Chapter 14
Inapproximability Results for Computational Problems on Lattices

Subhash Khot

Abstract In this article, we present a survey of known inapproximability results for computational problems on lattices, viz. the Shortest Vector Problem (SVP), the Closest Vector Problem (CVP), the Closest Vector Problem with Preprocessing (CVPP), the Covering Radius Problem (CRP), the Shortest Independent Vectors Problem (SIVP), and the Shortest Basis Problem (SBP).

Introduction

An n-dimensional lattice $\mathcal{L}$ is a set of vectors $\{\sum_{i=1}^{n} x_i \mathbf{b}_i \mid x_i \in \mathbb{Z}\}$ where $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n \in \mathbb{R}^m$ is a set of linearly independent vectors called the basis for the lattice (the same lattice could have many bases). In this article, we survey known results regarding the complexity of several computational problems on lattices. Most of these problems turn out to be intractable, and even computing approximate solutions remains intractable. Excellent references on the subject include Micciancio and Goldwasser's book [1], an expository article by Kumar and Sivakumar [2], and a survey of Regev [3] in the current proceedings.

The Shortest Vector Problem (SVP)

The most studied computational problem on lattices is the Shortest Vector Problem (SVP),[1] where given a basis for an n-dimensional lattice, we seek the shortest non-zero vector in the lattice.[2]

S. Khot
New York University, NY 10012, USA,
e-mail: khot@cs.nyu.edu.

[1] Formal definitions for all problems appear in Section "Notation and Problem Definitions" where we also clarify the issue of how the input is represented.
[2] In this article, we use ℓ_2 norm unless stated otherwise.

P.Q. Nguyen and B. Vallée (eds.), *The LLL Algorithm*, Information Security and Cryptography, DOI 10.1007/978-3-642-02295-1_14,

The problem has been studied since the time of Gauss ([4], 1801) who gave an algorithm that works for 2-dimensional lattices. The general problem for arbitrary dimensions was formulated by Dirichlet in 1842. A well-known theorem of Minkowski [5] deals with the existence of short non-zero vectors in lattices. In a celebrated result, Lenstra, Lenstra, and Lovász [6] gave a polynomial time algorithm for approximating SVP within factor $2^{n/2}$. This algorithm has numerous applications, e.g., factoring rational polynomials [6], breaking knapsack-based codes [7], checking solvability by radicals [8] and integer programming in a fixed number of variables [6, 9, 10]. Schnorr [11] improved the approximation factor to $2^{O(n(\log\log n)^2/\log n)}$. It is a major open problem whether SVP has an efficient polynomial factor approximation. Exact computation of SVP in exponential time is also investigated, see for instance Kannan [12] and Ajtai, Kumar, and Sivakumar [13]. The latter paper also gave a polynomial time $2^{O(n\log\log n/\log n)}$ factor approximation, an improvement over Schnorr's algorithm.

In 1981, van Emde Boas [14] proved that SVP in ℓ_∞ norm is NP-hard and conjectured that the same is true in any ℓ_p norm. However, proving NP-hardness in ℓ_2 norm (or in any finite ℓ_p norm for that matter) was an open problem for a long time. A breakthrough result by Ajtai [15] in 1998 finally showed that SVP is NP-hard under randomized reductions. Cai and Nerurkar [16] improved Ajtai's result to a hardness of approximation result showing a hardness factor of $\left(1+\frac{1}{n^\varepsilon}\right)$. Micciancio [17] showed that SVP is NP-hard to approximate within some constant factor, specifically any factor less than $\sqrt{2}$. Recently, Khot [18] proved that SVP is NP-hard to approximate within any constant factor and hard to approximate within factor $2^{(\log n)^{1/2-\varepsilon}}$ for any $\varepsilon > 0$, unless NP has randomized quasipolynomial time algorithms[1]. This hardness result was further improved to an almost polynomial factor, i.e., $2^{(\log n)^{1-\varepsilon}}$, by Haviv and Regev [19].

Showing hardness of approximation results for SVP was greatly motivated by Ajtai's discovery [20] of worst-case to average-case reduction for SVP and subsequent construction of a lattice-based public key cryptosystem by Ajtai and Dwork [21]. Ajtai showed that if there is a randomized polynomial time algorithm for solving (exact) SVP on a non-negligible fraction of lattices from a certain natural class of lattices, then there is a randomized polynomial time algorithm for approximating SVP on *every* instance within some polynomial factor n^c (he also presented a candidate one-way function). In other words, if approximating SVP within factor n^c is hard in the worst case, then solving SVP exactly is hard on average. Based on this reduction, Ajtai and Dwork [21] constructed a public-key cryptosystem whose security depends on (conjectured) worst-case hardness of approximating SVP (cryptography in general relies on average-case hardness of problems, but for SVP, it is same as worst-case hardness via Ajtai's reduction).

Cai and Nerurkar [22] and Cai [23] brought down the constant c to $9+\varepsilon$ and $4+\varepsilon$ respectively.

[1] Quasipolynmial (randomized) Time is the class $\cup_{C>0}\mathrm{BPTIME}(2^{(\log n)^C})$.

Recently, Regev [24] gave an alternate construction of a public key cryptosystem based on $n^{1.5}$-hardness of SVP.[2] Thus, in principle, one could show that approximating SVP within factor $n^{1.5}$ is NP-hard, and it would imply cryptographic primitives whose security relies on the widely believed conjecture that P $\neq$ NP, attaining the holy grail of cryptography! Unfortunately, there are barriers to showing such strong hardness results. We summarize the so-called *limits to inapproximability* results in Section "Limits to Inapproximability" and refer to Regev's article [3] in the current proceedings for a more detailed exposition.

*The Closest Vector Problem (*CVP*)*

Given a lattice and a point $\mathbf{z}$, the Closest Vector Problem (CVP) is to find the lattice point that is closest to $\mathbf{z}$. Goldreich, Micciancio, Safra, and Seifert [25] gave a Turing reduction from SVP to CVP, showing that any hardness for SVP implies the same hardness for CVP (but not vice versa). CVP was shown to be NP-hard by van Emde Boas [14]. Arora, Babai, Sweedyk, and Stern [26] used the PCP machinery to show that approximating CVP within factor $2^{\log^{1-\varepsilon} n}$ is hard unless NP has quasipolynomial time algorithms. This was improved to a NP-hardness result by Dinur, Kindler, and Safra [27]; their result gives even a subconstant value of ε, i.e., $\varepsilon = (\log\log n)^{-t}$ for any $t < \frac{1}{2}$.

*The Closest Vector Problem with Preprocessing (*CVPP*)*

The Closest Vector Problem with Preprocessing (CVPP) is the following variant of CVP: Given a lattice, one is allowed to do arbitrary preprocessing on it and store polynomial amount of information. The computational problem is to compute the closest lattice point to a given point $\mathbf{z}$. The motivation for studying this problem comes from cryptoraphic applications. In a common scenario, the encryption key is a lattice, the received message is viewed as a point $\mathbf{z}$ and decryption consists of computing the closest lattice point to $\mathbf{z}$. Thus, the lattice is fixed and only the received message changes as an input. A natural question to ask is whether the hardness of CVP arises because one needs to solve the problem on *every* lattice, or whether the problem remains hard even for some fixed lattice when arbitrary preprocessing is allowed.

CVPP was shown to be NP-hard by Micciancio [28] and NP-hard to approximate within any factor less than $\sqrt{5/3}$ by Feige and Micciancio [29]. This was improved to any factor less than $\sqrt{3}$ by Regev [30]. Alekhnovich, Khot, Kindler,

[2] Actually all these results assume hardness of a variant called unique-SVP, see [24] for its definition.

and Vishnoi [31] showed that for every $\varepsilon > 0$, CVPP cannot be approximated in polynomial time within factor $(\log n)^{1/2-\varepsilon}$ unless NP has quasipolynomial time algorithms.[3] Their reduction is from the problem of finding vertex cover on k-uniform hypergraphs. On the other hand, Aharonov and Regev [32] gave a polynomial time $\sqrt{n/\log n}$-approximation.

The Covering Radius Problem (CRP)

The Covering Radius Problem (CRP) asks for a minimum radius r such that balls of radius r around all lattice points cover the whole space. CRP is (clearly) in Π_2, but not even known to be NP-hard. Recently, Haviv and Regev [33] showed that for every large enough p, there is a constant $c_p > 1$ such that CRP under ℓ_p norm is Π_2-hard to approximate within factor c_p. For $p = \infty$, they achieve inapproximability factor of $c_\infty = 1.5$. Their reduction is from a Π_2-hard problem called GroupColoing.

The Shortest Independent Vectors Problem (SIVP) *and the Shortest Basis Problem* (SBP)

The Shortest Independent Vectors Problem (SIVP) asks for the minimum length r such that the given n-dimensional lattice has n linearly independent vectors each of length at most r. The Shortest Basis Problem (SBP) asks for the minimum length r such that the given lattice has a basis with each vector of length at most r. Blömer and Seifert [34] showed that both SIVP and SBP are NP-hard and inapproximable within almost polynomial factor unless NP has quasipolynomial time algorithms. Their reduction is from CVP, and they use specific properties of hard CVP instances produced by Arora et al. [26] reduction.

Results in ℓ_p Norms

Regev and Rosen [35] showed a reduction from lattice problems in ℓ_2 norm to corresponding problems in ℓ_p norm for any $1 \leq p \leq \infty$. The reduction preserves the inapproximability gap upto $1 + \varepsilon$ for any $\varepsilon > 0$. Thus, all hardness results for CVP, SVP, CVPP, SIVP, SBP mentioned above apply to the respective problems in ℓ_p norm for every $1 \leq p \leq \infty$. The idea behind Regev and Rosen's reduction

[3] Because of the peculiar definition of CVPP, the hardness results actually rely on the assumption that NP does not have (quasi)polynomial size circuits.

is the well-known fact that ℓ_2^n *embeds* into $\ell_p^{\mathrm{poly}(n)}$ with distortion $1+\varepsilon$ for every $1 \le p < \infty$, and moreover the embedding is linear. Thus, a lattice in ℓ_2^n space can be mapped to a lattice in $\ell_p^{\mathrm{poly}(n)}$ space, essentially preserving all distances.

In ℓ_∞ norm, stronger inapproximability results are known for SVP and CVP; both are NP-hard to approximate within factor $n^{c/\log\log n}$ for some constant $c > 0$, as proved by Dinur [36].

Limits to Inapproximability

For all the lattice problems, there is a limit to how strong an inapproximately result can be proved. For example, Banaszczyk [37] showed that GapSVP_n is in coNP.[4] Thus, if GapSVP_n is NP-hard then NP = coNP. We state the best known results along this line (see Aharonov and Regev [32], Goldreich and Goldwasser [38], Guruswami, Micciancio, and Regev [39]). We note that AM is the class of languages that have a constant round interactive proof system. A well-known complexity theoretic result is that if NP $\subseteq$ coAM, then polynomial hierarchy collapses.

- $\mathsf{GapCVP}_{\sqrt{n}} \in$ coNP [32], $\mathsf{GapCVP}_{\sqrt{n/\log n}} \in$ coAM [38].
- $\mathsf{GapSVP}_{\sqrt{n}} \in$ coNP [32], $\mathsf{GapSVP}_{\sqrt{n/\log n}} \in$ coAM [38].
- $\mathsf{GapCVPP}_{\sqrt{n/\log n}} \in$ P [32].
- $\mathsf{GapCRP}_2 \in$ AM, $\mathsf{GapCRP}_{\sqrt{n/\log n}} \in$ coAM, $\mathsf{GapCRP}_{\sqrt{n}} \in$ NP $\cap$ coNP [39].
- $\mathsf{GapSIVP}_{\sqrt{n/\log n}} \in$ coAM, $\mathsf{GapSIVP}_{\sqrt{n}} \in$ coNP [39].

In short, CVP, SVP, CRP, SIVP cannot be NP-hard to approximate within $\sqrt{n/\log n}$ unless NP $\subseteq$ coAM (and polynomial hierarchy collapses). CRP cannot be Π_2-hard to approximate within factor 2 unless Π_2 = AM. CVPP has a polynomial time $\sqrt{n/\log n}$-approximation.

Overview of the Article

After introducing the necessary notation and definitions, in the rest of the article, we present inapproximability results for CVP and SVP. For CVP, we include essentially complete proofs and for SVP, only a sketch of the proofs. We refrain from presenting inapproximability results for the remaining problems. A more comprehensive treatment of the subject is beyond the scope of this article.

In Section "Inapproximability of CVP", we present inapproximability results for CVP. We present two results: one gives an arbitrarily large constant factor hardness

[4] See Section "Notation and Problem Definitions" for the definitions of gap-versions of problems.

via a polynomial time reduction from Set Cover and and the other gives almost polynomial factor hardness (i.e., $2^{(\log n)^{1-\varepsilon}}$ for every $\varepsilon > 0$) via a quasipolynomial time reduction from the Label Cover Problem. Both results are due to Arora, Babai, Stern, and Sweedyk [26], though our presentation is somewhat different.

In Section "Inapproximability of SVP", we sketch inapproximability results for SVP. We note that computing SVP exactly was proved NP-hard only in 1998, a breakthrough result of Ajtai [15]. We skip Ajtai's proof from this article (see [2] for a nice sketch) and jump directly to inapproximability results. First we present a reduction of Micciancio [17] showing that GapSVP_γ is NP-hard for any constant $1 < \gamma < \sqrt{2}$.

Next, we present a result of Khot [18] and Haviv and Regev [19] showing that $\mathsf{GapSVP}_{2^{(\log n)^{1-\varepsilon}}}$ is hard via a quasipolynomial time reduction.

Notation and Problem Definitions

In this section, we formally define all the lattice problems considered in this article. We also define their gap-versions which are useful towards proving inapproximability results.

All vectors are column vectors and denoted by bold face letters. A lattice $\mathcal{L}$ generated by a basis $\mathbf{B}$ is denoted as $\mathcal{L}(\mathbf{B})$. $\mathbf{B}$ is a $m \times n$ real matrix whose columns are the basis vectors. The columns are linearly independent (and hence $m \geq n$). The n-dimensional lattice $\mathcal{L}$ in $\mathbb{R}^m$ is given by

$$\mathcal{L} = \mathcal{L}(\mathbf{B}) := \{\mathbf{Bx} \mid \mathbf{x} \in \mathbb{Z}^n\}.$$

We call $\mathbf{x}$ as the coefficient vector (with respect to the specific basis) and any $\mathbf{z} = \mathbf{Bx}$ as the lattice vector. The norm $\|\mathbf{z}\|$ denotes ℓ_2 norm. We restrict to the ℓ_2-norm for much of the article, but Section "Results in ℓ_p Norms" does mention known results for other ℓ_p norms.

Let $\lambda_1(\mathcal{L})$ denote the length of the shortest vector in a lattice, i.e.,

$$\lambda_1(\mathcal{L}(\mathbf{B})) := \min_{\mathbf{x} \in \mathbb{Z}^n,\ \mathbf{x} \neq \mathbf{0}} \|\mathbf{Bx}\|.$$

Definition 1. The Shortest Vector Problem (SVP) asks for the value of $\lambda_1(\mathcal{L}(\mathbf{B}))$ when a lattice basis $\mathbf{B}$ is given as input.

Remark 1. In this article, the dimension m of the ambient space will always be polynomial in the dimension n of the lattice. All real numbers involved are either integers with poly(n) bits or represented by an approximation with poly(n) bits, but we hide this issue for the ease of presentation. Thus, the input size for all the problems is parameterized by the dimension n of the lattice.

Let $\mathrm{dist}(\mathbf{z}, \mathcal{L}(\mathbf{B}))$ denote the minimum distance between a vector $\mathbf{z} \in \mathbb{R}^m$ and any vector in lattice $\mathcal{L}(\mathbf{B})$, i.e.,

$$\text{dist}(\mathbf{z}, \mathcal{L}(\mathbf{B})) := \min_{\mathbf{x}\in\mathbb{Z}^n} \|\mathbf{z} - \mathbf{B}\mathbf{x}\|.$$

Definition 2. The Closest Vector Problem (CVP) asks for the value of $\text{dist}(\mathbf{z}, \mathcal{L}(\mathbf{B}))$ when a lattice basis $\mathbf{B}$, and a vector $\mathbf{z}$ are given.

Definition 3. The Closest Vector Problem with Preprocessing (CVPP) is the following variant: Given a lattice $\mathcal{L}(\mathbf{B})$, one is allowed to do arbitrary preprocessing on it and store polynomial (in the dimension of the lattice) amount of information. The computational problem is to compute $\text{dist}(\mathbf{z}, \mathcal{L}(\mathbf{B}))$ for a given point $\mathbf{z} \in \mathbb{R}^m$.

Let $\text{span}(\mathbf{B})$ denote the linear span of the columns of $\mathbf{B}$. This is a n-dimensional linear subspace of $\mathbb{R}^m$. Let $\rho(\mathcal{L}(\mathbf{B}))$ denote the covering radius of a lattice, i.e., the least radius r such that balls of radius r around lattice points cover $\text{span}(\mathbf{B})$. Equivalently, it is the maximum distance of any point in $\text{span}(\mathbf{B})$ from the lattice:

$$\rho(\mathcal{L}(\mathbf{B})) := \max_{\mathbf{z}\in\text{span}(\mathbf{B})} \text{dist}(\mathbf{z}, \mathcal{L}(\mathbf{B})).$$

Definition 4. The Covering Radius Problem (CRP) asks for the value of $\rho(\mathcal{L}(\mathbf{B}))$ when a lattice basis $\mathbf{B}$ is given.

Let $\lambda_n(\mathcal{L})$ denote the minimum length r such that ball of radius r around the origin contains n linearly independent vectors from the (n-dimensional) lattice $\mathcal{L}$.

Definition 5. The Shortest Independent Vectors Problem (SIVP) asks for the value of $\lambda_n(\mathcal{L}(\mathbf{B}))$ when a lattice basis $\mathbf{B}$ is given.

Definition 6. The Shortest Basis Problem (SBP) asks for the minimum length r such that given lattice $\mathcal{L}(\mathbf{B})$ has a basis whose every vector has length at most r.

We note that CVP, SIVP, SBP are NP-complete and SVP is NP-complete under randomized reductions.[5] CVPP is NP-complete in the following sense: there is a polynomial time reduction from a SAT instance ϕ to CVPP instance $(\mathcal{L}(\mathbf{B}), \mathbf{z})$ such that the lattice $\mathcal{L}(\mathbf{B})$ depends only on $|\phi|$ and not on ϕ itself. This implies that if there is a polynomial time algorithm for CVPP, then SAT has polynomial size circuits (and polynomial hierarchy collapses). Finally, CRP is in Π_2, but not known even to be NP-hard (but it is known to be Π_2-hard for ℓ_p norms with large p).

In this article, we focus on inapproximability results for lattice problems. Such results are proved by a reduction from a *hard* problem (such as SAT) to the gap-version of the lattice problem. Towards this end, we define the gap-versions of all the problems under consideration. In the following $g(n) > 1$ is a function of the dimension of the lattice that corresponds to the *gap-function*. In general, a gap-version $\text{GapX}_{g(n)}$ of an optimization problem X is a promise problem where the

[5] We defined all problems as search problems, so to be precise, one considers their natural decision versions while talking about NP-completeness.

instance is guaranteed to either have a good optimum (the YES instances) or is far from it (the NO instances). The ratio between the optimum value in the YES and the NO cases is at least $g(n)$. An inapproximability result for problem X is typically proved by exhibiting a polynomial time reduction from SAT to $\mathsf{GapX}_{g(n)}$ that preserves the YES and NO instances. Such a reduction clearly implies that it is NP-hard to approximate X within a factor of $g(n)$.

Definition 7. $\mathsf{GapSVP}_{g(n)}$ is a promise problem $(\mathcal{L}(\mathbf{B}), r)$ whose YES instances satisfy $\lambda_1(\mathcal{L}(\mathbf{B})) \leq r$, and NO instances satisfy $\lambda_1(\mathcal{L}(\mathbf{B})) \geq g(n)r$.

Definition 8. $\mathsf{GapCVP}_{g(n)}$ is a promise problem $(\mathcal{L}(\mathbf{B}), \mathbf{t}, r)$ whose YES instances satisfy $\mathrm{dist}(\mathbf{t}, \mathcal{L}(\mathbf{B})) \leq r$, and NO instances satisfy $\mathrm{dist}(\mathbf{t}, \mathcal{L}(\mathbf{B})) \geq g(n)r$.

Definition 9. $\mathsf{GapCVPP}_{g(n)}$ is a promise problem $(\mathcal{L}(\mathbf{B}), \mathbf{t}, r)$ whose YES instances satisfy $\mathrm{dist}(\mathbf{t}, \mathcal{L}(\mathbf{B})) \leq r$, and NO instances satisfy $\mathrm{dist}(\mathbf{t}, \mathcal{L}(\mathbf{B})) \geq g(n)r$. The lattice $\mathcal{L}(\mathbf{B})$ is fixed once the dimension n is fixed.

Definition 10. $\mathsf{GapCRP}_{g(n)}$ is a promise problem $(\mathcal{L}(\mathbf{B}), r)$ whose YES instances satisfy $\rho(\mathcal{L}(\mathbf{B})) \leq r$, and NO instances satisfy $\rho(\mathcal{L}(\mathbf{B})) \geq g(n)r$.

Definition 11. $\mathsf{GapSIVP}_{g(n)}$ is a promise problem $(\mathcal{L}(\mathbf{B}), r)$ whose YES instances satisfy $\lambda_n(\mathcal{L}(\mathbf{B})) \leq r$, and NO instances satisfy $\lambda_n(\mathcal{L}(\mathbf{B})) \geq g(n)r$.

Definition 12. $\mathsf{GapSBP}_{g(n)}$ is a promise problem $(\mathcal{L}(\mathbf{B}), r)$ whose YES instances have a basis with each basis vector of length at most r, and for NO instances, there is no basis with each basis vector of length at most $g(n)r$.

Inapproximability of CVP

In this section, we present two results:

Theorem 1. *For any constant $\eta > 0$, $\mathsf{GapCVP}_{1/\sqrt{\eta}}$ is NP-hard. Thus, CVP is NP-hard to approximate within any constant factor.*

Theorem 2. *For any constant $\varepsilon > 0$, there is a reduction from SAT instance ϕ to $\mathsf{GapCVP}_{2^{(\log n)^{1-\varepsilon}}}$ that runs in time $2^{(\log|\phi|)^{O(1/\varepsilon)}}$. Thus CVP is hard to approximate within almost polynomial factor unless $\mathsf{NP} \subseteq \mathsf{DTIME}(2^{(\log n)^{O(1)}})$.*

Both results are due to Arora, Babai, Stern, and Sweedyk [26], though our presentation is different, especially for the second result.

Proof of Theorem 1

We prove the following theorem which implies Theorem 1 along with some additional properties of GapCVP instance that we need later.

Theorem 3. *For any constant $\eta > 0$, there are constants C, C', C'', and a reduction from* SAT *instance of size n to a* CVP *instance $(\mathcal{L}(\mathbf{B}_{\text{cvp}}), \mathbf{t})$ with the following properties:*

1. $\mathbf{B}_{\text{cvp}}$ *is an integer matrix with size $C'd \times Cd$. The vector $\mathbf{t}$ also has integer co-ordinates and it is linearly independent of the columns of matrix $\mathbf{B}_{\text{cvp}}$.*
2. *The reduction runs in time $n^{C''}$ and therefore $d \leq n^{C''}$.*
3. *If the* SAT *instance is a* YES *instance, then there is a coefficient vector $\mathbf{y} \in \{0,1\}^{Cd}$ such that the vector $\mathbf{B}_{\text{cvp}}\mathbf{y} - \mathbf{t}$ is also a $\{0,1\}$-vector and has exactly ηd co-ordinates equal to 1. In particular, $\text{dist}(\mathbf{t}, \mathcal{L}(\mathbf{B}_{\text{cvp}})) \leq \|\mathbf{B}_{\text{cvp}}\mathbf{y} - \mathbf{t}\| = \sqrt{\eta d}$.*
4. *If the SAT instance is a NO instance, then for any coefficient vector $\mathbf{y} \in \mathbb{Z}^{Cd}$, and any non-zero integer j_0, the vector $\mathbf{B}_{\text{cvp}}\mathbf{y} - j_0\mathbf{t}$ either has a co-ordinate equal to d^{4d}, or has at least d non-zero co-ordinates. In particular, $\text{dist}(\mathbf{t}, \mathcal{L}(\mathbf{B}_{\text{cvp}})) \geq \sqrt{d}$.*

Proof. The reduction is from Exact Set Cover. It is known that for any constant $\eta > 0$, there is a polynomial time reduction from SAT to the Set Cover problem such that : If the SAT instance is a YES instance, then there are ηd sets that cover each element of the universe exactly once. If the SAT instance is a NO instance then there is no set-cover of size d. Let the universe for the set cover instance be $[n']$ and the sets be $S_1, S_2, \ldots, S_{n''}$. It holds that $n' = C_1 d$ and $n'' = Cd$ for some constants C_1, C.

Let the matrix $\mathbf{B}_{\text{cvp}}$ and vector $\mathbf{t}$ be as shown in Fig. 14.1. Here Q is a large integer, say $Q = d^{4d}$. The matrix $\mathbf{B}_{\text{cvp}}$ has $n' + n'' = C'd$ rows and n'' columns. $\mathbf{B}_{\text{cvp}}$ is Q-multiple of the element-set inclusion matrix appended by an identity matrix. The vector $\mathbf{t}$ has first n' co-ordinates equal to Q and the rest are 0.

Let $\mathbf{y} = (y_1, y_2, \ldots, y_{n''}) \in \mathbb{Z}^{n''}$ be the coefficient vector. If the Set Cover instance has an exact cover consisting of ηd sets, then define $y_j = 1$ if the set S_j is

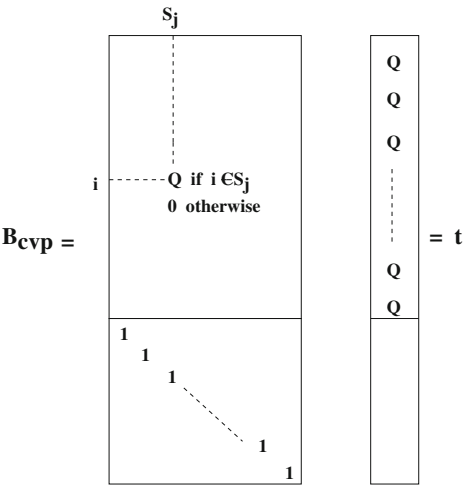

Fig. 14.1 The CVP instance

included in the set cover and $y_j = 0$ otherwise. Clearly, $\mathbf{B}_{\text{cvp}}\mathbf{y} - \mathbf{t}$ has exactly ηd co-ordinates equal to 1 and the rest are zero.

Now assume there is no set cover of size d. Let $\mathbf{y}$ be an arbitrary coefficient vector and $j_0 \in \mathbb{Z}$, $j_0 \neq 0$. If at least d of the co-ordinates y_j are non-zero, we are done. Otherwise the family of sets S_j such that $y_j \neq 0$ has fewer than d sets. This family cannot cover the universe and therefore there is a coordinate in $\mathbf{B}_{\text{cvp}}\mathbf{y} - j_0\mathbf{t}$ that is a non-zero multiple of Q. This coordinate corresponds to an element that is not covered.

Proof of Theorem 2

We prove Theorem 2 using a reduction from the Label Cover problem (see Def. 13). The reduction is essentially from Arora et al. paper [26] which also defined the Label Cover problem.

We first give a reformulation of CVP as the following problem: Let $\mathbf{y} = (y_1, y_2, \ldots, y_n)$ be a vector of integer valued variables. For $1 \leq i \leq m$, $\phi_i(\mathbf{y}) = \sum_j a_{ij} y_j$ be (homogeneous) linear forms and for $1 \leq k \leq t$, $\psi_k(\mathbf{y}) = c_k + \sum_j b_{kj} y_j$ be (non-homogeneous) linear forms. Then CVP (in ℓ_2 norm) is same as the following optimization problem:

$$\min_{\mathbf{y} \in \mathbb{Z}^n} \left(\sum_{i=1}^{m} |\phi_i(\mathbf{y})|^2 \right)^{1/2}$$
$$\text{subject to} \quad \psi_k(\mathbf{y}) = 0 \ \ \forall\, 1 \leq k \leq t.$$

To see that this is just a reformulation of CVP, one can think of the constraints $\psi_k(\mathbf{y}) = 0$ as defining an affine subspace of $\mathbb{R}^n$. The set of all points on this affine subspace corresponding to $\mathbf{y} \in \mathbb{Z}^n$ is of the form $\{\mathbf{z_0} - \mathbf{v} \mid \mathbf{v} \in \mathcal{L}_0\}$ for a suitable point $\mathbf{z_0}$ and a suitable lattice $\mathcal{L}_0$. If Φ denotes the matrix whose rows are the linear forms ϕ_i, then we are minimizing $\|\Phi\mathbf{y}\|$ over $\mathbf{y} \in \mathbb{Z}^n$. This is same as minimizing $\|\Phi(\mathbf{z_0} - \mathbf{v})\|$ over $\mathbf{v} \in \mathcal{L}_0$. This, in turn, is same as minimizing the distance of point $\Phi\mathbf{z_0}$ from the lattice $\Phi\mathcal{L}_0$ (whose basis is obtained by linearly transforming the basis for $\mathcal{L}_0$ via matrix Φ).

The Label Cover Problem

Definition 13. (Label Cover Problem): An instance of label cover is specified as:

$$LC(G(V, W, E), n, m, \{\pi_{v,w}\}_{(v,w)\in E}, [R], [S]).$$

$G = (V, W, E)$ is a bipartite graph with left side vertices V, right side vertices W and a set of edges E. The graph is left regular, i.e., all vertices in V have the same degree. $n = |V|$ and $m = |W|$.

The goal is to assign one "label" to every vertex, where the vertices in V are required to receive a label from set $[R]$ and the vertices in W are required to receive a label from set $[S]$. Thus, a labeling A is just a map $A : V \mapsto [R]$, $A : W \mapsto [S]$. The labeling is supposed to satisfy certain constraints given by maps $\pi_{v,w} : [R] \mapsto [S]$. There is one such map for every edge $(v, w) \in E$. A labeling A "satisfies" an edge (v, w), if

$$\pi_{v,w}(A(v)) = A(w).$$

The optimum $OPT(LC)$ of the instance is defined to be the maximum fraction of edges satisfied by any labeling. We assume that $n \geq m$, and $R \geq S$ (thus the left side is viewed as *larger*).

The following theorem can be obtained by combining the PCP Theorem (Arora and Safra [40], Arora et al. [41]) with Raz's Parallel Repetition Theorem [42]. This theorem is the starting point for most of the recent PCP constructions and hardness results.

Theorem 4. *There exists an absolute constant $\beta > 0$ such that for every integer $R \geq 7$, there is a reduction from* SAT *instance ϕ to Label Cover instance $LC(G(V, W, E), n, m, \{\pi_{v,w}\}, [R], [S])$ with the following property. The* YES *instances of* SAT *map to label cover instances with* $\mathrm{OPT(LC)} = 1$ *and the* NO *instances map to label cover instances with* $\mathrm{OPT(LC)} \leq R^{-\beta}$. *The running time of the reduction and size of the label cover instance are bounded by $|\phi|^{O(\log R)}$.*

Reduction from Label Cover to GapCVP

Let $LC(G(V, W, E), n, m, \{\pi_{v,w}\}, [R], [S])$ be the instance of Label Cover given by Theorem 4. We describe a reduction from this instance to GapCVP_g where the gap $g = \frac{1}{20} R^{\beta/2}$. We construct the CVP instance according to the new CVP-formulation described in the beginning of this section. The set of integer valued variables is:

$$Y := \{y_{v,j} \mid v \in V, j \in [R]\} \bigcup \{z_{w,i} \mid w \in W, i \in [S]\}.$$

The function to be minimized is

$$OBJ := \left(m \cdot \sum_{v \in V, j \in [R]} y_{v,j}^2 + n \cdot \sum_{w \in W, i \in [S]} z_{w,i}^2 \right)^{1/2}.$$

The affine *constraints* are:

$$\forall\, v \in V, \qquad \sum_{j\in[R]} y_{v,j} = 1. \tag{14.1}$$

$$\forall\, w \in W, \qquad \sum_{i\in[S]} z_{w,i} = 1. \tag{14.2}$$

$$\forall\, (v,w) \in E, \forall\, i \in [S], \qquad z_{w,i} = \sum_{j\in[R]:\pi_{v,w}(j)=i} y_{v,j}. \tag{14.3}$$

The YES Case:

We prove that if the Label Cover instance has a labeling that satisfies all edges (i.e., $OPT(LC) = 1$), then there is an integer assignment to variables in Y such that $OBJ \le \sqrt{2mn}$. Indeed, let $A : V \mapsto [R]$, $A : W \mapsto [S]$ be such a labeling. Define

$$y_{v,j} := \begin{cases} 1 & \text{if } j = A(v) \\ 0 & \text{otherwise.} \end{cases}$$

Similarly, define $z_{w,i} = 1$ if $i = A(w)$ and $z_{w,i} = 0$ otherwise. Clearly, for every $v \in V$ ($w \in W$ resp.), there is exactly one $j \in [R]$ ($i \in [S]$ resp.) such that $y_{v,j}$ ($z_{w,i}$ resp.) is non-zero, and its value equals 1. Therefore

$$OBJ = \sqrt{m\cdot|V| + n\cdot|W|} = \sqrt{2mn}.$$

The above reasoning also shows that all constraints in (14.1) and (14.2) are satisfied. Now we show that all constraints in (14.3) are satisfied. Fix any such constraint, i.e., fix $(v,w) \in E$ and $i \in [S]$. We will show that

$$z_{w,i} = \sum_{j\in[R]:\pi_{v,w}(j)=i} y_{v,j}. \tag{14.4}$$

Let $i_0 = A(w)$ and $j_0 = A(v)$. Since the labeling satisfies the edge (v,w), we have $\pi_{v,w}(j_0) = i_0$. Clearly, if $i \neq i_0$, then both sides of (14.4) evaluate to zero, and if $i = i_0$, both sides evaluate to 1.

The NO Case:

We prove that if the Label Cover instance has no labeling that satisfies even α fraction of its edges for $\alpha < 0.1$, then for any integer assignment to variables in Y that satisfies constraints (14.1)–(14.3), one must have $OBJ \ge 0.1\sqrt{mn/\alpha}$. Note that, once proven, it implies that if $OPT(LC) \le R^{-\beta}$, then $OBJ \ge 0.1 \cdot R^{\beta/2}\sqrt{mn}$. Thus the gap between the YES and NO cases is

$$\frac{0.1 \cdot R^{\beta/2}\sqrt{mn}}{\sqrt{2mn}} \geq \frac{1}{20} R^{\beta/2} \qquad \text{as claimed.}$$

Consider any integer assignment to variables in Y that satisfies constraints (14.1)–(14.3). Define sets $T_v \subseteq [R]$, $T_w \subseteq [S]$ as:

$$T_v := \{j \in [R] \mid y_{v,j} \neq 0\}, \qquad T_w := \{i \in [S] \mid z_{w,i} \neq 0\}.$$

Due to constraints (14.1) and (14.2), the sets T_v, T_w are non-empty for all $v \in V$, $w \in W$.

Lemma 1. *For any $(v, w) \in E$ and $i \in T_w$, there exists $j^* \in T_v$ such that $\pi_{v,w}(j^*) = i$.*

Proof. Consider the constraint $z_{w,i} = \sum_{j \in [R]: \pi_{v,w}(j) = i} y_{v,j}$. Since $i \in T_w$, $z_{w,i} \neq 0$. Hence, one of the variables on the right side must be non-zero, say the variable y_{v,j^*}. Thus $j^* \in T_v$ and $\pi_{v,w}(j^*) = i$.

We consider two scenarios depending on whether the typical size of sets T_v is *small* or *large*. Towards this end, let

$$V^* := \{v \in V \mid |T_v| \geq 0.1/\alpha\}.$$

Case (i): $|V^*| \geq 0.1|V| = 0.1 \cdot n$. In this case,

$$OBJ \geq \left(m \cdot \sum_{v \in V, j \in [R]} y_{v,j}^2 \right)^{1/2} \geq \left(m \cdot \sum_{v \in V^*, j: y_{v,j} \neq 0} 1 \right)^{1/2} = \left(m \cdot \sum_{v \in |V^*|} |T_v| \right)^{1/2}$$
$$\geq \sqrt{m \cdot |V^*| \cdot 0.1/\alpha} \geq 0.1\sqrt{mn/\alpha}.$$

Case (ii): $|V^*| \leq 0.1|V|$. In this case, ignore the edges (v, w) that are incident on V^*. Since the graph of label cover instance is regular, we ignore only 0.1 fraction of its edges. Define the following labeling to V and W. The label of $w \in W$ is an arbitrary label from set T_w. The label of $v \in V$ is a random label from set T_v. We show that this labeling satisfies, in expectation, at least $0.9\alpha/0.1$ fraction of edges of label cover (arriving at a contradiction, since we know that there is no labeling that satisfies even α fraction of edges). Indeed, if (v, w) is any edge such that $v \notin V^*$, then $|T_v| \leq 0.1/\alpha$. Let label of w be some $i^* \in T_w$. By Lemma 1, we know that there exists a label $j^* \in T_v$ such that $\pi_{v,w}(j^*) = i^*$. With probability $1/|T_v| \geq \alpha/0.1$, we select j^* as the label of v and the edge (v, w) is satisfied. This completes the proof.

Finishing the Proof of Theorem 2

Let n be the size of SAT instance. Combining reduction from SAT to Label Cover in Theorem 4 with our reduction from Label Cover to GapCVP, we get a reduction from SAT to $\mathsf{GapCVP}_{1/20\cdot R^{\beta/2}}$ that runs in time $n^{C\log R}$ for some constant C.

Choose $R = 2^{(\log n)^k}$ for some large integer k. The size of CVP instance is $N \le n^{C\log R}$. Thus $\log N \le C\log R\log n \le (\log n)^{2+k}$. The inapproximability factor for CVP is

$$\frac{1}{20}R^{\beta/2} = \frac{1}{20}2^{\beta/2\log R} = \frac{1}{20}2^{\beta/2(\log n)^k} \ge 2^{(\log n)^{k-1}} \ge 2^{(\log N)^{(k-1)/(k+2)}}.$$

When $k \approx 1/\varepsilon$, the hardness factor is $\approx 2^{(\log N)^{1-\varepsilon}}$ which proves Theorem 2.

Inapproximability of SVP

In this section, we present two results:

Theorem 5. *For any constant* $1 < \gamma' < \sqrt{2}$, $\mathsf{GapSVP}_{\gamma'}$ *is* NP*-hard. Thus,* SVP *is* NP*-hard to approximate within any constant factor less than* $\sqrt{2}$.

Theorem 6. *For any constant* $\varepsilon > 0$, *there is a reduction from* SAT *instance* ϕ *to* $\mathsf{GapSVP}_{2^{(\log n)^{1-\varepsilon}}}$ *that runs in time* $2^{(\log|\phi|)^{O(1/\varepsilon)}}$. *Thus* SVP *is hard to approximate within almost polynomial factor unless* $\mathsf{NP} \subseteq \mathsf{DTIME}(2^{(\log n)^{O(1)}})$.

The first result is due to Micciancio [17] and the second is a combination of results of Khot [18] and Haviv and Regev [19]. We present only a sketch of both proofs.

Proof of Theorem 5

The reduction is from GapCVP. Let $(\mathbf{B}_{\text{cvp}}, \mathbf{t})$ be an instance of $\mathsf{GapCVP}_{1/\sqrt{\eta}}$ given by Theorem 1. Micciancio constructs GapSVP instance $\mathcal{L}(\mathbf{B}')$ as follows:

$$\mathbf{B}' = \left[\begin{array}{c|c} \boldsymbol{\alpha}\mathbf{B}_{\text{cvp}}\mathbf{T} & \boldsymbol{\alpha}\mathbf{t} \\ \hline \mathbf{B}_{\text{gad}} & \mathbf{s} \end{array}\right] \tag{14.5}$$

Here, α is a suitable constant, $\mathbf{B}_{\text{gad}}, \mathbf{T}$ are matrices and $\mathbf{s}$ is a vector (of appropriate dimensions). The crucial ingredient of Micciancio's reduction is construction of the *gadget* $(\mathbf{B}_{\text{gad}}, \mathbf{T}, \mathbf{s})$. Here, $\mathcal{L}(\mathbf{B}_{\text{gad}})$ is a lattice and $\mathbf{s}$ is a (non-lattice) point such that: (1) $\lambda_1(\mathcal{L}(\mathbf{B}_{\text{gad}})) \ge \gamma r$ for a parameter r, $1 < \gamma < \sqrt{2}$ and (2) the ball of radius r

around $\mathbf{s}$ contains exponentially many lattice points of $\mathcal{L}(\mathbf{B}_{\text{gad}})$. The set of all lattice points in this ball also satisfy an extra property, as made precise in the statement of the lemma below (and this is where the matrix $\mathbf{T}$ enters into the picture). The construction is quite involved, based on sphere packings, Schnorr-Adleman prime number lattice, and a probabilistic version of Sauer's Lemma.

Micciancio's Gadget Construction

Lemma 2. *For every $1 < \gamma < \sqrt{2}$ and integer m, one can construct in probabilistic polynomial time, matrices $\mathbf{B}_{\text{gad}}, \mathbf{T}$, a vector $\mathbf{s}$, and parameters k, ℓ, r such that:*

1. *$\mathbf{T}$ has size $m \times k$, $\mathbf{B}_{\text{gad}}$ has size $\ell \times k$, and $\mathbf{s}$ is a column vector of size ℓ. Here, $k, \ell \leq \text{poly}(m)$.*
2. *The lattice $\mathcal{L}(\mathbf{B}_{\text{gad}})$ has no non-zero vector of length less than γr, i.e.,*

$$\forall\, \mathbf{x} \in \mathbb{Z}^k, \mathbf{x} \neq 0, \quad \|\mathbf{B}_{\text{gad}}\mathbf{x}\| \geq \gamma r.$$

3. *For every $\mathbf{y} \in \{0,1\}^m$, there exists $\mathbf{x} \in \mathbb{Z}^k$ such that $\mathbf{T}\mathbf{x} = \mathbf{y}$ and $\|\mathbf{B}_{\text{gad}}\mathbf{x} - \mathbf{s}\| \leq r$. In particular, the ball of radius r around $\mathbf{s}$ contains at least 2^m points from the lattice $\mathcal{L}(\mathbf{B}_{\text{gad}})$.*

Micciancio's Reduction

We now present a reduction from GapCVP to GapSVP. Let $(\mathbf{B}_{\text{cvp}}, \mathbf{t})$ be the $\text{GapCVP}_{1/\sqrt{\eta}}$ instance as in Theorem 1. We will choose η to be a small enough constant later. Let $m' \times m$ denote the size of matrix $\mathbf{B}_{\text{cvp}}$ (and hence $\mathbf{t}$ is a column vector of size m). Let $(\mathbf{B}_{\text{gad}}, \mathbf{T}, \mathbf{s})$ be the gadget given by Lemma 2 with parameters m and $1 < \gamma < \sqrt{2}$. Parameters k, ℓ, r are as in that lemma.

Construct matrix $\mathbf{B}'$ as in Equation (14.5) where $\alpha = \gamma r/\sqrt{d}$. Let us denote the coefficient vector for lattice $\mathcal{L}(\mathbf{B}')$ by $\mathbf{x}'$ and write $\mathbf{x}' = (\mathbf{x}, j)$ with $j \in \mathbb{Z}$. Note that

$$\mathbf{B}'\mathbf{x}' = \left(\alpha(\mathbf{B}_{\text{cvp}}\mathbf{T}\,\mathbf{x} + j\,\mathbf{t}),\ \ \mathbf{B}_{\text{gad}}\,\mathbf{x} + j\,\mathbf{s}\right). \tag{14.6}$$

Note that the GapCVP instance satisfies Property 3 (the YES case) or Property 4 (the NO case) in Theorem 1. We show that in the YES case, the lattice $\mathcal{L}(\mathbf{B}')$ has a *short* non-zero vector, whereas in the NO case, every non-zero vector is *long*.

The YES Case:

In the YES case, we know that that there exists $\mathbf{y} \in \{0,1\}^m$ such that $\|\mathbf{B}_{\text{cvp}}\mathbf{y} - \mathbf{t}\| \leq \sqrt{\eta d}$. We prove that $\mathcal{L}(\mathbf{B}')$ has a non-zero vector of length at most $\sqrt{1+\gamma^2\eta} \cdot r$. Indeed, Lemma 2 guarantees existence of $\mathbf{x} \in \{0,1\}^k$ such that $\mathbf{T}\mathbf{x} = \mathbf{y}$ and $\|\mathbf{B}_{\text{gad}}\mathbf{x} - \mathbf{s}\| \leq r$. We let $\mathbf{x}' = (\mathbf{x}, -1)$. Clearly,

$$\|\mathbf{B}'\mathbf{x}'\|^2 = \alpha^2\|\mathbf{B}_{\text{cvp}}\mathbf{T}\,\mathbf{x} - \mathbf{t}\|^2 + \|\mathbf{B}_{\text{gad}}\,\mathbf{x} - \mathbf{s}\|^2$$
$$\leq \alpha^2\|\mathbf{B}_{\text{cvp}}\mathbf{y} - \mathbf{t}\|^2 + r^2 \leq \alpha^2\eta d + r^2 = (1 + \gamma^2\eta)r^2,$$

by the choice of $\alpha = \gamma r/\sqrt{d}$. Note that $\|\mathbf{B}'\mathbf{x}'\| \approx r$ by choosing η sufficiently small.

The NO Case:

In the NO case, for every $\mathbf{y} \in \mathbb{Z}^m$ and $j_0 \neq 0$, $\|\mathbf{B}_{\text{cvp}}\mathbf{y} + j_0\mathbf{t}\| \geq \sqrt{d}$. We prove that every non-zero vector in $\mathcal{L}(\mathbf{B}')$ has length at least γr.

Let $\mathbf{B}'\mathbf{x}'$ be an arbitrary non-zero lattice vector with $\mathbf{x}' = (\mathbf{x}, j_0)$. First consider the case when $j_0 \neq 0$. In this case

$$\|\mathbf{B}'\mathbf{x}'\| \geq \alpha\|\mathbf{B}_{\text{cvp}}(\mathbf{T}\,\mathbf{x}) + j_0\mathbf{t}\| \geq \alpha\sqrt{d} = \gamma r.$$

Now consider the case when $j_0 = 0$. In this case $\mathbf{x} \neq 0$ and from Lemma 2, Property (2),

$$\|\mathbf{B}'\mathbf{x}'\| \geq \|\mathbf{B}_{\text{gad}}\,\mathbf{x}\| \geq \gamma r.$$

Thus, the instance of GapSVP has a gap of $\gamma' = \frac{\gamma}{\sqrt{1+\gamma^2\eta}}$ which can be made arbitrarily close to $\sqrt{2}$ by choosing γ to be close enough to $\sqrt{2}$ and then choosing η small enough. This proves Theorem 5.

Proof of Theorem 6

Proof of Theorem 6 proceeds by first giving a basic reduction from GapCVP to $\text{GapSVP}_{1/\zeta}$ for some constant $\zeta < 1$ and then boosting the SVP-hardness by tensoring operation on the lattice. Let $\mathcal{L}_0$ be the instance of $\text{GapSVP}_{1/\zeta}$ produced by the basic reduction, i.e., for some parameter d, either $\lambda_1(\mathcal{L}_0(\mathbf{B})) \leq \zeta\sqrt{d}$ (YES case) or $\lambda_1(\mathcal{L}_0(\mathbf{B})) \geq \sqrt{d}$ (NO case). By taking the k-wise tensored lattice $\mathcal{L}_0^{\otimes k}$, it is easy to see that in the YES case,

$$\lambda_1(\mathcal{L}_0(\mathbf{B})) \leq \zeta\sqrt{d} \implies \lambda_1(\mathcal{L}_0^{\otimes k}(\mathbf{B})) \leq \zeta^k\sqrt{d}^k.$$

On the other hand, in the NO case, suppose it were true that

$$\lambda_1(\mathcal{L}_0(\mathbf{B})) \geq \sqrt{d} \implies \lambda_1(\mathcal{L}_0^{\otimes k}(\mathbf{B})) \geq \sqrt{d}^k. \tag{14.7}$$

The resulting gap would be boosted to $(1/\zeta)^k$ and the size of instance $\mathcal{L}_0^{\otimes k}$ would be $(size(\mathcal{L}_0))^k$. By choosing k appropriately, it would prove $2^{(\log n)^{1-\varepsilon}}$ hardness for SVP, i.e., Theorem 6. But, as we shall see, the implication in (14.7) is false for a general lattice. However, the implication does hold for the *specific* lattice $\mathcal{L}_0(\mathbf{B})$ produced in the NO Case in Khot's [18] reduction. Though he did not prove that (14.7) holds for his lattice, by using a slight variant of the tensor product, he was able to boost hardness to $2^{(\log n)^{1/2-\varepsilon}}$. In a subsequent paper, Haviv and Regev [19] proved that (14.7) holds for Khot's lattice. This boosts hardness to $2^{(\log n)^{1-\varepsilon}}$. Let us first define the tensor product operation.

Tensor Product of Lattices

For two column vectors $\mathbf{u}$ and $\mathbf{v}$ of dimensions m_1 and m_2 respectively, we define their tensor product $\mathbf{u} \otimes \mathbf{v}$ as the $m_1 m_2$-dimensional column vector

$$\begin{pmatrix} u_1\mathbf{v} \\ \vdots \\ u_{m_1}\mathbf{v} \end{pmatrix}.$$

If we think of the coordinates of $\mathbf{u} \otimes \mathbf{v}$ as arranged in an $m_1 \times m_2$ matrix, we obtain the equivalent description of $\mathbf{u} \otimes \mathbf{v}$ as the matrix $\mathbf{u} \cdot \mathbf{v}^T$. Finally, for an $m_1 \times n_1$ matrix $\mathbf{A}$ and an $m_2 \times n_2$ matrix $\mathbf{B}$, one defines their tensor product $\mathbf{A} \otimes \mathbf{B}$ as the $m_1 m_2 \times n_1 n_2$ matrix

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

Let $\mathcal{L}_1$ be a lattice generated by $m_1 \times n_1$ matrix $\mathbf{B}_1$ and $\mathcal{L}_2$ be a lattice generated by $m_2 \times n_2$ matrix $\mathbf{B}_2$. 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 $m_1 m_2 \times n_1 n_2$ matrix $\mathbf{B}_1 \otimes \mathbf{B}_2$ and is denoted by $\mathcal{L} = \mathcal{L}_1 \otimes \mathcal{L}_2$. Equivalently, $\mathcal{L}$ is generated by the $n_1 n_2$ vectors obtained by taking the tensor of two column vectors, one from $\mathbf{B}_1$ and one from $\mathbf{B}_2$.

We are interested in the behavior of the shortest vector in a tensor product of lattices. It is easy to see that for any two lattices $\mathcal{L}_1$ and $\mathcal{L}_2$, we have

$$\lambda_1(\mathcal{L}_1 \otimes \mathcal{L}_2) \leq \lambda_1(\mathcal{L}_1) \cdot \lambda_1(\mathcal{L}_2). \tag{14.8}$$

Indeed, any two vectors $\mathbf{v}_1$ and $\mathbf{v}_2$ satisfy $\|\mathbf{v}_1 \otimes \mathbf{v}_2\| = \|\mathbf{v}_1\| \cdot \|\mathbf{v}_2\|$. Applying this to shortest nonzero vectors of $\mathcal{L}_1$ and $\mathcal{L}_2$ implies Inequality (14.8).

Inequality (14.8) has an analogue for linear codes, with λ_1 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 the product of their minimal distances. However, contrary to what one might expect, there exist lattices for which Inequality (14.8) is *strict*. The following lemma due to Steinberg shows this fact (his lattice is actually self-dual).

Lemma 3 ([43, Page 48]). *For any large enough n there exists an n-dimensional lattice $\mathcal{L}$ satisfying*

$$\lambda_1(\mathcal{L} \otimes \mathcal{L}) \leq \sqrt{n} \text{ and } \lambda_1(\mathcal{L}) = \Omega(\sqrt{n}).$$

Khot's Reduction

Let us imagine a hypothetical reduction from CVP to an instance $\mathcal{L}_0(\mathbf{B})$ of SVP that has the following properties (we assume w.l.o.g. that all lattice vectors have integer co-ordinates):

1. If the CVP instance is a YES instance, then there is a non-zero lattice vector with norm at most $\zeta\sqrt{d}$ where $\zeta < 1$ is a constant.
2. If the CVP instance is a NO instance, then any non-zero lattice vector has at least d non-zero co-ordinates.

In particular, this gives a gap-instance of SVP with gap $1/\zeta$. It is not hard to see that if we had such a *magic reduction*, then the k-wise tensor product of the lattice $\mathcal{L}_0$ in NO case would satisfy implication (14.7) and lead to a gap-instance with gap $(1/\zeta)^k$. Thus the tensor product would work provided that in the NO case, every non-zero lattice vector is not only *long*, but also has *many* non-zero co-ordinates. However, we do not know whether such a reduction exists. Nevertheless, Khot [18] gives a reduction that achieves somewhat weaker properties, but still good enough for boosting purposes. The following theorem summarizes his reduction (with a minor modification by Haviv and Regev [19]).

Theorem 7. *There is a constant $\zeta < 1$ and a polynomial-time randomized reduction from* SAT *to* SVP *that outputs a lattice basis $\mathbf{B}$ and integers n, d such that, $\mathcal{L}(\mathbf{B}) \subseteq \mathbb{Z}^n$, and w.h.p. the following holds:*

1. *If the* SAT *instance is a* YES *instance, then $\lambda_1(\mathcal{L}(\mathbf{B})) \leq \zeta \cdot \sqrt{d}$.*
2. *If the* SAT *instance is a* NO *instance, then every nonzero vector $\mathbf{v} \in \mathcal{L}(\mathbf{B})$*
   - *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 $\|\mathbf{v}\|_2 \geq d$*
   - *Or has a coordinate with absolute value at least $Q := d^{4d}$*

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

Boosting the SVP Hardness Factor

We boost the hardness factor using the standard tensor product of lattices. If $(\mathcal{L}_0(\mathbf{B}), d)$ is a YES instance of the SVP instance in Theorem 7, then clearly

$$\lambda_1(\mathcal{L}_0^{\otimes k}) \leq \zeta^k d^{k/2}. \tag{14.9}$$

When $(\mathcal{L}_0(\mathbf{B}), d)$ is a NO instance, Haviv and Regev [19] show that any nonzero vector of $\mathcal{L}_0^{\otimes k}$ has norm at least $d^{k/2}$, i.e.,

$$\lambda_1(\mathcal{L}_0^{\otimes k}) \geq d^{k/2}. \tag{14.10}$$

This yields a gap of ζ^k between the two cases. Inequality (14.10) easily follows by induction from the central lemma of Haviv and Regev stated below, which shows that NO instances "tensor nicely." We skip the proof of this lemma.

Lemma 4. *Let* $(\mathcal{L}_0(\mathbf{B}), d)$ *be a* NO *instance of* SVP *given in Theorem 7. Then for any lattice* $\mathcal{L}$*,*

$$\lambda_1(\mathcal{L}_0 \otimes \mathcal{L}) \geq \sqrt{d} \cdot \lambda_1(\mathcal{L}).$$

References

1. D. Micciancio, S. Goldwasser. Complexity of lattice problems, A cryptographic perspective. Kluwer Academic Publishers, 2002
2. R. Kumar, D. Sivakumar. Complexity of SVP – A reader's digest. SIGACT News, 32(3), Complexity Theory Column (ed. L. Hemaspaandra), 2001, pp 40–52
3. O. Regev. On the Complexity of Lattice Problems with polynomial Approximation Factors. In Proc. of the LLL+25 Conference, Caen, France, June 29-July 1, 2007
4. C.F. Gauss. Disquisitiones arithmeticae. (leipzig 1801), art. 171. Yale University. Press, 1966. English translation by A.A. Clarke
5. H. Minkowski. Geometrie der zahlen. Leizpig, Tuebner, 1910
6. A.K. Lenstra, H.W. Lenstra, L. Lovász. Factoring polynomials with rational coefficients. Mathematische Ann., 261, 1982, pp 513–534
7. J.C. Lagarias, A.M. Odlyzko. Solving low-density subset sum problems. Journal of the ACM, 32(1), 1985, pp 229–246
8. S. Landau, G.L. Miller. Solvability of radicals is in polynomial time. Journal of Computer and Systems Sciences, 30(2), 1985, pp 179–208
9. H.W. Lenstra. Integer programming with a fixed number of variables. Tech. Report 81–03, Univ. of Amsterdam, Amstredam, 1981
10. R. Kannan. Improved algorithms for integer programming and related lattice problems. In Proc. of the 15th Annual ACM Symposium on Theory of Computing, 1983, pp 193–206
11. C.P. Schnorr. A hierarchy of polynomial-time basis reduction algorithms. In Proc. of Conference on Algorithms, Péecs (Hungary), 1985, pp 375–386
12. R. Kannan. Minkowski's convex body theorem and integer programming. Mathematics of Operations Research, 12:415–440, 1987
13. M. Ajtai, R. Kumar, D. Sivakumar. A sieve algorithm for the shortest lattice vector problem. In Proc. of the $33rd$ Annual ACM Symposium on the Theory of Computing, 2001, pp 601–610

14. P. van Emde Boas. Another NP-complete problem and the complexity of computing short vectors in a lattice. Tech. Report 81-04, Mathematische Instiut, University of Amsterdam, 1981
15. M. Ajtai. The shortest vector problem in L_2 is NP-hard for randomized reductions. In Proc. of the 30th Annual ACM Symposium on the Theory of Computing, 1998, pp 10–19
16. J.Y. Cai, A. Nerurkar. Approximating the SVP to within a factor $(1 + 1/\dim^{\varepsilon})$ is NP-hard under randomized reductions. In Proc. of the 13th Annual IEEE Conference on Computational Complexity, 1998, pp 151–158
17. D. Micciancio. The shortest vector problem is NP-hard to approximate to within some constant. In Proc. of the 39th IEEE Symposium on Foundations of Computer Science, 1998
18. S. Khot. Hardness of approximating the shortest vector problem in lattices. Journal of the ACM, 52(5), 2005, pp 789–808
19. I. Haviv, O. Regev. Tensor-based hardness of the Shortest Vector Problem to within almost polynomial factors. To appear in Proc. of the 39th Annual ACM Symposium on the Theory of Computing, 2007
20. M. Ajtai. Generating hard instances of lattice problems. In Proc. of the 28th Annual ACM Symposium on the Theory of Computing, 1996, pp 99–108
21. M. Ajtai, C. Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In Proc. of the 29th Annual ACM Symposium on the Theory of Computing, 1997, pp 284–293
22. J.Y. Cai, A. Nerurkar. An improved worst-case to average-case connection for lattice problems. In 38th IEEE Symposium on Foundations of Computer Science, 1997
23. J.Y. Cai. Applications of a new transference theorem to Ajtai's connection factor. In Proc. of the 14th Annual IEEE Conference on Computational Complexity, 1999
24. O. Regev. New lattice based cryptographic constructions. To appear in Proc. of the 35th Annual ACM Symposium on the Theory of Computing, 2003
25. O. Goldreich, D. Micciancio, S. Safra, J.P. Seifert. Approximating shortest lattice vectors is not harder than approximating closest lattice vectors. Information Processing Letters, 1999
26. S. Arora, L. Babai, J. Stern, E.Z. Sweedyk. The hardness of approximate optima in lattices, codes and systems of linear equations. Journal of Computer and Systems Sciences (54), 1997, pp 317–331
27. I. Dinur, G. Kindler, S. Safra. Approximating CVP to within almost-polynomial factors is NP-hard. In Proc. of the 39th IEEE Symposium on Foundations of Computer Science, 1998
28. D. Micciancio. The hardness of the closest vector problem with preprocessing. IEEE Transactions on Information Theory, vol 47(3), 2001, pp 1212–1215
29. U. Feige and D. Micciancio. The inapproximability of lattice and coding problems with preprocessing. Computational Complexity, 2002, pp 44–52
30. O. Regev. Improved inapproximability of lattice and coding problems with preprocessing. IEEE Transactions on Information Theory, 50(9), 2004, pp 2031–2037
31. M. Alekhnovich, S. Khot, G. Kindler, N. Vishnoi. Hardness of approximating the closest vector problem with pre-processing. In Proc. of the 46th IEEE Symposium on Foundations of Computer Science, 2005
32. D. Aharonov, O. Regev. Lattice problems in NP ∩ coNP. Journal of the ACM, 52(5), 2005, pp 749–765
33. I. Haviv, O. Regev. Hardness of the covering radius problem on lattices. In Proc. of the 21*st* Annual IEEE Computational Complexity Conference, 2006
34. J. Blömer, J.P. Seifert. On the complexity of compuing short linearly independent vectors and short bases in a lattice. In Proc. of the 31*st* Annual ACM Symposium on the Theory of Computing, 1999, pp 711–720
35. O. Regev, R. Rosen. Lattice problems and norm embeddings. In Proc. of the 38th Annual ACM Symposium on the Theory of Computing, 2006
36. I. Dinur. Approximating SVP_{∞} to within almost polynomial factors is NP-hard. Proc. of the 4th Italian Conference on Algorithms and Complexity, LNCS, vol 1767, Springer, 2000
37. W. Banaszczyk. New bounds in some transference theorems in the geometry of numbers. Mathematische Annalen, vol. 296, 1993, pp 625–635
38. O. Goldreich, S. Goldwasser. On the limits of non-approximability of lattice problems. In Proc. of the 30th Annual ACM Symposium on the Theory of Computing, 1998, pp 1–9

39. V. Guruswami, D. Micciancio, O. Regev. The complexity of the covering radius problem on lattices. Computational Complexity 14(2), 2005, pp 90–121
40. S. Arora and S. Safra. Probabilistic checking of proofs : A new characterization of NP. Journal of the ACM, 45(1), 1998, pp 70–122
41. S. Arora, C. Lund, R. Motwani, M. Sudan, M. Szegedy. Proof verification and the hardness of approximation problems. Journal of the ACM, 45(3), 1998, pp 501–555
42. R. Raz. A parallel repetition theorem. SIAM Journal of Computing, 27(3), 1998, pp 763–803
43. J. Milnor, D. Husemoller. Symmetric bilinear forms. Springer, Berlin, 1973
44. J.C. Lagarias, H.W. Lenstra, C.P. Schnorr. Korkine-Zolotarev bases and successive minima of a lattice and its reciprocal lattice. Combinatorica, vol 10, 1990, pp 333–348