} \cdot \lambda_1(\mathcal{L}'_2),$$

and this completes the proof of the lemma. ■

Let us restate and prove Theorem 1.2.

**Theorem 1.2.** *There exist  $c, c' > 0$ , such that for any  $1 \leq p \leq \infty$ , there exists a  $c'' > 0$  such that for any  $k = k(N)$ , there is no polynomial-time algorithm that approximates  $\text{GapSVP}_\gamma^p$  on  $N^{c''k}$ -dimensional lattices to within a factor of  $\gamma = 2^{-c'k}$  unless SAT is in  $\text{RTIME}(n^{O(k(n^c))})$ .*

**Proof:** Consider some SAT instance of size  $n$ . By Theorem 3.2 we can generate in polynomial-time an  $N$ -dimensional SVP instance  $(B, d)$  for  $N = n^c$  where  $c$  is an absolute constant, which satisfies with high probability the properties from Theorem 3.2. Therefore, in running time of  $n^{O(k(n^c))}$  we can also generate the SVP instance  $(B^{\otimes k}, d^k)$  where  $B^{\otimes k}$  is the  $k$ -fold tensor product of  $B$ , i.e., the matrix that generates the lattice  $\mathcal{L}(B)^{\otimes k}$ . The dimension of this lattice is  $N^k$ , and combining Inequalities (3) and (4) implies a gap of  $\gamma^{-k}$ . For some  $c', c''$ , the polynomial time reduction of Theorem 3.1 yields a lattice of dimension  $N^{c''k}$ , and a gap of at least  $\frac{1}{2}\gamma^{-k} \geq 2^{c'k}$  in the  $\ell_p$  norm. Thus, the existence of an algorithm as in the theorem implies that SAT is in  $\text{RTIME}(n^{O(k(n^c))})$ , and the theorem follows. ■

**Proof of Theorem 1.1:** For Item 1, simply choose  $k$  to be a large enough constant and apply Theorem 1.2. For Item 2, choose  $k = (\log N)^{\frac{1}{\varepsilon}}$  and let  $N' = N^{c''k}$ , where  $c''$  is the one from Theorem 1.2. With this choice of parameters, one gets that

$$k = \left( \frac{\log N'}{c''} \right)^{\frac{1}{1+\varepsilon}} > \left( \frac{\log N'}{c''} \right)^{1-\varepsilon}.$$

Hence, using Theorem 1.2, we see that SVP on  $N'$ -dimensional lattices is hard to approximate to within  $2^{\Omega((\log N')^{1-\varepsilon})}$  unless  $\text{NP} \subseteq \text{RTIME}(2^{\text{poly}(\log n)})$ , as desired. For Item 3, notice that  $\text{NP} \not\subseteq \text{RSUBEXP}$  implies that there exists a constant  $\delta > 0$  such that SAT cannot be solved in  $\text{RTIME}(2^{n^\delta})$ . We now apply Theorem 1.2 with  $k = N^{\delta'}$  for some small enough  $\delta'$ . ■

## Acknowledgement

We thank Mario Szegedy and the anonymous reviewers for their useful comments.

## References

- [1] D. Aharonov and O. Regev. Lattice problems in NP intersect coNP. *Journal of the ACM*, 52(5):749–765, 2005. Preliminary version in FOCS'04.
- [2] M. Ajtai. The shortest vector problem in  $l_2$  is NP-hard for randomized reductions (extended abstract). In *Proceedings of the thirtieth annual ACM symposium on theory of computing - STOC '98*, pages 10–19, Dallas, Texas, USA, May 1998.

- [3] M. Ajtai. Generating hard instances of lattice problems. In *Complexity of computations and proofs*, volume 13 of *Quad. Mat.*, pages 1–32. Dept. Math., Seconda Univ. Napoli, Caserta, 2004.
- [4] M. Ajtai, R. Kumar, and D. Sivakumar. A sieve algorithm for the shortest lattice vector problem. In *Proc. 33th ACM Symp. on Theory of Computing (STOC)*, pages 601–610, 2001.
- [5] N. Alon and J. H. Spencer. *The probabilistic method*. Wiley-Interscience Series in Discrete Mathematics and Optimization. Wiley-Interscience [John Wiley & Sons], New York, second edition, 2000.
- [6] S. Arora, L. Babai, J. Stern, and E. Z. Sweedyk. The hardness of approximate optima in lattices, codes, and systems of linear equations. *Journal of Computer and System Sciences*, 54(2):317–331, Apr. 1997. Preliminary version in FOCS 1993.
- [7] L. Babai. On Lovász lattice reduction and the nearest lattice point problem. *Combinatorica*, 6(1):1–13, 1986.
- [8] M. Bellare, S. Goldwasser, C. Lund, and A. Russell. Efficient probabilistically checkable proofs and applications to approximation. In *Proc. 25th ACM Symposium on Theory of Computing (STOC)*, pages 294–304, 1993.
- [9] R. Bhatia. *Matrix Analysis*. Springer, 1997.
- [10] J.-Y. Cai and A. Nerurkar. Approximating the SVP to within a factor  $(1+1/\dim^\epsilon)$  is NP-hard under randomized reductions. *J. Comput. Syst. Sci.*, 59(2):221–239, 1999.
- [11] H. Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.
- [12] E. de Shalit and O. Parzanchevski. On tensor products of semistable lattices. Preprint, 2006.
- [13] I. Dinur. Approximating  $\text{SVP}_\infty$  to within almost-polynomial factors is NP-hard. *Theoretical Computer Science*, 285(1):55–71, 2002.
- [14] I. Dinur, G. Kindler, R. Raz, and S. Safra. Approximating CVP to within almost-polynomial factors is NP-hard. *Combinatorica*, 23(2):205–243, 2003. Preliminary version in FOCS 1998.
- [15] I. Dumer, D. Micciancio, and M. Sudan. Hardness of approximating the minimum distance of a linear code. *IEEE Trans. Inform. Theory*, 49(1):22–37, 2003.
- [16] O. Goldreich and S. Goldwasser. On the limits of nonapproximability of lattice problems. *J. Comput. System Sci.*, 60(3):540–563, 2000.
- [17] R. Kannan. Minkowski’s convex body theorem and integer programming. *Math. Oper. Res.*, 12:415–440, 1987.
- [18] S. Khot. Hardness of approximating the shortest vector problem in lattices. *Journal of the ACM*, 52(5):789–808, Sept. 2005. Preliminary version in FOCS 2004.
- [19] A. Lenstra, H. Lenstra, and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261:515–534, 1982.

- [20] 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.
- [21] D. Micciancio and S. Goldwasser. *Complexity of Lattice Problems: A Cryptographic Perspective*, volume 671 of *The Kluwer International Series in Engineering and Computer Science*. Kluwer Academic Publishers, Boston, MA, 2002.
- [22] J. Milnor and D. Husemoller. *Symmetric bilinear forms*. Springer-Verlag, Berlin, 1973.
- [23] H. Minkowski. *Geometrie der Zahlen. I*. B. G. Teubner, Leipzig, 1896.
- [24] O. Regev and R. Rosen. Lattice problems and norm embeddings. In *Proc. 38th ACM Symp. on Theory of Computing (STOC)*, pages 447–456, 2006.
- [25] C.-P. Schnorr. A hierarchy of polynomial time lattice basis reduction algorithms. *Theoretical Computer Science*, 53(2-3):201–224, 1987.
- [26] P. van Emde Boas. Another NP-complete problem and the complexity of computing short vectors in a lattice. Technical Report 81-04, Math Inst., University Of Amsterdam, Amsterdam, 1981.

## A Proof of Theorem 3.2

In this appendix we show how Theorem 3.2 follows from Theorem 5.1 of [18]. For a detailed description of Khot’s construction and for complete proofs of the theorems and lemmas below the reader is referred to [18]. For convenience, we first restate Theorem 3.2.

**Theorem 3.2.** *There are a constant  $\gamma < 1$  and a polynomial-time randomized reduction from SAT to SVP outputting a lattice basis  $B$ , satisfying  $\mathcal{L}(B) \subseteq \mathbb{Z}^n$  for some integer  $n$ , and an integer  $d$  that with probability  $9/10$  have the following properties:*

1. *If the SAT instance is a YES instance, then  $\lambda_1(\mathcal{L}(B)) \leq \gamma \cdot \sqrt{d}$ .*
2. *If the SAT instance is a NO instance, then every nonzero vector  $v \in \mathcal{L}(B)$* 
  - *either has at least  $d$  nonzero coordinates,*
  - *or has all coordinates even and at least  $d/4$  of them are nonzero,*
  - *or has all coordinates even and  $\|v\|_2 \geq d$ ,*
  - *or has a coordinate with absolute value at least  $Q = d^{4d}$ .*

### A.1 Comparison with Khot’s Theorem

For the reader familiar with Khot’s proof, we now describe how Theorem 3.2 differs from the one in [18]. First, our theorem is only stated for the  $\ell_2$  norm (since we use Theorem 3.1 to extend the result to other norms). Second, the YES instances of Khot had another property that we do not need here (namely, that the coefficient vector of the short lattice vector is also short). Third, as a result of the augmented tensor product, Khot’s theorem includes an extra parameter  $k$  that specifies the number of times the lattice is supposed to be tensored with itself. Since we do not use the augmented tensor product, we simply fix  $k$  to be some constant.

In more detail, we choose the number of columns in the BCH code to be  $d^{O(1)}$ , as opposed to  $d^{O(k)}$ . This eventually leads to our improved hardness factor. Finally, the third and fourth possibilities in our NO case are merged into one in Khot's theorem (which says that there exists a coordinate with absolute value at least  $d^{O(k)}$ ). Our more refined statement is necessary for the proof of Lemma 3.3 to go through. To obtain it, we only need to make very minor modification to Khot's construction (namely, in the last step of the proof we multiply the randomly chosen row by  $d^{O(d)}$  instead of  $d^{O(k)}$ ). Apart from that, our construction is identical to Khot's, and one only needs to verify that our refined statement indeed holds, as we shall do below.

## A.2 The Proof

The proof of Theorem 3.2 proceeds in three steps. In the first, a variant of the Exact Set Cover problem which is known to be NP-hard is reduced to a gap variant of CVP. In the second step we construct a basis  $B_{int}$  of a lattice which informally contains many short vectors in the YES case and few short vectors in the NO case. Finally, in the third step we complete the reduction by taking a random sub-lattice.

### A.2.1 Step 1

First, consider the following variant of Exact Set Cover. Let  $\eta > 0$  be an arbitrarily small constant. An instance of the problem is a pair  $(S, d)$  where  $S = \{S_1, \dots, S_{n''}\}$  is a collection of subsets of some universe  $[n'] = \{1, \dots, n'\}$ , and  $d$  is some positive number satisfying  $n' + n'' = cd$  for some constant  $c > 1$ . In YES instances, there exists  $S' \subseteq S$  of size  $\eta d$  that covers each element of the universe exactly once. In NO instances, there is no  $S' \subseteq S$  of size less than  $d$  that covers all elements of the universe. This problem is known to be NP-hard for arbitrarily small  $0 < \eta < 1$  [8] and thus to prove Theorem 3.2 it suffices to reduce from this problem.

In the first step we reduce the above variant of Exact Set Cover to a variant of CVP, as was done in [6]. Given an instance  $(S, d)$  the reduction outputs an instance  $(B_{CVP}, t)$  as follows (see Figure 1). Recall that we choose  $Q$  to be a large number,  $Q = d^{4d}$ . Define the basis matrix  $B_{CVP} \in \mathbb{Z}^{cd \times n''}$  by

$$(B_{CVP})_{i,j} = \begin{cases} Q, & \text{if } 1 \leq i \leq n', 1 \leq j \leq n'' \text{ and } i \in S_j, \\ 1, & \text{if } i = j + n', \\ 0, & \text{otherwise.} \end{cases}$$

The target vector  $t \in \mathbb{Z}^{cd}$  is defined as the vector whose first  $n'$  entries contain  $Q$  and all the other contain zeros. The next theorem summarizes useful properties of the CVP instance  $(B_{CVP}, t)$ .

**Theorem A.1** (Theorem 3.1 in [18]). *If  $(S, d)$  is a YES instance of the above variant of Exact Set Cover, then there is a vector  $y$  such that  $B_{CVP}y - t$  is a  $\{0, 1\}$  vector and has exactly  $\eta d$  coordinates equal to 1. If  $(S, d)$  is a NO instance, then for any coefficient vector  $y$  and any nonzero integer  $j_0$ , the vector  $B_{CVP}y + j_0 t$  either has a coordinate with absolute value at least  $Q$ , or has at least  $d$  nonzero coordinates.*

### A.2.2 Step 2

The second step of the reduction is based on BCH codes, as described in the following theorem.

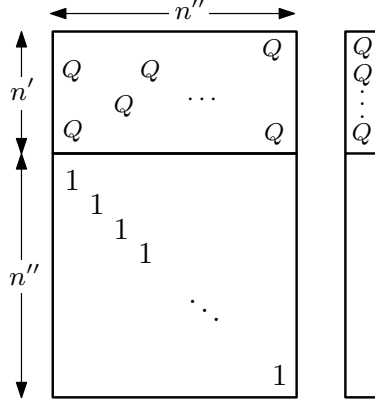


Figure 1:  $B_{\text{CVP}}$  and  $t$

**Theorem A.2** ([5, Page 255]). *Let  $N, d, h$  be integers satisfying  $h = \frac{d}{2} \log N$ . Then there exists an efficiently constructible matrix  $P_{BCH}$  of size  $h \times N$  with  $\{0, 1\}$  entries such that any  $d$  columns of the matrix are linearly independent over  $GF(2)$ .*

We now construct a  $(h + N) \times (h + N)$  matrix denoted by  $B_{BCH}$  (see Figure 2). The upper left block of size  $h \times N$  is  $Q \cdot P_{BCH}$ , i.e., the matrix obtained by multiplying each entry in  $P_{BCH}$  by  $Q$ . The upper right block of size  $h \times h$  is  $2Q \cdot I_h$  where  $I_h$  denotes the  $h \times h$  identity matrix. The lower left block is an  $N \times N$  identity matrix, and the lower right block is zero. The next lemma states some properties of the lattice generated by  $B_{BCH}$ .

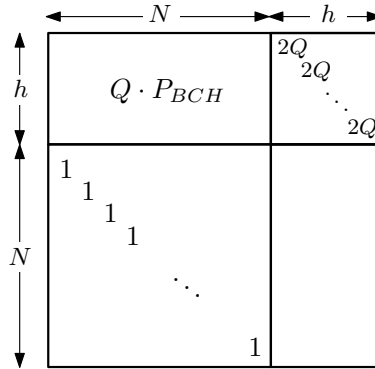


Figure 2:  $B_{BCH}$

**Lemma A.3** (Lemmas 4.2 and 4.3 in [18]). *Every nonzero vector in  $\mathcal{L}(B_{BCH})$  either has a coordinate with absolute value at least  $Q$ , or has at least  $d$  nonzero coordinates or has all coordinates even. Also, for any  $r > \frac{d}{2}$ , it is possible to find in polynomial-time with probability at least  $99/100$  a vector  $s \in \mathbb{Z}^{h+N}$ , so that there are at least  $\frac{1}{100 \cdot 2^h} \binom{N}{r}$  distinct coefficient vectors  $z \in \mathbb{Z}^{N+h}$  satisfying that  $B_{BCH}z - s$  is a  $\{0, 1\}$  vector with exactly  $r$  coordinates equal to 1.*

We now construct the *intermediate lattice* generated by a basis matrix  $B_{int}$  (see Figure 3). Let  $\eta$  be a small enough constant, say  $\frac{1}{100}$ . Let  $r = (\frac{3}{4} + \eta)d$  and choose  $s$  as in Lemma A.3. We choose the parameters of  $B_{BCH}$  to be  $N = d^{42c/\eta}$ ,  $d$  and  $h = \frac{d}{2} \log N$ . Consider a matrix whose upper left block is  $2 \cdot B_{\text{CVP}}$ ,

whose lower right block is  $B_{BCH}$  and all other entries are zeros. Adding to this matrix the column given by the concatenation of  $2 \cdot t$  and  $s$ , we obtain the basis matrix  $B_{int}$  of the intermediate lattice.

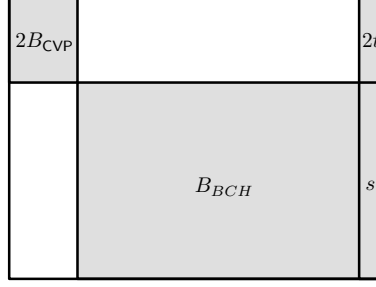


Figure 3:  $B_{int}$

The following two lemmas describe the properties of  $\mathcal{L}(B_{int})$ . The first states that if the CVP instance is a YES instance then  $\mathcal{L}(B_{int})$  contains many short vectors. Define  $\gamma = \sqrt{\frac{3}{4} + 5\eta} < 1$ . A nonzero lattice vector of  $\mathcal{L}(B_{int})$  is called *good* if it has  $\ell_2$  norm at most  $\gamma \cdot \sqrt{d}$ , has  $\{0, 1, 2\}$  coordinates, and has at least one coordinate equal to 1.<sup>1</sup>

**Lemma A.4** (Lemma 5.4 in [18]). *If the CVP instance is a YES instance, then there are at least  $\frac{1}{100 \cdot 2^h} \binom{N}{r}$  good lattice vectors in  $\mathcal{L}(B_{int})$ .*

The second lemma shows that if the CVP instance is a NO instance then  $\mathcal{L}(B_{int})$  contains few vectors that do not satisfy the property from Theorem 3.2, Item 2 – we call such vectors *annoying*. In more detail, a lattice vector of  $\mathcal{L}(B_{int})$  is annoying if it satisfies *all* of the following:

- The number of its nonzero coordinates is fewer than  $d$ .
- Either it contains an odd coordinate or the number of its nonzero coordinates is fewer than  $\frac{d}{4}$ .
- Either it contains an odd coordinate or it has norm smaller than  $d$ .
- All its coordinates have absolute value smaller than  $Q = d^{4d}$ .

The proof of the lemma is very similar to that of Lemma 5.5 in [18]. The difference is in our third and fourth cases that in Khot's definition are merged in one.

**Lemma A.5.** *If the CVP instance is a NO instance, then there are at most  $\binom{N+h}{d/4} d^{40cd}$  annoying lattice vectors in  $\mathcal{L}(B_{int})$ .*

**Proof:** Assume that the CVP instance is a NO instance and let  $B_{int}x$  be an annoying vector with coefficient vector  $x = y \circ z \circ (j_0)$ , where  $\circ$  denotes concatenation of vectors. We have

$$B_{int}x = 2(B_{CVP}y + j_0t) \circ (B_{BCH}z + j_0s).$$

By Theorem A.1, if  $j_0 \neq 0$  then the vector  $B_{CVP}y + j_0t$  either has a coordinate with absolute value at least  $Q$  or has at least  $d$  nonzero coordinates. In both cases  $B_{int}x$  is not an annoying vector and thus we can assume that  $j_0 = 0$  and therefore  $B_{int}x = 2(B_{CVP}y) \circ (B_{BCH}z)$ .

<sup>1</sup>The latter two facts are used in the proof of Lemma A.6.

Since  $B_{int}x$  is annoying we know that it has no coordinate with absolute value at least  $Q$  and has less than  $d$  nonzero coordinates. By Lemma A.3 we get that all coordinates of  $B_{int}x$  are even. Again by the definition of an annoying vector, we conclude that less than  $\frac{d}{4}$  of the coordinates of  $B_{int}x$  are nonzero and all of them have absolute value smaller than  $d$ . Thus, we get a bound of  $d^{d/4} \cdot \binom{N+h}{d/4}$  on the number of possible choices for  $B_{BCH}z$  and a bound of  $d^{cd}$  on the number of possible choices for  $B_{CVP}y$ . Multiplying these two bounds completes the proof of the lemma. ■

### A.2.3 Step 3

In the third step we construct the final SVP instance as claimed in Theorem 3.2. By Lemma A.4, the number of good vectors in the YES case is at least

$$\frac{1}{100 \cdot 2^h} \binom{N}{r} = \frac{1}{100 \cdot 2^{d \log N/2}} \binom{N}{(3/4 + \eta)d} \geq \frac{N^{(3/4+\eta)d}}{d^d \cdot N^{d/2}} = N^{(1/4+\eta)d} / d^d.$$

By Lemma A.5, in the NO case there are at most

$$\binom{N+h}{d/4} d^{40cd} \leq (2N)^{d/4} d^{40cd} \leq N^{d/4} d^{41cd}$$

annoying vectors.

Define  $G := N^{(1/4+\eta)d} / d^d$  and  $A := N^{d/4} d^{41cd}$ . By our choice of  $N$ , for large enough  $d$  we have  $G \geq 10^5 A$ . Choose a prime  $q$  in the interval  $[100A, G/100]$  and let  $w$  be an integer row vector with  $cd + h + N$  coordinates each of which is chosen randomly from the range  $\{0, \dots, q-1\}$ . To get the generating matrix  $B$  of the final lattice we add one more column and one more row to the matrix  $B_{int}$ . The new row starts with the vector  $Q \cdot wB_{int}$  and in the last coordinate it contains  $Q \cdot q$ . The other coordinates of the new column are all zeros. As in the previous step, the YES case is as in [18] and for the NO case we prove a slight strengthening of Lemma 5.6 in [18].

**Lemma A.6** (Lemma 5.7 in [18]). *If the CVP instance is a YES instance then with probability at least 99/100 over the choice of the vector  $w$ , there exists a lattice vector in  $\mathcal{L}(B)$  with  $\ell_2$  norm at most  $\gamma \cdot \sqrt{d}$ .*

**Lemma A.7.** *If the CVP instance is a NO instance then with high probability over the choice of the vector  $w$  every nonzero lattice vector of  $\mathcal{L}(B)$*

- either has at least  $d$  nonzero coordinates,
- or has all coordinates even and at least  $d/4$  of them are nonzero,
- or has all coordinates even and  $\|v\|_2 \geq d$ ,
- or has a coordinate with absolute value at least  $Q = d^{4d}$ .

**Proof:** Let  $Bx' = B(x \circ (l_0)) \in \mathcal{L}(B)$  be some nonzero lattice vector. By the definition of  $B$  we have  $Bx' = B_{int}x \circ Q(wB_{int}x + l_0q)$ . The last coordinate is a multiple of  $Q$ , so if it is nonzero we are done. Hence, we can assume that  $w(B_{int}x) \equiv 0 \pmod{q}$ . If the vector  $Bx'$  does not satisfy any of the four conditions of the lemma, it is an annoying vector and thus all its coordinates are bounded in absolute value by  $Q$ . The fact that  $Q < q$  implies that it is a nonzero vector modulo  $q$ . The probability that there exists a vector which is zero modulo  $q$  is bounded from above using union bound by  $A \cdot \frac{1}{q} \leq \frac{1}{100}$ . Therefore with probability at least  $\frac{99}{100}$  no lattice vector is annoying, and the lemma follows. ■

Lemmas A.6 and A.7 imply Theorem 3.2.