On the Complexity of Computing Short Linearly Independent Vectors and Short Bases in a Lattice

Johannes Blömer*[1] and Jean-Pierre Seifert**[2]

[1] Institut für Theoretische Informatik, ETH Zürich, ETH Zentrum
CH-8092 Zürich, SWITZERLAND
bloemer@inf.ethz.ch.
[2] Department of Mathematics and Computer Science, University of Frankfurt
60054 Frankfurt on the Main, P.O. Box 11 19 32, GERMANY
seifert@cs.uni-frankfurt.de

Abstract. Motivated by Ajtai's worst-case to average-case reduction for lattice problems, we study the complexity of computing short linearly independent vectors (short basis) in a lattice. We show that approximating the length of a shortest set of linearly independent vectors (shortest basis) within any constant factor is NP-hard. Under the assumption that problems in NP cannot be solved in $\mathsf{DTIME}(n^{\mathrm{polylog}(n)})$ we show that no polynomial time algorithm can approximate the length of a shortest set of linearly independent vectors (shortest basis) within a factor of $2^{\log^{1-\epsilon}(n)}$, $\epsilon > 0$ arbitrary, but fixed. Finally, we obtain results on the limits of non-approximability for computing short linearly independent vectors (short basis). Our strongest result in this direction states that under reasonable complexity-theoretic assumptions, approximating the length of a shortest set of linearly independent vectors (shortest basis) within a factor of $n/\sqrt{\log(n)}$ is not NP-hard.

Key Words. Algorithmic geometry of numbers, lattices, worst-case complexity, average-case complexity, shortest lattice basis, shortest vector, closest vector, hardness of approximations.

1 Introduction

Recently, interest in the geometry of numbers has increased due to Ajtai's discovery of the connection between the average-case complexity and the worst-case complexity of some lattice problems. More precisely, for every $n \in \mathbb{N}$, Ajtai defined a natural class Λ_n of lattices and proved the following theorem

Theorem (Ajtai [A1]). *Assume there is a probabilistic polynomial time algorithm $\mathcal{A}$ that, for a uniformly chosen lattice from the class Λ_n, finds a non-zero*

* Research supported by Schweizer Nationalfonds, grant No. 21-49626.96.
** Done while visiting ETH - Institut für Theoretische Informatik.

vector $\mathbf{v}$ *of length at most* n*. Then there is a probabilistic polynomial time algorithm* $\mathcal{B}$ *that, for any given lattice* $\mathsf{L} \subset \mathbb{R}^n$ *and for some constants* c_0, c_1, c_2*, with high probability will solve either one of the following three problems.*

IVP (INDEPENDENT VECTORS PROBLEM)
Find n *linearly independent vectors* $\mathbf{v}_1, \ldots, \mathbf{v}_n$ *in* L*, whose length is up to some factor of* n^{c_0}*, smallest possible. Here the length of a set of vectors is defined as* $\max_{1 \leq i \leq n} \|\mathbf{v}_i\|$.
GVP (GENERATING VECTORS PROBLEM)
Find a basis $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ *for the lattice* L*, whose length is up to some factor of* n^{c_1} *smallest possible. The length of a basis is defined as* $\max_{1 \leq i \leq n} \|\mathbf{b}_i\|$,
SVP (SHORTEST VECTOR PROBLEM)
Find the length of a shortest non-zero vector in L *within a factor of* n^{c_2}.

Improving upon Ajtai's original values, Cai/Nerurkar [CN] and Cai [Ca1], showed that we may take any $c_0 > 3, c_1 > 3.5$, and $c_2 > 4$.

These results clearly raise the question, how difficult the above mentioned lattice problems are. At the time of Ajtai's discovery none of these problems was known to be NP-complete. For all three problems the best polynomial time approximation algorithm is based on the L^3-algorithm (see for example [L]). The algorithms achieve approximation factors that are exponential in the dimension of the lattice. After Ajtai's discovery most effort to prove hardness results for IVP, GVP, or SVP has been directed towards the problem SVP. This is due to the importance of SVP in other areas of computer science, its connection to cryptography as evidenced by the Ajtai/Dwork cryptosystem [AD], and due to its long history. It is also important to note that computing short vectors in a random lattice chosen from Λ_n cannot be difficult, unless computing a shortest vector in a lattice is difficult in the worst-case. Currently, the best hardness result for SVP is due to Micciancio [M]. Building on work of Ajtai [A2], Micciancio proved that approximating the length of a shortest vector within a factor of $\approx \sqrt{2}$ is NP-hard under randomized reductions.

If combined with Ajtai's theorem, this hardness result for approximating the length of a shortest vector is still far from providing a reduction from a provably worst-case difficult problem to an average-case problem. Moreover, we have reason to believe that such a reduction cannot be achieved if one works with the problem SVP. Let us elaborate this a little bit further. In Ajtai's proof as well as in the subsequent improvements by Cai/Nerurkar and Cai, the problem IVP is directly reduced to a random instance in Λ_n. The reductions for GVP and SVP are obtained from this result for IVP by invoking general results from the geometry of numbers. In particular, the only known reduction of SVP to IVP uses so-called transference theorems. These theorems relate a lattice and its so-called dual lattice. Examples of Conway and Thompson (see [MH]) show that using these theorems in a reduction of SVP to IVP inevitably leads to a loss of n in the approximation factor. On the other hand, Goldreich and Goldwasser show that SVP is probably not hard for the approximation factor $\sqrt{n/\log(n)}$.

Having said all this, it seems to be natural to study the complexity of problems IVP and GVP. This is the purpose of this paper. Although the results we obtain are far from establishing hardness results for these problems that are close to the hardness results required by Ajtai's theorem, our results are much stronger than the known non-approximability results for SVP. In particular, we first show that for every constant C, solving IVP or GVP within a factor of C is NP-hard. Using the widely accepted assumption that problems in NP cannot be solved in $\mathsf{DTIME}(n^{\text{polylog}(n)})$, we also rule out polynomial time algorithms solving the problem IVP or GVP within a factor of $2^{\log^{1-\epsilon}(n)}$, where $\epsilon > 0$ is arbitrarily small, but fixed. A result of this form is often understood as providing strong evidence that the corresponding problem is in fact hard to approximate within some polynomial factor (see [AL]). We believe that IVP and GVP are hard to approximate within a polynomial factor, but the methods we use do not seem capable of proving such a result. We note that compared to the methods in [A2,M] our constructions and proofs are relatively simple. Our methods are variations of the methods used in [ABSS,AL] for the closest vector problem.

We also generalize methods in [LLS] and [GG] to obtain results on the limits of non-approximability for the problems IVP and GVP. We show that under Karp-reductions approximating IVP and GVP within a factor of $n^{3/2}$ is not NP-hard unless NP = co-NP. This result is obtained by a direct generalization of the methods in [LLS]. Combining methods from [LLS] and [GG], we also show that, under Karp-reductions, approximating IVP and GVP within a factor of $n/\sqrt{\log(n)}$ is not NP-hard unless the polynomial hierarchy collapses to its second level. Therefore, it is unlikely that non-approximability results as required by the current versions of Ajtai's theorem are achievable (see also [GG]). This leads to one of the main questions this paper raises. We believe that a hardness result for approximating IVP within a factor of $n^{1-\epsilon}, \epsilon > 0$ arbitrary, may be possible. Hence, in Ajtai's theorem, can the approximation factor for IVP be improved to $n^{1-\epsilon}, \epsilon > 0$?

The paper is organized as follows. In Section 2 we state the main definitions. Section 3 contains an NP-completeness proof for problems IVP and GVP. The construction presented there is fundamental for the non-approximability results in Section 4. In Section 5, we present our results on the limits of non-approximability for problems IVP and GVP.

2 Definitions

$\mathbb{R}^m$ is the m-dimensional Euclidean real vector space endowed with the Euclidean inner product $\langle \cdot, \cdot \rangle$ on $\mathbb{R}^m$ and the Euclidean norm $||\mathbf{v}||^2 = \sum_{i=1}^m \mathbf{v}_i^2$ for $\mathbf{v} \in \mathbb{R}^m$.

A *lattice* L is a discrete additive subgroup of $\mathbb{R}^m$. Its *rank*, denoted by rank(L), is the dimension of the $\mathbb{R}$-subspace span(L) that it spans. Each lattice L of rank n has a *basis*, i.e., a sequence $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ of n elements of L that generate L as an abelian group. For a lattice L, $\nu(\mathsf{L})$ is the smallest real number r such that there are rank(L) linear independent vectors in L of length at most r that generate L. The i^{th} *successive minimum* $\lambda_i(\mathsf{L})$ of a lattice L is the smallest real number r such that there are i linear independent vectors in L of length at most r. Furthermore, $\mu(\mathbf{x}, \mathsf{L})$ is the Euclidean distance from $\mathbf{x} \in \mathbb{R}^m$ to the closest vector in L. It may be tempting to assume that $\lambda_{\mathsf{rank}(\mathsf{L})} = \nu(\mathsf{L})$. However, in general $\nu(\mathsf{L})$ is strictly larger than $\lambda_{\mathsf{rank}(\mathsf{L})}$ (see for example [LLS]). In [CN] it is shown that

$$\nu(\mathsf{L}) \leq (\sqrt{\mathrm{rank}(\mathsf{L})}/2)\lambda_{\mathsf{rank}(\mathsf{L})}.$$

Examples in [LLS] show that this is best possible.

An important and easily computable invariant of a lattice is the *determinant* $\det(\mathsf{L})$ of a lattice L. It is defined by choosing any basis $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ for L and then setting

$$\det(\mathsf{L})^2 = \det[\langle \mathbf{b}_i, \mathbf{b}_j \rangle]_{1 \leq i,j \leq n}.$$

Minkowski's classical theorems on successive minima provide simple upper bounds for the values of λ_i in term of the determinant of a lattice (see [C]).

In the following definitions we state some fundamental computational problems related to lattices. The purpose of this paper is to study the complexity of these problems. We always assume that a lattice L is given by a basis $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ generating L.

Definition 1. SHORTEST LINEARLY INDEPENDENT VECTORS PROBLEM (IVP)
GIVEN: A lattice $\mathsf{L} \subseteq \mathbb{Q}^m$ of rank n and a positive number $r \in \mathbb{R}$
DECIDE: Whether there are n linear independent vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathsf{L}$ with

$$\max_{1 \leq i \leq n} \|\mathbf{v}_i\| \leq r$$

Definition 2. SHORTEST GENERATING VECTORS PROBLEM (GVP)
GIVEN: A lattice $\mathsf{L} \subseteq \mathbb{Q}^m$ of rank n and a positive number $r \in \mathbb{R}$
DECIDE: Whether there are n linear independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathsf{L}$ that generate L and

$$\max_{1 \leq i \leq n} \|\mathbf{b}_i\| \leq r$$

Definition 3. The promise problem GAPIVP$_g$, where g is a gap function, is defined as follows:

> YES-instances are pairs (L, r), where $\mathsf{L} \subseteq \mathbb{Q}^m$ is a lattice of rank n, $r \in \mathbb{R}_+$ and $\lambda_n(\mathsf{L}) \leq r$
> NO-instances are pairs (L, r), where $\mathsf{L} \subseteq \mathbb{Q}^m$ is a lattice of rank n, $r \in \mathbb{R}_+$ and $\lambda_n(\mathsf{L}) > g(n) \cdot r$

Definition 4. The promise problem GAPGVP$_g$, where g is a gap function, is defined as follows:

> YES-instances are pairs (L, r) where $\mathsf{L} \subseteq \mathbb{Q}^m$ is a lattice of rank n, $r \in \mathbb{R}_+$ and $\nu(\mathsf{L}) \leq r$
> NO-instances are pairs (L, r) where $\mathsf{L} \subseteq \mathbb{Q}^m$ is a lattice of rank n, $r \in \mathbb{R}_+$ and $\nu(\mathsf{L}) > g(n) \cdot r$

For later purposes we also need to define the following problems. Previous research on the complexity of lattice problems has focused on these problems.

Definition 5. SHORTEST VECTOR PROBLEM (SVP)
GIVEN: A lattice $\mathsf{L} \subseteq \mathbb{R}^m$ of rank n and a positive number $r \in \mathbb{R}$
DECIDE: Whether there exist a non-zero vector $\mathbf{v} \in \mathsf{L}$ with

$$||\mathbf{v}|| \leq r$$

Definition 6. The promise problem GAPSVP$_g$ where g is a gap function, is defined as follows:

> YES-instances are pairs (L, r) where $\mathsf{L} \subseteq \mathbb{Q}^m$ is a lattice of rank n, $r \in \mathbb{R}_+$ and $\lambda_1(\mathsf{L}) \leq r$
> NO-instances are pairs (L, r) where $\mathsf{L} \subseteq \mathbb{Q}^m$ is a lattice of rank n, $r \in \mathbb{R}_+$ and $\lambda_1(\mathsf{L}) > g(n) \cdot r$

Definition 7. CLOSEST VECTOR PROBLEM (CVP)
GIVEN: A lattice $\mathsf{L} \subseteq \mathbb{Q}^m$ of rank n, a vector $\mathbf{x} \in \mathbb{Q}^m$ and a positive number $r \in \mathbb{R}$
DECIDE: Whether there exist a vector $\mathbf{v} \in \mathsf{L}$ with

$$||\mathbf{x} - \mathbf{v}|| \leq r$$

Definition 8. The promise problem GAPCVP$_g$ where g is a gap function, is defined as follows:

> YES-instances are triples $(\mathsf{L}, \mathbf{x}, r)$ where $\mathsf{L} \subseteq \mathbb{Q}^m$ is a lattice of rank n, $\mathbf{x} \in \mathbb{Q}^m$ and $r \in \mathbb{R}_+$ satisfying $\mu(\mathbf{x}, \mathsf{L}) \leq r$
> NO-instances are triples $(\mathsf{L}, \mathbf{x}, r)$ where $\mathsf{L} \subseteq \mathbb{Q}^m$ is a lattice of rank n, $\mathbf{x} \in \mathbb{Q}^m$ and $r \in \mathbb{R}_+$ satisfying $\mu(\mathbf{x}, \mathsf{L}) > g(n) \cdot r$

Strictly speaking, to obtain well-defined decision problems the bounds r in the definitions above always need to be rational numbers. In all our constructions and proofs naturally these bounds are square roots of rational numbers. It is always straightforward to resolve the problems caused by real numbers. To keep the notation simple, for the rest of the paper, we will ignore these problems.

3 IVP and GVP are NP-complete

In this section we show that the problems IVP and GVP are NP-complete. We include these proofs to motivate the proofs for the non-approximability results of the following section.

Theorem 1. *The problems* IVP *and* GVP *are* NP*-complete.*

Proof. Both problems are in NP, since in polynomial time we can decide whether

(i) n vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$ are linearly independent.
(ii) A vector $\mathbf{v}$ is an element of a given lattice L [BK].
(iii) n vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$ are a basis for a given lattice [BK].

To show that IVP is NP-hard we reduce CVP to IVP. Clearly, we can restrict ourselves to lattices $\mathsf{L} \subset \mathbb{Z}^m$. Let $(\mathsf{L}, \mathbf{v}, r)$ be an instance of CVP. To reduce the instance of CVP to an instance of IVP, let $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ be a basis of L. First we choose a constant D such that $D > \max\{r, \lambda_n(\mathsf{L})\}$. By Minkowski's theorem on successive minima we may take $D = \max\{r+1, \lceil n^{n/2} \det(\mathsf{L}) \rceil\}$ (This is the only place where we need integral lattices.). Since $\det(\mathsf{L})$ can be computed in polynomial time, D can be computed in polynomial time. Let M be the lattice generated by the columns of the matrix

$$\begin{bmatrix} \mathbf{b}_1 \; \mathbf{b}_2 \cdots \mathbf{b}_n \; \mathbf{v} \\ 0 \;\; 0 \;\; \cdots \;\; 0 \;\; D \end{bmatrix} = \begin{bmatrix} \mathbf{d}_1 \; \mathbf{d}_2 \cdots \mathbf{d}_n \; \mathbf{d}_{n+1} \end{bmatrix}$$

The instance of IVP is defined by $(\mathsf{M}, \sqrt{r^2 + D^2})$.

Assume first that $(\mathsf{L}, \mathbf{v}, r)$ is a YES-instance of CVP. Then there is a vector $\mathbf{w} = \sum_{i=1}^n c_i \mathbf{b}_i \in \mathsf{L}$ such that $\|\mathbf{w} - \mathbf{v}\| \leq r$. By construction of D, the lattice L contains n linearly independent vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$ with $\|\mathbf{v}_i\| \leq \lambda_n(\mathsf{L}) \leq D$ for all i. The vectors $(\mathbf{v}_1, 0)^\top, \ldots, (\mathbf{v}_n, 0)^\top, (\mathbf{w} - \mathbf{v}, D)^\top$ are $n+1$ linearly independent vectors in M, whose length is bounded by $\sqrt{r^2 + D^2}$.

Now assume that $(\mathsf{L}, \mathbf{v}, r)$ is a NO-instance of CVP. Then any vector $\mathbf{w} \in \mathsf{L}$ satisfies $\|\mathbf{w} - \mathbf{v}\| > r$. In every set of $n+1$ linearly independent vectors $\{\mathbf{w}_1, \ldots, \mathbf{w}_{n+1}\} \subseteq \mathsf{M}$ at least one vector must depend on $\mathbf{d}_{n+1}$, say,

$$\mathbf{w}_{n+1} = \sum_{i=1}^{n+1} c_i \mathbf{d}_i, c_{n+1} \neq 0.$$

If $|c_{n+1}| \geq 2$, then

$$\|\mathbf{w}_{n+1}\| \geq \sqrt{4D^2} > \sqrt{r^2 + D^2}.$$

If $c_{n+1} = \pm 1$, say $c_{n+1} = -1$, then $\|\mathbf{w}_{n+1}\| > \sqrt{r^2 + D^2}$. Otherwise, $\| \sum_{i=1}^n c_i \mathbf{b}_i - \mathbf{v}\| \leq r$, contradicting the fact that $(\mathsf{L}, \mathbf{v}, r)$ is a NO-instance of CVP.

To show that GVP is NP-complete we use the same reduction. We only need to increase D slightly. In [CN] it is shown that for any lattice L we have $\nu(\mathsf{L}) \leq (\sqrt{\mathrm{rank}(\mathsf{L})}/2)\lambda_n(\mathsf{L})$. Hence by Minkowski's theorem on successive minima $n^{(n+1)/2} \det(\mathsf{L})$ is an upper bound on $\nu(\mathsf{L})$. To reduce CVP to GVP we use the construction from above with

$$D = \max\{r+1, \lceil n^{(n+1)/2} \det(\mathsf{L}) \rceil\}.$$

For any lattice $\lambda_n(\mathsf{L}) \leq \nu(\mathsf{L})$, therefore a NO-instance of CVP will be mapped onto a NO-instance of GVP. To see that a YES-instance of CVP will be mapped onto a YES-instance of GVP let $\mathbf{v}_1, \ldots, \mathbf{v}_n$ be a basis of L with $\|\mathbf{v}_i\| \leq \nu(\mathsf{L}) \leq D$. Note that $(\mathbf{v}, D)^\top$ can be written as a linear combination of the vectors $(\mathbf{v}_1, 0)^\top, \ldots, (\mathbf{v}_n, 0)^\top, (\mathbf{w} - \mathbf{v}, D)^\top$ with integer coefficients. Hence the vectors $(\mathbf{v}_1, 0)^\top, \ldots, (\mathbf{v}_n, 0)^\top, (\mathbf{w} - \mathbf{v}, D)^\top$ are a basis for M. The length of these vectors is bounded by $\sqrt{r^2 + D^2}$. □

We note that the same reduction can be used to show the following result.

Corollary 1. *Given an oracle that solves* Ivp *or* Gvp *exactly, in polynomial time* Svp *and* Cvp *can be solved exactly.*

Proof. The result for Cvp follows by the reduction used above. To obtain the result for Svp we use a recent result by Goldreich and Seifert that shows that Svp can be solved exactly in polynomial time, given an oracle that solves Cvp exactly. □

We do not know how to obtain an approximation to Cvp or to Svp given an oracle that approximately solves Ivp or Gvp. In particular, because of the value of D, the construction used above cannot be used to transform approximation algorithms for Ivp to approximation algorithms for Cvp. In general, D is a not at all related to $\mu(\mathbf{v}, \mathsf{L})$ for $\mathbf{v} \in \mathbb{R}^m$. However, every approximation algorithm for Ivp, if applied to the construction above, will produce an estimate for $\mu(\mathbf{v}, \mathsf{L})$ that depends on D. This will not be a useful approximation for $\mu(\mathbf{v}, L)$.

However, to obtain non-approximability results for Ivp, we do not work with arbitrary lattices. In fact, non-approximability results for Cvp shown in [ABSS,AL] rely on very special lattices. For these lattices L we have more precise information about the successive minima and about the distance $\mu(\mathbf{v}, \mathsf{L})$ of a specific vector $\mathbf{v}$ to the lattice L. Exploiting this information allows us to use a variant of the construction from above to obtain non-approximability results for Ivp and Gvp. Keeping these remarks in mind will help understanding the constructions and proofs of the following section.

4 Non-approximability results for Ivp and Gvp

In this section we prove the non-approximability results for Ivp and Gvp. First we need to review results from [AL].

4.1 The Min Label Cover Problem

In the following $G = (V_1, V_2, E)$ denotes a bipartite graph, $\mathcal{A}$ a set of labels for the vertices in $V_1 \cup V_2$, and Π_e a partial relation $\Pi_e : \mathcal{A} \to \mathcal{A}$ describing the admissible pairs of labels for every edge $e \in E$. We adapt the notation of [AL,ABSS]. A *labeling* of $G = (V_1, V_2, E)$ is a pair $(\mathcal{P}_1, \mathcal{P}_2)$ of functions $\mathcal{P}_i : V_i \to 2^{\mathcal{A}}$, $i = 1, 2$, assigning each vertex in $V_1 \cup V_2$ a possibly empty set of labels.

Let $(\mathcal{P}_1, \mathcal{P}_2)$ a labeling of $G = (V_1, V_2, E)$ and $e = (v_1, v_2)$, $v_1 \in V_1$, $v_2 \in V_2$, an edge of G. We call $e = (v_1, v_2)$ *covered* iff $\mathcal{P}_1(v_1) \neq \emptyset$, $\mathcal{P}_2(v_2) \neq \emptyset$ and for all labels $b_2 \in \mathcal{P}_2(v_2)$ there is a label $b_1 \in \mathcal{P}_1(v_1)$ such that $\Pi_e(b_1) = b_2$. A labeling $(\mathcal{P}_1, \mathcal{P}_2)$ of $G = (V_1, V_2, E)$ is called a *cover* of G iff every edge of G is covered by the labeling $(\mathcal{P}_1, \mathcal{P}_2)$.

The *cost* of a labeling $(\mathcal{P}_1, \mathcal{P}_2)$ for a graph $G = (V_1, V_2, E)$ is defined as

$$cost(\mathcal{P}_1, \mathcal{P}_2) = \sum_{v \in V_1} |\mathcal{P}_1(v)|.$$

Definition 9. MIN LABEL COVER (MINLC)
INSTANCE: A (d_1, d_2)-regular bipartite graph $G = (V_1, V_2, E)$, a set of labels $\mathcal{A} = \{1, \dots, N\}$, $N \in \mathbb{N}_+$, and for every edge $e \in E$ a partial relation $\Pi_e : \mathcal{A} \to \mathcal{A}$ such that $\Pi_e^{-1}(1) \neq \emptyset$ for the distinguished label $1 \in \mathcal{A}$
SOLUTION: A cover $(\mathcal{P}_1, \mathcal{P}_2)$ of G. The minimal cost for an instance I will be denoted by $opt_{\text{MINLC}}(I)$.

In the above definition we can always ensure the existence of a cover with cost at most $|V_1|N$; simply let $\mathcal{P}_2(v_2) = \mathcal{A}$ for all $v_2 \in V_2$ and $\mathcal{P}_1(v_1) = \mathcal{A}$ for all $v_1 \in V_1$. Therefore,

$$opt_{\text{MINLC}}(I) \leq N \cdot |V_1|, \text{ for all instances } I.$$

The following lemma is due to Arora and Lund [AL].

Lemma 1. *There is a constant $g > 1$ and a polynomial-time transformation τ from* 3-SAT *to* MIN LABEL COVER *such that for all instances φ we have:*

1. $\varphi \in$ 3-SAT $\Longrightarrow opt_{\text{MINLC}}(\tau(\varphi)) = 1 \cdot |V_1|$
   $\varphi \notin$ 3-SAT $\Longrightarrow opt_{\text{MINLC}}(\tau(\varphi)) > g \cdot |V_1|$.
2. *$|V_1|$ is the number of clauses in φ.*
3. *The bipartite graph of the* MIN LABEL COVER *instance $\tau(\varphi)$ is $(3,5)$-regular.*
4. *The number N of labels of the instance $\tau(\varphi)$ is 8.*

Building on work in [ABSS], Arora and Lund also show the following reduction from MIN LABEL COVER to CVP.

Lemma 2. *Let g be the constant from the previous lemma. There is a polynomial-time transformation from* MIN LABEL COVER *to* CVP *that for all instances $I = (V_1, V_2, E, \mathcal{A})$ of* MIN LABEL COVER *generates a lattice $\mathsf{L} = \mathsf{L}(\mathbf{b}_1, \dots, \mathbf{b}_n)$ and a vector $\mathbf{b}_{n+1}$ with the following properties:*

1. $\mathsf{L} \subset \mathbb{Z}^m, m = 9|E| + 8|V_1|$ *and* $n = 8|V_1| + 8|V_2|$.
2. *Every basis vector $\mathbf{b}_i, i = 1, \dots, n$, has at most 25 non-zero coordinates.*
3. *The first $9|E|$ coordinates in $\mathbf{b}_i, i = 1, \dots, n+1$, are either 0 or $K := 9|V_1|$. The remaining coordinates are either 0 or 1.*
4. $opt_{\text{MINLC}}(I) = 1 \cdot |V_1| \Longrightarrow \mu(\mathbf{b}_{n+1}, \mathsf{L}) = \sqrt{|V_1|}$
   $opt_{\text{MINLC}}(I) > g \cdot |V_1| \Longrightarrow \forall \beta \in \mathbb{Z} \setminus \{0\} : \mu(\beta \cdot \mathbf{b}_{n+1}, \mathsf{L}) > \sqrt{g} \cdot \sqrt{|V_1|}$.

   Moreover, in the first case, there is a vector $\mathbf{v} \in \mathsf{L}$ such that $\mathbf{b}_{n+1} - \mathbf{v}$ has among its last $8|V_1|$ coordinates exactly $|V_1|$ coordinates being 1.
   In the second case, for all $\mathbf{v} \in \mathsf{L}$ and all $\beta \in \mathbb{Z} \setminus \{0\}$, if the first $9|E|$ coordinates of $\beta \cdot \mathbf{b}_{n+1} - \mathbf{v}$ are zero, then more than $g|V_1|$ of the last coordinates in $\beta \cdot \mathbf{b}_{n+1} - \mathbf{v}$ are non-zero.

Using a construction from [ABSS] we will strengthen this lemma, such that we only require 0, 1-vectors in the construction.

Corollary 2. *There is a polynomial-time transformation from the problem* Min Label Cover *to* Cvp *that for all instances $I = (V_1, V_2, E, \mathcal{A})$ of* Min Label Cover *generates a lattice $\mathsf{L}' = \mathsf{L}(\mathbf{b}'_1, \ldots, \mathbf{b}'_n)$ and a target vector $\mathbf{b}'_{n+1}$ with the following properties:*

1. $\mathsf{L}' \subset \mathbb{Z}^m, m = 9K|E| + 8|V_1|$ *and* $n = 8|V_1| + 8|V_2|$.
2. $\mathbf{b}'_i \in \{0,1\}^m, i = 1, \ldots, n+1,$ *and* $\mathbf{b}'_i$ *has* $\leq 25K$ *non-zero coordinates,* $i = 1, \ldots, n$.
3. $opt_{\mathrm{MinLC}}(I) = 1 \cdot |V_1| \Longrightarrow \mu(\mathbf{b}'_{n+1}, \mathsf{L}') = 1 \cdot \sqrt{|V_1|}$
   $opt_{\mathrm{MinLC}}(I) > g \cdot |V_1| \Longrightarrow \forall \beta \in \mathbb{Z} \setminus \{0\} : \mu(\beta \cdot \mathbf{b}'_{n+1}, \mathsf{L}') > \sqrt{g} \cdot \sqrt{|V_1|}$.

   Moreover, in the first case, there is a vector $\mathbf{v}' \in \mathsf{L}'$ such that $\mathbf{b}'_{n+1} - \mathbf{v}'$ has exactly $|V_1|$ non-zero coordinates.
   In the second case, for all $\mathbf{v}' \in \mathsf{L}'$ and all $\beta \in \mathbb{Z} \setminus \{0\}$, the difference vector $\beta \cdot \mathbf{b}'_{n+1} - \mathbf{v}'$ has more than $g \cdot |V_1|$ non-zero coordinates.

Proof. Consider the vectors $\mathbf{b}_1, \ldots, \mathbf{b}_{n+1}$ constructed by the transformation of Lemma 2. The first $9|E|$ coordinates are either K or 0. The other coordinates are either 0 or 1. To obtain the vectors $\mathbf{b}'_i, i = 1, \ldots, n+1$, and the lattice $\mathsf{L}' = \mathsf{L}(\mathbf{b}'_1, \ldots, \mathbf{b}'_n)$ in each $\mathbf{b}_i$ we replace the first $9|E|$ coordinates by a set of K coordinates each. If a vector had a K in one of these coordinates, it has a 1 in each of the new K coordinates corresponding to the original coordinate. Otherwise the new coordinates are set to 0.

The first two properties in the lemma are easily verified. We still have to show the last property. In the case $opt_{\mathrm{MinLC}}(I) = |V_1|$ by Lemma 2 we know that for the original lattice L and the original vector $\mathbf{b}_{n+1}$ the distance $\mu(\mathbf{b}_{n+1}, \mathsf{L})$ is attained by a vector $\mathbf{v}$ whose first $9|E|$ coordinates are 0. Applying to this vector the construction used to obtain the vectors $\mathbf{b}'_i$, proves the corollary for this case.

In the case $opt_{\mathrm{MinLC}}(I) > g|V_1|$, observe that in the original lattice L any lattice vector has a multiple of $K > g \cdot |V_1|$ in its first $9|E|$ coordinates. Similarly, the first $9|E|$ coordinates of $\mathbf{b}_{n+1}$ are $K > g \cdot |V_1|$. By Lemma 2 for every $\mathbf{v} \in \mathsf{L}$ and every $\beta \in \mathbb{Z} \setminus \{0\}$ the difference $\beta \mathbf{b}_{n+1} - \mathbf{v}$ either has at least one non-zero coordinate among its first $9|E|$ coordinates or more than $g|V_1|$ of the last coordinates are 0 or 1. We conclude that for every vector $\mathbf{v}' \in \mathsf{L}'$ and all integers $\beta \neq 0$ the difference vector $\beta \cdot \mathbf{b}'_{n+1} - \mathbf{v}'$ has more than $g|V_1|$ non-zero coordinates and in particular $\mu(\beta \cdot \mathbf{b}'_{n+1}, \mathsf{L}') > \sqrt{g} \cdot \sqrt{|V_1|}$. □

4.2 Non-approximability to within some Constant Factor for Ivp and Gvp

Based on the previous lemma we can show the following lemma, which is the key to all our non-approximability results for Ivp and Gvp.

Lemma 3. *There is a constant $c > 1$, a polynomial-time computable function $s(\cdot)$, and a polynomial-time transformation from* Min Label Cover *to* Ivp *that for all instances $I = (V_1, V_2, E, \mathcal{A})$ of* Min Label Cover *generates a lattice $\mathsf{L} = \mathsf{L}(\mathbf{b}_1, \ldots, \mathbf{b}_{n+1})$ with the following properties:*

1. $\mathsf{L} \subset \mathbb{Z}^m, m = 9K|E| + 8|V_1| + 26K, K := 9|V_1|$ *and* $n = 8|V_1| + 8|V_2|$.
2. $\mathbf{b}_i \in \{0,1\}^m, i = 1, \dots, n+1$, *and* $\mathbf{b}_i$ *has* $\leq s(|V_1|)^2$ *non-zero entries,* $i = 1, \dots, n$.
3. $opt_{\textsc{MinLC}}(I) = 1 \cdot |V_1| \Longrightarrow \lambda_{\mathsf{rank}(\mathsf{L})} \leq 1 \cdot s(|V_1|)$
   $opt_{\textsc{MinLC}}(I) > g \cdot |V_1| \Longrightarrow \lambda_{\mathsf{rank}(\mathsf{L})} > c \cdot s(|V_1|)$.
4. *Let* M *be the sublattice generated by* $[\mathbf{b}_1, \dots, \mathbf{b}_n]$. *Then*

   $$opt_{\textsc{MinLC}}(I) = 1 \cdot |V_1| \Longrightarrow \mu(\mathbf{b}_{n+1}, \mathsf{M}) \leq 1 \cdot s(|V_1|)$$
   $$opt_{\textsc{MinLC}}(I) > g \cdot |V_1| \Longrightarrow \forall \beta \in \mathbb{Z} \setminus \{0\} : \mu(\beta \cdot \mathbf{b}_{n+1}, \mathsf{M}) > c \cdot s(|V_1|).$$

   Moreover, in the first case, there is a vector $\mathbf{v} \in \mathsf{M}$ *such that* $\mathbf{b}_{n+1} - \mathbf{v}$ *has at most* $s(|V_1|)^2$ *non-zero coordinates.*
   In the second case, for all $\mathbf{v} \in \mathsf{M}$ *and all* $\beta \in \mathbb{Z} \setminus \{0\}$, *the difference vector* $\beta \cdot \mathbf{b}_{n+1} - \mathbf{v}$ *has more than* $c^2 \cdot s(|V_1|)^2$ *non-zero coordinates.*

Proof. The function $s(|V_1|)$ will simply be $\sqrt{26K + |V_1|} = \sqrt{235|V_1|}$.

Let $\mathbf{b}'_i$ be the vectors from Corollary 2. For $i = 1, \dots, n$ let $\mathbf{b}_i$ be the vector obtained from $\mathbf{b}'_i$ by adding $26K$ coordinates to $\mathbf{b}_i$, each coordinate being zero. $\mathbf{b}_{n+1}$ is obtained from $\mathbf{b}'_{n+1}$ by adding $26K$ coordinates to $\mathbf{b}'_{n+1}$, each coordinate being 1. Let L be the lattice generated by the vectors $\mathbf{b}_1, \dots, \mathbf{b}_{n+1}$ and let M be the sublattice generated by the vectors $\mathbf{b}_1, \dots, \mathbf{b}_n$. *1* and *2* are immediate from the construction.

To prove *3* and *4* note that in any vector $\beta \cdot \mathbf{b}_{n+1} - \mathbf{v}$ with $\mathbf{v} \in \mathsf{M}$ and $\beta \in \mathbb{Z} \setminus \{0\}$, the last $26K$ coordinates are β. Since $||\mathbf{b}_i||^2 \leq 25K, i = 1, \dots, n$,

$$\mu^2(\mathbf{b}_{n+1}, \mathsf{M}) = \min_{\substack{\mathbf{v} \in \mathsf{M} \\ \beta \in \mathbb{Z} \setminus \{0\}}} ||\beta \cdot \mathbf{b}_{n+1} - \mathbf{v}||^2 \geq 26 \cdot K > ||\mathbf{b}_i||^2, i = 1, \dots, n.$$

Since

$$\mathsf{rank}(\mathsf{L}) = \mathsf{rank}(\mathsf{M}) + 1,$$

any set of $\mathsf{rank}(\mathsf{L})$ linearly independent vectors of L contains at least one vector $\mathbf{v}$ that depends on $\mathbf{b}_{n+1}$. That is, in the representation of $\mathbf{v}$ as a linear combination of the vectors $\mathbf{b}_i$, the coefficient in front of $\mathbf{b}_{n+1}$ is a non-zero integer. Hence we are able to conclude

$$\lambda^2_{\mathsf{rank}(\mathsf{L})} = \min_{\beta \in \mathbb{Z} \setminus \{0\}} \mu^2(\beta \cdot \mathbf{b}_{n+1}, \mathsf{M}).$$

Therefore

$$\lambda^2_{\mathsf{rank}(\mathsf{L})} = \min_{\beta \in \mathbb{Z} \setminus \{0\}} \mu^2(\beta \cdot \mathbf{b}_{n+1}, \mathsf{M}) = \min_{\beta \in \mathbb{Z} \setminus \{0\}} \mu^2(\beta \cdot \mathbf{b}'_{n+1}, \mathsf{L}(\mathbf{b}'_1, \dots, \mathbf{b}'_n)) + \beta^2 \cdot 26K,$$

where $\mathbf{b}'_1, \dots, \mathbf{b}'_{n+1}$ are as in Corollary 2. Thus, by the same corollary

$$\begin{aligned} & opt_{\textsc{MinLC}}(I) = 1 \cdot |V_1| \\ \Longrightarrow\ & \lambda_{\mathsf{rank}(\mathsf{L})} \leq \mu(\mathbf{b}_{n+1}, \mathsf{M}) \leq \sqrt{|V_1| + 26K} \\ & = s(|V_1|) \end{aligned}$$

and

$$\begin{aligned} & opt_{\text{MinLC}}(I) > g \cdot |V_1| \\ \Longrightarrow\ & \lambda_{\text{rank}(\mathsf{L})} = \min_{\beta \in \mathbb{Z}\setminus\{0\}} \mu(\beta \cdot \mathbf{b}_{n+1}, \mathsf{M}) > \sqrt{g \cdot |V_1| + 26K} \\ & \qquad\qquad\qquad\qquad\qquad\qquad\qquad = c \cdot s(|V_1|), \end{aligned}$$

for $c = \sqrt{1 + \frac{g-1}{235}}$. This proves the lemma, except for the last claims in *4*. One easily goes through the proof to check that even these stronger claims are true. □

From Lemma 3 we can derive the first non-approximability results for IVP and GVP.

Theorem 2. *There is a constant $c > 1$ such that* GAPIVP$_c$ *and* GAPGVP$_c$ *are* NP*-hard.*

Proof. Let c be the constant in Lemma 3. This lemma together with Lemma 1 proves the theorem for GAPIVP$_c$.

For GAPGVP$_c$ we also want to apply Lemma 1. First note that $\nu(\mathsf{L}) \geq \lambda_{\text{rank}(\mathsf{L})}$. Hence, in the case $opt_{\text{MinLC}}(I) > g \cdot |V_1|$ the reduction in Lemma 3 shows

$$\nu(\mathsf{L}) > c \cdot s(|V_1|).$$

For the case $opt_{\text{MinLC}}(I) = |V_1|$, Lemma 3 shows that $\mu(\mathbf{b}_{n+1}, \mathsf{M}) \leq s(|V_1|)$. Let $\mathbf{v} \in \mathsf{M} = \mathsf{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ be a vector with $\|\mathbf{b}_{n+1} - \mathbf{v}\| \leq s(|V_1|)$. The vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n, \mathbf{b}_{n+1} - \mathbf{v}$ are a basis for L. Since $\|\mathbf{b}_i\| \leq \mu(\mathbf{b}_{n+1}, \mathsf{M})$ (see the proof of Lemma 3), we conclude that in this case

$$\nu(\mathsf{L}) \leq s(|V_1|).$$

The theorem follows. □

4.3 Hardness of Approximating IVP and GVP within Large Factors

To improve the hardness results of the previous section we will use again a technique from [ABSS]. The technique is based on an iterative construction that will gradually increase the constant c in Lemma 3. We will now describe the first step of the iteration.

Given an instance I of MIN LABEL COVER, let $\mathbf{b}_1, \ldots, \mathbf{b}_{n+1}$ be the vectors from Lemma 3. In these vectors replace each entry α by a block of m coordinates equal to the vector $\alpha \cdot \mathbf{b}_{n+1}$. Call these new vectors $\mathbf{w}_i, i = 1, \ldots, n+1$. Let B be the $(m \times n)$-matrix whose columns are the vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$ and let $\overline{B}$ be the $(m^2 \times nm)$-matrix

$$\overline{B} = \begin{pmatrix} \boxed{B_1} & \cdots & \boxed{0} & \boxed{0} \\ \boxed{0} & \boxed{B_2} & \cdots & \boxed{0} \\ \vdots & \vdots & \ddots & \vdots \\ \boxed{0} & \boxed{0} & \cdots & \boxed{B_m} \end{pmatrix}$$

where each B_i is a copy of B. By Lemma 3 the length of the column vectors in $\overline{B}$ is at most $s(|V_1|)$. Let L be the lattice generated by the columns of $\overline{B}$ and the vectors $\mathbf{w}_i, i = 1, \ldots, n+1$. Similarly, M is the sublattice generated by the same vectors except for $\mathbf{w}_{n+1}$.

Consider the case where the instance I of Min Label Cover satisfies $opt_{\text{MinLC}}(I) = |V_1|$. By Lemma 3 we can subtract a suitable integer linear combination of the vectors $\mathbf{w}_i, i \neq n+1$, from $\mathbf{w}_{n+1}$ to obtain a new vector $\mathbf{w}_{n+1}$, which has only $s(|V_1|)^2$ non-zero blocks consisting of copies of $\mathbf{b}_{n+1}$. By Lemma 3 the vectors $\mathbf{w}_i, i = 1, \ldots, n$, also have at most $s(|V_1|)^2$ non-zero blocks consisting of copies of $\mathbf{b}_{n+1}$.

For all $\mathbf{w}_i$ by subtracting suitable linear combinations of the columns of $\overline{B}$ we can eliminate all but $s(|V_1|)^2$ non-zero entries in the blocks consisting of a copy of $\mathbf{b}_{n+1}$. Hence we can replace the vectors $\mathbf{w}_i, i = 1, \ldots, n+1$, by vectors $\mathbf{v}_i$ such that

$$||\mathbf{v}_i|| \leq s(|V_1|)^2.$$

We also conclude

$$\mu(\mathbf{w}_{n+1}, \mathsf{M}) \leq s(|V_1|)^2.$$

The vectors $\mathbf{v}_i, i = 1, \ldots, n+1$, together with the columns of $\overline{B}$ are still a basis for the lattice L. To prove this observe that replacing $\mathbf{w}_{n+1}$ by $\mathbf{w}_{n+1} - \mathbf{v}, \mathbf{v} \in \mathsf{M}$, still gives a basis. Next observe that the columns of $\overline{B}$ have not been changed. But then replacing $\mathbf{w}_i$ by $\mathbf{v}_i$ still gives a basis. We conclude that in the case a cover with cost $|V_1|$ exists,

$$\lambda_{\text{rank}(\mathsf{L})}, \nu(\mathsf{L}) \leq s(|V_1|)^2.$$

Next we consider the case where the instance I of Min Label Cover satisfies $opt_{\text{MinLC}}(I) > g|V_1|$. Note that the vector $\mathbf{w}_{n+1}$ is the only vector in the basis for L whose last coordinate is non-zero. Hence any linearly independent set with

$\mathsf{rank}(\mathsf{L})$ many elements, and in particular, any basis of L, must contain a vector of the form $\beta\mathbf{w}_{n+1} - \mathbf{v}$ with $\beta \in \mathbb{Z} \setminus \{0\}$ and $\mathbf{v} \in \mathsf{M}$. Assume that a non-zero integer β and a vector $\mathbf{v} \in \mathsf{M}$ exist such that

$$||\beta \cdot \mathbf{w}_{n+1} - \mathbf{v}|| \leq c^2 \cdot s(|V_1|)^2.$$

This implies that the number of non-zero coordinates in $\beta \cdot \mathbf{w}_{n+1} - \mathbf{v}$ is bounded by $c^4 \cdot s(|V_1|)^4$. Then either there is a non-zero block in $\beta \cdot \mathbf{w}_{n+1}$ consisting of a copy a $\mathbf{b}_{n+1}$, in which, by subtracting a suitable combination of columns of $\overline{B}$, the number of non-zero coordinates can be reduced below $c^2 \cdot s(|V_1|)^2$. Or by subtracting a suitable combination of the vectors $\mathbf{w}_i, i = 1, \ldots, n$, the number of non-zero blocks in $\mathbf{w}_{n+1}$ can be reduced below $c^2 \cdot s(|V_1|)^2$. Both cases contradict Lemma 3. So we may conclude, that in this case for every $\beta \in \mathbb{Z} \setminus \{0\}$,

$$\mu(\beta \cdot \mathbf{w}_{n+1}, \mathsf{M}) > c^2 \cdot s(|V_1|)^2.$$

and

$$\lambda_{\mathsf{rank}(\mathsf{L})}, \nu(\mathsf{L}) > c^2 \cdot s(|V_1|)^2.$$

Hence we have increased the gap c in Lemma 3 to c^2 at the expense of increasing the dimension of the Euclidean space underlying the lattice from m to m^2 and at the expense of increasing the size of the generating set of vectors of the lattice from $n+1$ to $n(m+1)+1$. Applying the same construction once more, this time using $\mathbf{w}_{n+1}$ to replace coordinates in the vectors $\mathbf{w}_i, i = 1, \ldots, n+1$, and in the vectors corresponding to the columns of $\overline{B}$ the gap c increases to c^4. Iterating the construction further we obtain

Lemma 4. *Let n, m, c and the function s be as in Lemma 3. Let ℓ be an arbitrary integer. There is a transformation that for all instances $I = (V_1, V_2, E, \mathcal{A})$ of* Min Label Cover *generates a lattice $\mathsf{L} = \mathsf{L}(\mathbf{b}_1, \ldots, \mathbf{b}_{N+1})$ with the following properties:*

1. $\mathsf{L} \subset \mathbb{Z}^M, M = m^{2^\ell}, N = n\prod_{i=0}^{\ell}(m^{2^i}+1)$
2. $\mathrm{opt}_{\mathrm{MinLC}}(I) = 1 \cdot |V_1| \Longrightarrow \lambda_{\mathsf{rank}(\mathsf{L})}, \nu(\mathsf{L}) \leq s(|V_1|)^{2^\ell}$
   $\mathrm{opt}_{\mathrm{MinLC}}(I) > g \cdot |V_1| \Longrightarrow \lambda_{\mathsf{rank}(\mathsf{L})}, \nu(\mathsf{L}) > c^{2^\ell} \cdot s(|V_1|)^{2^\ell}$.

The running time of the transformation is polynomial in $|I|^{2^\ell}$, where $|I|$ is the description size of I.

From this we obtain our final non-approximability results.

Theorem 3. *1. For every fixed constant $C > 1$ the problems* GAPIVP$_C$ *and* GAPGVP$_C$ *are* NP*-hard.*

2. For every $\epsilon > 0$, there is no approximation algorithm approximating $\lambda_{\mathsf{rank}(\mathsf{L})}$ or $\nu(\mathsf{L})$ within a factor of $2^{\log^{1-\epsilon}(\mathsf{rank}(\mathsf{L}))}$ unless $\mathsf{NP} \subseteq \mathsf{DTIME}(n^{\mathrm{polylog}(n)})$.

Proof. To prove the first statement we use Lemma 1 and Lemma 4 with

$$\ell = \log \log_c(C).$$

Since c and C are constant, so is $\log \log_c(C)$. Hence the overall reduction from 3-SAT to GAPIVP$_C$ and GAPGVP$_C$ is polynomial time.

To prove the second statement we can use the same reasoning as in [ABSS]. Let φ be an instance of 3-SAT. By $|\varphi|$ denote the size of this instance. Applying the transformation in Lemma 1 we obtain an instance I of MIN LABEL COVER with size $|I| = |\varphi|^{O(1)}$. Applying the transformation in Lemma 4 with $\ell = \ell(|\varphi|)$ such that $2^{\ell(|\varphi|)} = \log^{\beta}(|\varphi|)$ for some β, we obtain a lattice L with rank

$$\mathrm{rank}(\mathsf{L}) = R = 2^{O(\log^{\beta+1}(|\varphi|))}.$$

The running time of the transformation is polynomial in $2^{O(\log^{\beta+1}(|\varphi|))}$. We also have

$$\varphi \text{ satisfiable} \Longrightarrow \lambda_{\mathrm{rank}(\mathsf{L})}, \nu(\mathsf{L}) \leq s(|V_1|)^{\log^{\beta}(|\varphi|)}$$
$$\varphi \text{ not satisfiable} \Longrightarrow \lambda_{\mathrm{rank}(\mathsf{L})}, \nu(\mathsf{L}) > c^{\log^{\beta}(|\varphi|)} \cdot s(|V_1|)^{\log^{\beta}(|\varphi|)}.$$

The gap between satisfiable and non-satisfiable instances φ of 3-SAT is

$$c^{\log^{\beta}(|\varphi|)}.$$

However, we have to measure this in terms of the rank R of the lattice L. With respect to R the gap is

$$c^{\log^{\beta}(|\varphi|)} = 2^{\Omega(\log^{\beta/(\beta+1)}(R))},$$

since $\log(R) = O(\log^{\beta+1}(|\varphi|))$.

Now let $\epsilon > 0$. Choose β such that

$$\beta/(\beta+1) > 1 - \epsilon.$$

Then we can apply an approximation algorithm for $\lambda_{\mathrm{rank}(\mathsf{L})}$ or $\nu(\mathsf{L})$ with approximation factor $2^{\log^{1-\epsilon}(\mathrm{rank}(\mathsf{L}))}$ to distinguish between satisfiable and non-satisfiable instances φ of 3-SAT. The theorem follows since we apply the algorithm to a lattice L whose overall description size is bounded by $2^{O(\log^{\beta+1}(|\varphi|))}$. □

5 Limits of Non-Approximability for IVP and GVP

Extending results in [LLS] and [GG] we show that GAPIVP$_{n^{3/2}}$ and GAPGVP$_{n^{3/2}}$ are in $\mathsf{NP} \cap \text{co-}\mathsf{NP}$ and that GAPIVP$_{n/O(\sqrt{\log(n)})}$ and GAPGVP$_{n/O(\sqrt{\log(n)})}$ are in $\mathsf{NP} \cap \text{co-}\mathsf{AM}$. The first result implies that under Karp-reductions GAPIVP$_{n^{3/2}}$ and GAPGVP$_{n^{3/2}}$ are not NP-hard unless NP = co-NP. Again under Karp-reductions, the second result implies that GAPIVP$_{n/\sqrt{\log(n)}}$ and GAPGVP$_{n/\sqrt{\log(n)}}$ are not

NP-hard unless the polynomial hierarchy collapses to its second level. For a thorough discussion of the complexity-theoretic implications of these results we refer to [GG].

To prove the results on the limits of non-approximability we need a few definitions from the geometry of numbers. Given a lattice L in $\mathbb{R}^m$ with basis $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$, by $\mathsf{L}^{(n-i+1)}$ we denote the orthogonal projection of L onto the orthogonal complement $(\mathbb{R}\mathbf{b}_1 + \ldots + \mathbb{R}\mathbf{b}_{i-1})^\perp$ of $\mathbb{R}\mathbf{b}_1 + \ldots + \mathbb{R}\mathbf{b}_{i-1}$. By $\mathbf{b}_i^\dagger$ we denote the projection of $\mathbf{b}_i$ onto $\mathsf{L}^{(n-i+1)}$. Then $[\mathbf{b}_1^\dagger, \ldots, \mathbf{b}_n^\dagger]$ is called the *Gram-Schmidt orthogonalization* of $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$. Note that $\mathsf{L}^{(n-i+1)}$ is a $n - i + 1$-dimensional lattice with basis $[\mathbf{b}_i^\dagger, \ldots, \mathbf{b}_n^\dagger]$.

By definition of the Gram-Schmidt orthogonalization

$$\mathbf{b}_i = \mathbf{b}_i^\dagger + \sum_{j=1}^{i-1} \mu_{ij} \mathbf{b}_j^\dagger.$$

A basis $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ is called *weakly reduced* iff $|\mu_{ij}| \leq 1/2$ for $1 \leq j < i \leq n$. By replacing $\mathbf{b}_i$ by $\mathbf{b}_i - m_{ij}\mathbf{b}_j, 1 \leq j < i \leq n$ for suitable integers m_{ij} every basis can be transformed into a weakly reduced basis [L].

Definition 10. A basis $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ of a lattice L is called a *HKZ-basis* (Hermite, Korkin, Zolotarev) iff

(i) $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ is weakly reduced.
(ii) $\mathbf{b}_i^\dagger$ is a shortest non-zero vector in $\mathsf{L}^{(n-i+1)}, i = 1, \ldots, n$.

For a function $g : \mathbb{N} \to \mathbb{R}_+$, a basis $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ is called a *g-approximate HKZ-basis* of L iff

(i) $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ is weakly reduced.
(ii) $\mathbf{b}_i^\dagger$ is within a factor of $g(n-i+1)$ a shortest non-zero vector in $\mathsf{L}^{(n-i+1)}, i = 1, \ldots, n$.

Every lattice has a HKZ-basis of polynomial size.

We also need the dual of a lattice and of a basis. Let L be a lattice in $\mathbb{R}^m$ with basis $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$. The *dual lattice* L^* is the set of all vectors $\mathbf{v}^* \in \mathbb{R}\mathbf{b}_1 + \ldots + \mathbb{R}\mathbf{b}_n$ that satisfy $\langle \mathbf{v}^*, \mathbf{v} \rangle \in \mathbb{Z}$ for all $\mathbf{v} \in \mathsf{L}$. The set L^* is also a lattice. If $\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*$ are defined by

$$\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle = \begin{cases} 1 \text{ if } i + j = n + 1 \\ 0 \text{ otherwise} \end{cases}$$

then $[\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*]$ is a basis of L^*. It is called the *basis dual to* $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$. A basis $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ of L is called a *dual HKZ-basis* iff the basis $[\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*]$ is a HKZ-basis of L^*.

Given a basis $B = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$ of a lattice L then we set

$$\lambda(B) = \min\{||\mathbf{b}_1^\dagger||, \ldots, ||\mathbf{b}_n^\dagger||\}.$$

It is well-known [L] that $\lambda_1(\mathsf{L}) \geq \lambda(B)$ for any basis B of a lattice L. On the other hand, in [LLS] it is shown that for a dual HKZ-basis B of a lattice L we have

$\lambda_1(\mathsf{L}) \leq n\lambda(B)$. Since the Gram-Schmidt orthogonalization of a basis $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ can be computed in polynomial time, guessing a vector $\mathbf{b} \in \mathsf{L}$ and a dual HKZ-basis of L, we can check in polynomial time whether $||\mathbf{b}|| \leq n\lambda_1(\mathsf{L})$. Hence, we have a non-deterministic algorithm for GAPSVP$_n$. Since GAPSVP$_n \in$ NP, we obtain that the problem GAPSVP$_n$ is in NP $\cap$ co-NP. This result and the proof are from [LLS].

To obtain a similar result for IVP and GVP we need one crucial fact about HKZ-bases. It is an easy extension of a result in [LLS] and, using different notation, it was proved in [L].

Theorem 4. *Let* $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ *be a g-approximate HKZ-basis of the lattice* L. *Then*

$$||b_i|| \leq g(n-i+1)\sqrt{i}\lambda_i(\mathsf{L}).$$

From this we obtain

Theorem 5. GAPIVP$_{n^{3/2}}$ *and* GAPGVP$_{n^{3/2}}$ *are in* NP $\cap$ co-NP.

Proof. Both problems are in NP. To show that GAPIVP$_{n^{3/2}}$ is in co-NP we need to describe a non-deterministic polynomial time algorithm that computes linear independent vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathsf{L}$ and a proof that $||\mathbf{v}_i|| \leq n^{3/2}\lambda_n(\mathsf{L})$. The algorithm first guesses a HKZ-basis $B = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$ of L. Furthermore the algorithm guesses dual HKZ-bases $B_j, j = 1, \ldots, n$, for the lattices $\mathsf{L}^{(j)}$. Then the algorithm checks whether the sets B, B_j are bases of the respective lattices. Finally, the algorithm determines whether

$$||\mathbf{b}_j^\dagger|| \leq n\lambda(\mathsf{L}^{(j)}), j = n, \ldots, 1.$$

If $\mathbf{b}_j$ passes this test, by what has been said above, we know that

$$||\mathbf{b}_j^\dagger|| \leq n\lambda_1(\mathsf{L}^{(j)}).$$

Hence, if all $\mathbf{b}_j$ pass the test, B is a n-approximate HKZ-basis of L. Using Theorem 4 we conclude that $||\mathbf{b}_i|| \leq n^{3/2}\lambda_n(\mathsf{L})$. This proves the theorem for GAPIVP$_{n^{3/2}}$.

Since $\nu(\mathsf{L}) \geq \lambda_n(\mathsf{L})$ and the vectors $\mathbf{b}_i$ we computed in the non-deterministic algorithm for IVP form a basis for L, the theorem follows for GAPGVP$_{n^{3/2}}$ as well. □

Next we want to prove

Theorem 6. GAPIVP$_{n/O(\sqrt{\log(n)})}$ *and* GAPGVP$_{n/O(\sqrt{\log(n)})}$ *are in* NP$\cap$co-AM.

Proof. We will use the protocol of Goldreich and Goldwasser which shows that the problem GAPSVP$_{\sqrt{n/O(\log(n))}}$ is in co-AM [GG]. More precisely, for every constant $c > 0$, [GG] describes a protocol with the following properties. The input is an instance (L, d) of SVP. If a shortest vector in L has length $> \sqrt{n/c\log(n)}d$, then the verifier accepts with probability 1. On the other hand, if a shortest vector in L has length $\leq d$, then the verifier accepts with probability at most $1 - n^{-2c}$.

Based on this protocol, for every $c > 0$ we describe an AM-protocol for co-$\text{GAPIVP}_{n/\sqrt{c\log(n)}}$. Hence the input for the protocol is an instance (L, d) of the problem $\text{GAPIVP}_{n/\sqrt{c\log(n)}}$. If (L, d) is a NO-instance, then the verifier accepts with probability 1. If (L, d) is a YES-instance, then the verifier accepts with probability at most $1 - n^{-2c}$. This protocol will prove the theorem.

The protocol is as follows. First, the prover sends vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$ to the verifier. The verifier checks that this is a weakly reduced basis of L and that $\max\{||\mathbf{b}_j||\} > n/\sqrt{c\log(n)}d$. Then the verifier computes the lattices $\mathsf{L}^{(j)}, j = n, \ldots, 1$. For $j = 1, \ldots, n$ in parallel, the AM-protocol in [GG] for the problem co-$\text{GAPSVP}_{\sqrt{n/O(\log(n))}}$ is used with input $(\mathsf{L}^{(j)}, ||\mathbf{b}_j^{\dagger}||\sqrt{c\log(n)/n})$. He accepts iff all these protocols lead to acceptance. Note that this is an MAM-protocol, but any MAM-protocol can be transformed in an AM-protocol [B].

Suppose first that (L, d) is a NO-instance of $\text{GAPIVP}_{n/\sqrt{c\log(n)}}$. Then by sending a HKZ-basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ of L the prover can ensure that $\mathbf{b}_j^{\dagger}$ is a shortest vector in $\mathsf{L}^{(j)}$. Hence for $j = 1, \ldots, n$ the verifier in the [GG]-protocol will accept $(\mathsf{L}^{(j)}, ||\mathbf{b}_j^{\dagger}||\sqrt{c\log(n)/n})$ with probability 1. Therefore, the verifier in the protocol for co-$\text{GAPIVP}_{n/\sqrt{c\log(n)}}$ will accept the instance (L, d) with probability 1.

Now assume that (L, d) is a YES-instance of $\text{GAPIVP}_{n/\sqrt{c\log(n)}}$. Assume that the vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$ are a weakly-reduced basis and satisfy $\max\{||\mathbf{b}_j||\} > n/\sqrt{c\log(n)}d$. Since (L, d) is a YES-instance, we see that $\lambda_n(\mathsf{L}) \leq d$. Then by Theorem 4 $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ can not be a $\sqrt{n/c\log(n)}$-approximate HKZ-basis of L. Hence there is at least one $j \in \{1, \ldots, n\}$ such that the length of a shortest vector in $\mathsf{L}^{(j)}$ is at most $||\mathbf{b}_j^{\dagger}||\sqrt{c\log(n)/n}$. By the analysis in [GG], running the co-AM-protocol for $\text{GAPSVP}_{\sqrt{n/c\log(n)}}$ for this j the verifier will accept $(\mathsf{L}^{(j)}, ||\mathbf{b}_j^{\dagger}||\sqrt{c\log(n)/n})$ with probability at most $1 - n^{-2c}$. Hence the verifier will accept the input (L, d) with probability at most $1 - n^{-2c}$.

Since $\lambda_n(\mathsf{L}) \leq \nu(\mathsf{L})$ and since in the AM-protocol for co-$\text{GAPIVP}_{n/\sqrt{c\log(n)}}$ described above the verifier checks that the vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$ sent by the prover form a basis, we see that the same protocol is also an AM-protocol for co-$\text{GAPGVP}_{n/\sqrt{c\log(n)}}$. □

6 Conclusions and Open Problems

The main open problem this paper raises is: What is the complexity of computing short linearly independent vectors and bases in a lattice? Is there some constant $c > 0$ such that GAPIVP_{n^c} and GAPGVP_{n^c} are NP-hard? It is widely believed that any problem that is hard to approximate within a factor of $2^{\log^{1-\epsilon}(n)}$ actually is hard to approximate within some polynomial factor (see [AL]). Currently, a proof for this general statement seems to be out of reach. However, some progress in this direction has been achieved recently for the closest vector problem [DKS].

Since our results rely on methods originally used for hardness results for the closest vector problem, it is natural to ask whether the hardness results of [DKS] for the closest vector problem hold for IVP and GVP as well.

Our hardness results for IVP and GVP (almost) match the known hardness results for CVP. However, we were not able to generalize the known results on the limits of non-approximability of CVP to IVP and GVP. Instead our bounds are worse by a factor of $\sqrt{n}$. That opens up the possibility that IVP and GVP are strictly harder than CVP or SVP. The current picture is somewhat mixed. On the one hand, we have reductions that reduce the exact versions of SVP and CVP to exact versions of IVP and GVP. No such reductions are known for the opposite direction. However, for the corresponding approximate versions the situation is different. We have reductions of approximate versions of IVP and GVP to approximate versions of SVP and CVP with a loss of $\sqrt{n}$ in the approximation factor [LLS]. These reductions actually compute a relatively short basis, for example. For reductions of an approximate version of SVP to approximate versions of IVP and GVP the corresponding loss in the approximation factor is n. This is based on so-called transference theorems [Ba,Ca1]. Moreover, in this case, we only get a numerical estimate for the length of a shortest vector, we do not get a relatively short vector. In general, no such reduction is known for an approximate version of CVP. It would be nice to have a clearer picture of the relationship between the various lattice problems.

References

[A1] M. Ajtai, "Generating Hard Instances of Lattice Problems", *Proc. 28th Symposium on Theory of Computing* 1996, pp. 99-108.

[A2] M. Ajtai, "The Shortest Vector Problem is NP-Hard for Randomized Reductions", *Proc. 30th Symposium on Theory of Computing* 1998, pp. 10-19.

[A3] M. Ajtai, "Worst-Case Complexity, Average-Case Complexity and Lattice Problems", *Proc. International Congress of Mathematicians* 1998, Vol. III, pp. 421-428.

[AL] S. Arora, C. Lund, "Hardness of Approximations", in D. S. Hochbaum (ed.), *Approximation Algorithms for* NP*-Hard Problems*, PWS Publishing, 1997.

[ABSS] S. Arora, L. Babai, J. Stern, Z. Sweedyk, "The Hardness of Approximate Optima in Lattices, Codes, and Systems of Linear Equations", *Journal of Computer and System Sciences* Vol. 54, pp. 317-331, 1997.

[AD] M. Ajtai, C. Dwork "A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence", *Proc. 29th Symposium on Theory of Computing* 1997, pp. 284-293.

[B] L. Babai, "Trading Group Theory for Randomness", *Proc. 17th Symposium on Theory of Computing* 1985, pp. 421-430.

[Ba] W. Banaszcyk, "New Bounds in Some Transference Theorems in the Geometry of Numbers", *Mathematische Annalen* Vol. 296, pp. 625-635, 1993.

[BK] A. Bachem, R. Kannan, "Lattices and the Basis Reduction Algorithm", Technical Report, Carnegie Mellon University, 1984.

[C] J. W. S. Cassels, *An Introduction to the Geometry of Numbers*, Springer-Verlag, 1971.

[Ca1] J. Y. Cai, "A New Transference Theorem and Applications to Ajtai's Connection Factor", available as Report No. 5, *Electronic Colloquium on Computational Complexity*, 1998.

[Ca2] J. Y. Cai, "A relation of primal–dual lattices and the complexity of shortest lattice vector problem", *Theoretical Computer Science* Vol. 207, pp. 105-116, 1998.

[CN] J. Y. Cai, A. P. Nerurkar, "An Improved Worst-Case to Average-Case Reduction for Lattice Problems", *Proc. 38th Symposium on Foundations of Computer Science* 1997, pp. 468-477.

[DKS] I. Dinur, G. Kindler, S. Safra, "Approximating-CVP to Within Almost-Polynomial Factors is NP-Hard", to appear in *Proc. 39th Symposium on Foundations of Computer Science* 1998.

[GG] O. Goldreich, S. Goldwasser, "On the Limits of Non-Approximability of Lattice Problems", *Proc. 30th Symposium on Theory of Computing* 1998, pp. 1-9.

[L] L. Lovasz, *An Algorithmic Theory of Graphs, Numbers and Convexity*, SIAM, 1986.

[LLS] J. Lagarias, H. W. Lenstra, C.P. Schnorr, "Korkin-Zolotarev Bases and Successive Minima of a Lattice and its Reciprocal Lattice", *Combinatorica* Vol. 10, No. 4, pp. 333-348, 1990.

[M] D. Micciancio, "The Shortest Vector in a Lattice is Hard to Approximate to within Some Constant", to appear in *Proc. 39th Symposium on Foundations of Computer Science* 1998.

[MH] J. Milnor, D. Husemoller, *Symmetric Bilinear Forms*, Springer-Verlag, 1973.

Johannes Blömer

(are random instances hard?)

$b_1, \dots, b_n$ linearly independant $\in \mathbb{R}^n$

$L(b_1, \dots, b_n) = \mathbb{Z} b_1 + \dots + \mathbb{Z} b_n$ = lattice generated by these vectors.

$\lambda_i(L) = \min_{r \in \mathbb{R}} \{ r \cdot S^n :$ contains i linearly ind. vectors in $L \}$

$\lambda_1(L)$ = length of shortest non-zero vector in L.

$\nu(L) = \min_{r \in \mathbb{R}^+} \{ r S_n$ contain a basis of $L \}$

Note: $\nu(L) \geq \lambda_n(L)$

take $L = \{ v \in \mathbb{Z}^n \mid v_i = v_j \mod 2 \}$

e_i = standard unit vector.

$2 \cdot e_i \in L \Rightarrow \lambda_n = 2$

$\nu / \lambda_n \approx \frac{\sqrt{n}}{2}$

Atjai = constructed Λ_n ← class of lattice, probabilistic alg. that generates a "true" random element.

$L \in \Lambda_n$ $\lambda_1(L) \leq n$

Thm: If there is a probabilistic polynomial time alg that for a random $L \in \Lambda_n$ finds a vector $v \in L$ with $|v| \leq n$ then $\exists$ a probabilistic prob P-time Algorithm that for ALL $L \subseteq \mathbb{R}^n$

1) Approximates λ_n with factor $\leq n^{c_0}$, $c_0 > 3$

2) Approximatas ν " " $\leq n^{c_1}$, $c_1 > 3.5$

3) Appuoximatas λ_n " " $\leq n^{c_2}$, $c_2 > 4$

Best approximation $(1+\varepsilon)^n$, $\varepsilon > 0$.

GOAL to actually prove it is NP-hard to approximate.

Results: Decision problem: is $\lambda_1 \leq B$ is NP-complete (under randomized reduction).

Approximating λ_1 with $\sqrt{2}$ is NPH.

Approximatting with $\sqrt{n/\log n}$ is not NPH. (

With Seifart:

* λ_n, ν for any constant c are NPH to approx with factor c.

* If NP $\subseteq$

(L, r) yes instance iff $\lambda_n(L) \leq r$
no otherwise.

(L, v, r) yes iff $\mu(v, L) \leq r$ ↙ (?)

distance from v to L

"FUNNY" no otherwise.

Fact: $\lambda_n(L) \le n^{\frac{n}{2}} \det(L)$

Take $\begin{bmatrix} b_1 & \cdots & b_n & v \\ 0 & & 0 & D \end{bmatrix}$

$D = \max\{r+1, \lceil n^{n/2} \det(L) \rceil + 1\}$

take $(L', \sqrt{r^2+D^2})$.

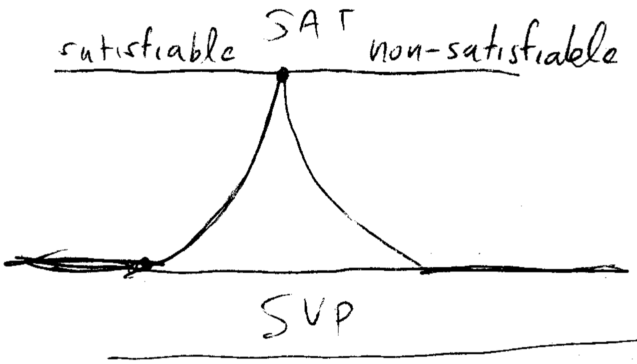
Same dependance works D.

They really use the reduction ~~to~~ Between SAT and the "FUNNY" problem to do the problem

Thm $\lambda_1(L) \leq B$ decision problem within $c\sqrt{n/\log n}$ is probably not NP-hard. ← By

SVP_g: (L, B) such that $\lambda_1(L) \leq B$ yes-instances

(L, B) such that $\lambda_1(L) > g \cdot B$ no instances



Primes ∈ NP (Pratt did it), Prime ∈ Co-NP
thus prime NP-hard ⇒ NP = Co-NP ...!!

→ Hence prime is probably NOT NP-Hard