Information Processing Letters 116 (2016) 631–637

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

Improved hardness results for unique shortest vector problem

Divesh Aggarwal [a,*], Chandan Dubey [b]

[a] *Department of Computer Science, EPFL, Switzerland*
[b] *Department of Computer Science, ETH Zurich, Switzerland*

ARTICLE INFO

Article history:
Received 18 August 2015
Received in revised form 6 May 2016
Accepted 18 May 2016
Available online 24 May 2016
Communicated by Ł. Kowalik

Keywords:
Computational complexity
Lattices
Unique SVP
NP hardness
Reductions

ABSTRACT

The unique shortest vector problem on a rational lattice is the problem of finding the shortest non-zero vector under the promise that it is unique (up to multiplication by -1). We give several incremental improvements on the known hardness of the unique shortest vector problem (uSVP) using standard techniques. This includes a deterministic reduction from the shortest vector problem to the uSVP, the NP-hardness of uSVP on $\left(1+\frac{1}{\mathrm{poly}(n)}\right)$-unique lattices, and a proof that the decision version of uSVP defined by Cai [4] is in co-NP for $n^{1/4}$-unique lattices.

1. Introduction

Despite its simple grid like structure, lattices have wide and varied applications in many areas of mathematics and after the discovery of the LLL algorithm [13] also in computer science. The scope of the application was furthered by the breakthrough result of Ajtai [2], who showed that lattice problems have a very desirable property for cryptography: a worst-case to average-case reduction. This property yields one-way functions and collision resistant hash functions, based on the *worst-case* hardness of lattice problems. This is in a stark contrast to the traditional number theoretic constructions which are based on the average-case hardness e.g., factoring, discrete logarithms.

A *lattice* L is the set of all integer combinations of n linearly independent vectors $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ in $\mathbb{R}^m$. These vectors are referred to as a *basis* of the lattice and n is called the *rank* of the lattice. The *successive minima* $\lambda_i(\mathrm{L})$ (where $i = 1, \ldots, n$) of the lattice L are among the most fundamental parameters associated to a lattice. The $\lambda_i(\mathrm{L})$ is defined as the smallest value such that a sphere of radius $\lambda_i(\mathrm{L})$ centered around the origin contains at least i linearly independent lattice vectors.

The shortest vector problem (SVP) is arguably the most important problem on rational lattices. Given a lattice L, the problem asks for a shortest non-zero vector in the lattice. A generalization of the decision version of the SVP leads to the GapSVP problem. The GapSVP_γ can be seen as a promise problem, which given a lattice L and an integer d, asks to distinguish between the case $\lambda_1(\mathrm{L}) \le d$ and $\lambda_1(\mathrm{L}) > \gamma d$.

A lattice L is called γ-unique if $\lambda_2(\mathrm{L}) > \gamma\lambda_1(\mathrm{L})$. In this work, we will be concerned with the unique shortest vector problem (uSVP for short). For a parameter γ, the uSVP_γ is defined as follows. Given a γ-unique lattice L; find the shortest non-zero vector in L. Notice that for uSVP, γ can be interpreted both as a uniqueness factor, and approximation factor. The two resulting problems are equivalent. This justifies the uSVP_γ notation. The security of the first lattice based public-key cryptosystem by Ajtai–Dwork [1] was based on the worst-case hardness of $\mathrm{uSVP}_{O(n^8)}$. A series of subsequent papers(in particular, [7, 16]) improved the uniqueness factor, i.e., obtained public-key cryptosystems based on the worst-case hardness of $\mathrm{uSVP}_{O(n^{1.5})}$.

* Corresponding author.
E-mail address: divesh.aggarwal@epfl.ch (D. Aggarwal).

http://dx.doi.org/10.1016/j.ipl.2016.05.003
0020-0190/© 2016 Published by Elsevier B.V.

There are still some gaps in our understanding of the hardness of uSVP. The uSVP problem was proved equivalent to the GapSVP problem upto an approximation factor of $\sqrt{n}$ [14]. Unfortunately, the reduction from GapSVP to uSVP in [14] does not imply NP-hardness of uSVP, because of the loss factor of $\sqrt{n}$ and the fact that GapSVP_γ is known to be NP-hard only for sub-polynomial factors [9]. Kumar–Sivakumar [12], via a randomized reduction from SVP, show that uSVP_γ is NP-hard for $\gamma = 1 + 2^{-O(n^2)}$. One of our main results is a derandomization of the result of [12] thereby giving a deterministic reduction from SVP to uSVP. We also give a randomized reduction which shows that uSVP is NP-hard for $\gamma = 1 + 1/\text{poly}(n)$ under randomized reductions. This result was recently improved to $\gamma = 1 + O(\log n/n)$ [17].

There are two versions of the decision uSVP in the literature: one given by Cai [4] (denoted, duSVP) and another by Regev [16] (denoted, duSVP′). Unlike the duSVP′ defined by Regev, a search to decision reduction is not known for the duSVP. Cai also shows that duSVP is in co-AM for $n^{1/4}$-unique lattices. We give three results here, all concerning duSVP.

(i). We show that the search uSVP_γ can be solved in polynomial time given an oracle for the $\text{duSVP}_{\gamma/2}$.
(ii). The duSVP problem is in co-AM on $\left(\frac{n}{\log n}\right)^{1/4}$-unique lattices and is in co-NP for $n^{1/4}$-unique lattices.
(iii). The duSVP problem is NP-hard under randomized reductions on $(1 + 2^{-O(n^2)})$-unique lattices.

It is unlikely that GapSVP_γ is NP-hard for $\gamma = \left(\frac{n}{\log n}\right)^{1/2}$, as otherwise the polynomial hierarchy collapses [6,5]. The same conclusion does not follows from item (ii) in case of duSVP as the duSVP is a promise problem (as opposed to a *total* problem) and, unlike GapSVP, we do not know how to handle the queries which do not satisfy the promise.

The results on duSVP can be interpreted as follows. Items (i)+(iii) indicate that duSVP is likely to be a difficult problem, especially if we assume that uSVP is a hard problem. On the other hand, item (ii) points out that duSVP perhaps is not so hard on $\left(\frac{n}{\log n}\right)^{1/4}$-unique lattices. Showing that the polynomial hierarchy collapses if duSVP is NP-hard on $\left(\frac{n}{\log n}\right)^{1/4}$-unique lattices is an open problem.

2. Preliminaries

For a positive integer k we use the notation $[k]$ to denote the set $\{1, \ldots, k\}$.

A lattice basis is a set of linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^m$. It is sometimes convenient to think of the basis as an $m \times n$ matrix $\mathbf{B}$, whose n columns are the vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$. The lattice generated by the basis $\mathbf{B}$ will be written as $\mathrm{L}(\mathbf{B})$ and is defined as $\mathrm{L}(\mathbf{B}) = \{\mathbf{Bx} | \mathbf{x} \in \mathbb{Z}^n\}$. A vector $\mathbf{v} \in \mathrm{L}$ is called a primitive vector of the lattice L if it is not an integer multiple of another lattice vector except $\pm\mathbf{v}$. In order for the input to be representable in a finite number of bits, we must assume that $\mathbf{b}_1, \ldots, \mathbf{b}_n$ are in $\mathbb{Q}^m$. By appropriately scaling the lattice by an integer factor, we can assume that the given lattice is over integers, i.e., $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{Z}^m$. For the remainder of the paper, we will assume this unless otherwise stated. The *successive minima* $\lambda_i(\mathrm{L})$ (where $i = 1, \ldots, n$) of the lattice L is defined as the smallest radius of a sphere centered at the origin that contains at least i linearly independent lattice vectors. A lattice L is called γ-unique if $\lambda_2(\mathrm{L}) > \gamma\lambda_1(\mathrm{L})$. In this paper we are concerned with the following variants of the unique shortest vector problem.

uSVP_γ*:* Given a γ-unique lattice basis $\mathbf{B}$, find a vector $\mathbf{v} \in \mathrm{L}(\mathbf{B})$ such that $\|\mathbf{v}\| = \lambda_1(\mathrm{L}(\mathbf{B}))$.

duSVP_γ*:* Given a γ-unique lattice basis $\mathbf{B}$, and an integer d, say "YES" if $\lambda_1(\mathbf{B}) \le d$ and "NO" otherwise.

duSVP'_γ*:* Given a γ-unique lattice basis $\mathbf{B} = [\mathbf{b}_1, \cdots, \mathbf{b}_n]$ and a prime $p > 2$, say "YES" if p divides the coefficient of $\mathbf{b}_1$ in the shortest vector of the lattice $\mathrm{L}(\mathbf{B})$ and say "NO" otherwise.

There are two decision variants of the uSVP problem. Chronologically, the first one i.e., duSVP was defined implicitly in [4] and explicitly in [5]. The second one i.e., duSVP′, is given in [16] and has the desirable property that uSVP_γ can be solved using an oracle that solves duSVP'_γ.

We will also need the following definition of the GapSVP problem.

GapSVP_γ*:* Given a lattice basis $\mathbf{B}$, and an integer d, say "YES" if $\lambda_1(\mathbf{B}) \le d$ and "NO", if $\lambda_1(\mathbf{B}) > \gamma \cdot d$.

We now prove some useful results on lattices. The following lemma is taken from [12]. A proof is provided for completeness.

Lemma 1. *Let* $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ *be a basis of a lattice* L*. For any two vectors* $\mathbf{u} = \sum_{i=1}^n \alpha_i \mathbf{b}_i, \mathbf{v} = \sum_{i=1}^n \beta_i \mathbf{b}_i \in \mathrm{L}$ *such that* $\mathbf{u} \ne \pm\mathbf{v}$ *and* $\|\mathbf{u}\| = \|\mathbf{v}\| = \lambda_1(\mathrm{L})$*, there exists* $j \in [n]$ *such that* $\alpha_j \not\equiv \beta_j \pmod 2$.

Proof. For the sake of contradiction, assume that there exists a lattice vector $\mathbf{u} = \sum_{i=1}^n \alpha_i \mathbf{b}_i$ and a lattice vector $\mathbf{v} = \sum_{i=1}^n \beta_i \mathbf{b}_i$ such that $\|\mathbf{u}\| = \|\mathbf{v}\| = \lambda_1(\mathrm{L})$ and $\alpha_j \equiv \beta_j \pmod 2$ for all $j \in [n]$. But then, $\frac{\mathbf{u}+\mathbf{v}}{2} \in \mathrm{L}$ and $\frac{\mathbf{u}-\mathbf{v}}{2} \in \mathrm{L}$. Since $\mathbf{u} \ne \pm\mathbf{v}$, both these vectors are non-zero. Also,

$$\left\|\frac{\mathbf{u}+\mathbf{v}}{2}\right\|^2 + \left\|\frac{\mathbf{u}-\mathbf{v}}{2}\right\|^2 = \frac{\|\mathbf{u}\|^2 + \|\mathbf{v}\|^2}{2} = (\lambda_1(\mathrm{L}))^2 .$$

But this implies that $0 < \|\frac{\mathbf{u}+\mathbf{v}}{2}\|, \|\frac{\mathbf{u}-\mathbf{v}}{2}\| < \lambda_1(\mathrm{L})$, which is a contradiction. □

We next define the LLL reduced basis [13].

Definition 1. *Given a basis* $\mathbf{B} = [\mathbf{b}_1\ \mathbf{b}_2\ \ldots\ \mathbf{b}_n]$*, the Gram–Schmidt orthogonalization of* $\mathbf{B}$ *is defined by* $\tilde{\mathbf{b}}_i = \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{i,j} \tilde{\mathbf{b}}_j$*, where* $\mu_{ij} = \frac{\langle \mathbf{b}_i, \tilde{\mathbf{b}}_j \rangle}{\langle \tilde{\mathbf{b}}_j, \tilde{\mathbf{b}}_j \rangle}$.

Note that the Gram–Schmidt orthogonal basis satisfies $\langle \tilde{\mathbf{b}}_i, \tilde{\mathbf{b}}_j \rangle = 0$, for all $i \ne j$.