On the Maximum Distance Sublattice Problem and Closest Vector Problem

Rajendra Kumar, Shashank Mehta and Mahesh Rajasree

September 21, 2024

On the Maximum Distance Sublattice Problem and Closest Vector Problem

Rajendra Kumar
Department of Computer Science & Engineering
Indian Institute of Technology Delhi
New Delhi, India
r_kumar@cse.iitd.ac.in

Shashank K Mehta
Department of Computer Science & Engineering
Indian Institute of Technology Kanpur
Uttar Pradesh, India
skmehta@cse.iitk.ac.in

Mahesh Sreekumar Rajasree
Department of Computer Science & Engineering
Indian Institute of Technology Delhi
New Delhi, India
srmahesh1994@gmail.com

***Abstract*—In this paper, we introduce the Maximum Distance Sublattice Problem (MDSP). We observed that the problem of solving an instance of the Closest Vector Problem (CVP) in a lattice $\mathcal{L}$ is the same as solving an instance of MDSP in the dual lattice of $\mathcal{L}$. We give an alternate reduction between the CVP and MDSP. This alternate reduction does not use the concept of dual lattice.**

***Index Terms*—lattice, Karp reduction, geometry, CVP, GSO**

I. Introduction

For any set of linearly independent vectors $B = \{\vec{b_1}, \ldots, \vec{b_n}\} \in \mathbb{R}^{m\times n}$, a *lattice* $\mathcal{L}$ is defined to be the set of vectors that consists of the integer linear combinations of vectors from B. Formally it is defined as follows.

$$\mathcal{L} = \mathcal{L}(\vec{b_1}, \ldots, \vec{b_n}) = \left\{ \sum_{i=1}^{n} z_i b_i \mid z_1, \ldots, z_n \in \mathbb{Z} \right\}$$

Here, we call n the rank of the lattice $\mathcal{L}$ and m as the ambient dimension. We call the set B a basis of the lattice. Note that, a lattice can have infinitely many bases. Lattices have an enormous number of applications in Number theory [1]–[3] and Cryptanalysis [4], [5]. In the last two decade lattices got special attention due to their applications in Cryptography. Lattice-based Cryptosystems are considered the most prominent candidate for Post-Quantum Cryptography [6]–[9].

The Shortest Vector problem (SVP) and Closest Vector problem (CVP) are two well known and widely studied lattice problems. Given a basis B of the lattice $\mathcal{L}$, the shortest vector problem is to find a shortest (in some norm, usually in Euclidean-norm) non-zero vector in the lattice. In the closest vector problem we are also given a target vector $\vec{t}$ in the vector space of the lattice and the goal is to find the lattice vector closest (usually in Euclidean-norm) to the target $\vec{t}$. CVP is known to be NP-hard for approximation factor less than $n^{1/\log\log n}$ [10]–[12]. SVP is only shown to be NP-hard to approximate with constant approximation factor only by a randomized reduction[1] [13]–[15]. It is also known to be poly-time hard for approximation factor $n^{\mathcal{O}(1/\log\log n)}$ under some complexity theoretic assumption [16], [17]. Recently, there is also a series of works on the fine grained hardness of CVP [18]–[20] and SVP [21]. It is also know that CVP is at least as hard as SVP as there is an approximation factor, rank and dimension preserving reduction from SVP to CVP [22].

All known algorithms for SVP and CVP require at least exponential time. Kannan [2] gave an enumeration based algorithm for CVP which takes $n^{\mathcal{O}(n)}$ time and polynomial space. There are also some improvements on running time of Kannan's algorithm [23], [24]. In 2001, Ajtai, Kumar and Sivakumar gave the first $2^{\mathcal{O}(n)}$ time and space sieving algorithm for SVP [25] and CVP [26]. There has been extensive works to improve the sieving algorithms for SVP and CVP [27]–[32]. Fastest known classical algorithm for SVP and CVP takes $2^{n+o(n)}$ time and space, based on Discrete Gaussian Sampling [33], [34]. Recently Aggarwal, Chen, Kumar and Shen gave a faster quantum algorithm for SVP that requires $2^{0.835n+o(n)}$ time and exponential size QRAM and classical space [35].

In 1982, Lenstra, Lenstra and Lovasz [1] gave a polynomial time algorithm (known as LLL) for finding an exponential approximation of the shortest vector in the lattices. The applications of LLL are found in factoring polynomials over rationals, finding linear Diophantine approximations, cryptanalysis of RSA and other cryptosystems [4], [36], [37]. Babai [38] gave a polynomial time algorithm, which uses LLL, for approximating CVP with exponential approximation factor. Schnorr has given improvements over the LLL algorithm [39], [40].

A. *Our Contributions:*

In this paper, we introduce the Maximum Distance Sublattice Problem (MDSP). Given a lattice vector $\vec{v}$, the goal is to

[1]It is an long standing open problem to show NP-hardness for SVP via a deterministic reduction.

find a sublattice of $n-1$ rank whose distance from the lattice vector $\vec{v}$ is maximum. We first observe that the MDSP problem reduces to the CVP on the dual lattice. The main technical contribution of our work is a reduction between the MDSP and CVP without using the notion of the dual lattice. The reduction employs novel geometric results that might be of independent importance. Our reduction preserves the dimension and rank of the lattice[2].

Theorem 1. *There exists a polynomial time rank-preserving dimension-preserving many-one (Karp) reduction between* MDSP *and* CVP.

The proof of the theorem is presented in Section III. We state our reduction for only for exact problem. It is easy to extend it for any approximation factor.

B. Organisation:

The rest of the paper is organised as follows. In section 2, we provide definitions and the trivial reduction between CVP and MDSP. Section 3 contains our new reduction between CVP and MDSP.

II. Preliminaries

In this paper $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{Q}$ will denote the sets of integers, reals and rationals respectively. Vectors will be denoted by small letters as in $\vec{v}$ and matrices and basis sets will be denoted in capital letters. We will use $\mathbb{I}_n$ to denote the $n \times n$ identity matrix. Let $B = \{\vec{b_1}, \dots, \vec{b_k}\}$ be a set of vectors in $\mathbb{R}^n$. The subspace of $\mathbb{R}^n$ spanned by B will be denoted by $span(B)$.

In this paper, we will work with vector space $V = \mathbb{R}^n$. For any vectors $\vec{u}, \vec{v} \in \mathbb{R}^n$, we use the notation $\langle \vec{u}, \vec{v} \rangle$ to denote the dot-product of the two vectors, i.e., $\langle \vec{u}, \vec{v} \rangle = \sum_{i=1}^{n} \vec{u}_i \vec{v}_i$ and $||\vec{u}||$ denotes the ℓ_2 norm of the $\vec{u}$, i.e., $||\vec{u}|| = (\sum_{i=1}^{n} \vec{u}_i^2)^{1/2}$. For a subspace $S \subseteq \mathbb{R}^n$, $S^\perp = \{\vec{x} \in \mathbb{R}^n | \langle \vec{x}, \vec{y} \rangle = 0, \ \forall \vec{y} \in S\}$ is also a subspace and it is called the *orthogonal subspace* of S.

Definition 1 (Lattice)**.** *Given a set of linearly independent vectors $B = \{\vec{b_1}, \dots, \vec{b_m}\}$ in a vector space V, the lattice spanned by B is the set*

$$\mathcal{L}(B) = \left\{ \sum_{i=1}^{m} c_i \vec{b_i} \mid c_i \in \mathbb{Z} \text{ for all } 1 \leq i \leq m \right\}$$

In other words, a lattice is an integral span of B. The set B is referred to as a *basis* of the lattice. The *rank* of the lattice is the number of linearly independent vectors in B and the dimension of a lattice is the dimension of the ambient vector space containing the lattice. In this paper, we denote B by a matrix where column vectors are the vectors of the generating set. In this representation, the rank of a lattice is the same as the rank of the matrix B. Similar to a vector space, a lattice has infinitely many bases. We will need the concept of unimodular matrices to characterize the bases of a given lattice.

[2]We say a reduction is dimension-preserving and rank-preserving as long as the rank and dimension increases (or decreases) at most by 1.

Definition 2 (Unimodular Matrix)**.** *A matrix $U \in \mathbb{Z}^{n \times n}$ which has a determinant equal to 1 or -1, is called a unimodular matrix.*

Notice that the inverse and the transpose of a unimodular matrix are also unimodular. The following theorem states that two bases generate the same lattice if they are related by a unimodular matrix.

Theorem 2. *B and B' (in matrix form) are bases of the same rank-n lattice $\mathcal{L}$ in $\mathbb{R}^n$ if and only if there exists an $n \times n$ unimodular matrix U such that $B' = BU$.*

An important concept in lattice theory is the dual of a lattice which is defined as follows.

Definition 3 (Dual Lattice)**.** *Let $\mathcal{L} = \mathcal{L}(B)$ be a lattice in $\mathbb{R}^n$. Then, the dual lattice of $\mathcal{L}$, denoted by $\mathcal{L}^*$ is*

$$\mathcal{L}^* = \{\vec{v} \mid \forall \vec{u} \in \mathcal{L}, \langle \vec{v}, \vec{u} \rangle \in \mathbb{Z}\}$$

Let B be an invertible matrix. Then, it can be easily shown that if B is the basis of $\mathcal{L}$, then $D = (B^{-1})^T$ is a basis for the dual lattice $\mathcal{L}^*$. D is called the dual basis of B. Observe that from the definition of dual basis, we have $D^T B = I$.

Claim 1. *If D is the dual basis of B, then for a basis $B' = BU$ where U is a unimodular matrix, the dual basis is $D' = D(U^{-1})^T$.*

We will now proceeds to define certain computationally hard problems in lattice theory.

Definition 4 (Shortest Vector Problem (SVP))**.** *Given a basis $B = \{\vec{b_1}, \dots, \vec{b_n}\}$, find a shortest non-zero vector $\vec{v}$ in the lattice $\mathcal{L}(B)$, i.e*

$$\vec{v} \in \underset{\vec{u} \in \mathcal{L}(B) \setminus \{0\}}{\arg\min} \ ||\vec{u}||$$

Definition 5 (Closest Vector Problem (CVP))**.** *Given a basis B and a vector $\vec{t}$, find a vector $\vec{v}$ in the lattice $\mathcal{L}(B)$ which is closest from $\vec{t}$, i.e*

$$\vec{v} \in \underset{\vec{u} \in \mathcal{L}(B)}{\arg\min} ||\vec{u} - \vec{t}||$$

In this paper, we assume the vector $\vec{t}$ in CVP instance is linearly independent of basis B. In the case where t is not independent, we can increase the dimension of the vector space and obtain linear independence as follows. We work with B' and t' such that

$$\vec{b_i'} = \begin{bmatrix} \vec{b_i} \\ 0 \end{bmatrix}, \vec{t'} = \begin{bmatrix} \vec{t} \\ 1 \end{bmatrix}$$

Except for a constant factor, this one-dimensional increase has no effect on our/existing algorithms' running time.

Definition 6. *Given a basis $B = \{\vec{b_1}, \dots, \vec{b_k}\}$ of a subspace in $\mathbb{R}^n$, the subspace $span(B)$ has an orthogonal basis $B^* = \{\vec{b_1^*}, \dots, \vec{b_k^*}\}$ given by $\vec{b_i}^* = \vec{b_i} - \sum_{j=1}^{i-1} \mu_{ij} \vec{b_j}^*$ where $\mu_{ij} = \langle \vec{b_i}, \vec{b_j}^* \rangle / (\vec{b_j}^*)^2$. This transformation of the basis is called* Gram Schmidt orthogonalization.

Using a Gram Schmidt orthogonalization of a basis of a subspace S, it is easy to compute the projection of a vector $\vec{v}$ onto the subspace S as follows. Let $B = \{\vec{b_1}, \dots, \vec{b_k}\}$ be a basis of a k-dimensional subspace of $\mathbb{R}^n$ and $\vec{v}$ be a vector in $\mathbb{R}^n$. The projection of $\vec{v}$ on the subspace $S = span(B)$ is its component in S. If B^* is an orthogonal basis of $span(B)$ (such as the one computed by Gram-Schmidt orthogonalization), then the projection of $\vec{v}$ on S is

$$proj_S(\vec{v}) = \sum_{i=1}^{k} \frac{\langle \vec{v}^T, \vec{b_i^*} \rangle}{\langle \vec{b_i^*}, \vec{b_i^*} \rangle} \cdot \vec{b_i^*}$$

The component of $\vec{v}$ perpendicular to S is $\vec{v} - proj_S(\vec{v})$. It is equal to the projection of $\vec{v}$ on $S^{\perp}$, i.e., $proj_{S^{\perp}}(\vec{v}) = \vec{v} - proj_S(\vec{v})$. The *distance* of the point $\vec{v}$ from the subspace S is the length of this vector. So

$$dist(\vec{v}, S) = ||\vec{v} - proj_S(\vec{v})|| = ||proj_{S^{\perp}}(\vec{v})||$$

We now proceed to define *Maximum Distance Sublattice Problem.*

Definition 7 (Maximum Distance Sublattice Problem (MDSP)). *Given a basis $[\vec{v} \mid B] = \{\vec{v}, \vec{b_1}, \dots, \vec{b_n}\}$ for an $n+1$ dimensional lattice $\mathcal{L}$, find $B' = \{\vec{b'_1}, \dots, \vec{b'_n}\}$ such that $\{\vec{v}, \vec{b'_1}, \dots, \vec{b'_n}\}$ is also a basis for $\mathcal{L}$ and the distance $dist(\vec{v}, span(B'))$ is maximum. Here, we call $\vec{v}$ the fixed vector.*

The following theorem shows that a solution B' to the MDSP can be achieved from B by adding integral multiples of $\vec{v}$ to vectors in B.

Theorem 3. *Let $[\vec{v} \mid B]$ be a basis of an $n+1$ dimensional lattice $\mathcal{L}$ in $\mathbb{R}^{n+1}$. Then for any basis of the lattice of the form $[\vec{v} \mid B'']$, there exists integers $\alpha_1, \alpha_2, \dots, \alpha_n$ such that $[\vec{v} \mid B']$ is also a lattice basis and $span(B') = span(B'')$ where*

$$B' = B + [\alpha_1 \vec{v}, \alpha_2 \vec{v}, \dots, \alpha_n \vec{v}]$$

We have included a proof of the above theorem in the Section A as we were unable to provide a reference for it.

The following theorem shows a trivial reduction between SVPS and MDSP.

Theorem 4. *There exist polynomial time rank and dimension preserving many-one (Karp) reductions between* CVP *and* MDSP.

Proof. We will show that MDSP$([\vec{v}, \vec{b}_1, \dots, \vec{b}_n])$ is equivalent to CVP on basis $([\vec{d}_1, \dots, \vec{d}_n])$ and target $\vec{u}$ where $[\vec{u}, \vec{d}_1, \dots, \vec{d}_n]$ is the dual basis of $[\vec{v}, \vec{b}_1, \dots, \vec{b}_n]$. We will first show the reduction from MDSP to CVP and since all the computations in the reduction are invertible, the other direction is trivial.

Let the input to MDSP be $B = [\vec{v}, \vec{b}_1, \dots, \vec{b}_n]$ and its dual basis be $D = [\vec{u}, \vec{d}_1, \dots, \vec{d}_n]$. From Theorem 3, we know that a solution $B' = [\vec{v}, \vec{b}'_1, \dots, \vec{b}'_n]$ to MDSP can be written as $B' = BU = [\vec{v}, \vec{b}_1 + \alpha_1 \vec{v}, \dots, \vec{b}_n + \alpha_n \vec{v}]$, i.e.,

$$U = \begin{bmatrix} 1 & \vec{\alpha}^T \\ 0 & \\ \vdots & \mathbb{I}_n \\ 0 & \end{bmatrix}$$

where $\vec{\alpha}^T = [\alpha_1, \dots, \alpha_n]$ is an integer vectors. From Claim 1, we know that the dual basis D' of B' is $D(U^{-1})^T$ where

$$(U^{-1})^T = \begin{bmatrix} 1 & 0 & \dots & 0 \\ -\vec{\alpha} & & \mathbb{I}_n & \end{bmatrix}$$

Therefore, $D' = [\vec{u} - \sum_{i=1}^{n} \alpha_i \vec{d}_i, \vec{d}_1, \dots, \vec{d}_n]$. Also, from the definition of dual basis, we have $(D')^T B' = I$, therefore,

$$\langle \vec{v}, \left(\vec{u} - \sum_{i=1}^{n} \alpha_i \vec{d}_i \right) \rangle = 1 \tag{1}$$

Using the fact that $\langle \vec{a}, \vec{b} \rangle = ||\vec{a}|| \cdot ||\vec{b}|| \cdot \cos(\theta)$ where θ is the angle between $\vec{a}$ and $\vec{b}$, we get

$$||\vec{v}|| \cdot \cos(\theta) = \frac{1}{||\vec{u} - \sum_{i=1}^{n} \alpha_i \vec{d}_i||} \tag{2}$$

where θ is the angle between $\vec{v}$ and $\vec{u} - \sum \alpha_i \vec{d}_i$. Using the definition of dual basis, we know that $\vec{u} - \sum \alpha_i \vec{d}_i$ is perpendicular to all $\vec{b}'_i$ because D' is the dual of B'. Therefore, $\vec{u} - \sum \alpha_i \vec{d}_i$ is perpendicular to $span(\vec{b}'_1, \dots, \vec{b}'_n)$. This implies that $90 - \theta$ is the angle between $\vec{v}$ and $span(\vec{b}'_1, \dots, \vec{b}'_n)$. Hence, $||\vec{v}|| \cdot \sin(90 - \theta)$ is the perpendicular distance between $\vec{v}$ and $span(\vec{b}'_1, \dots, \vec{b}'_n)$.

Recall that B' is the solution to the MDSP instance, which means that the perpendicular distance between $\vec{v}$ and $span(\vec{b}'_1, \dots, \vec{b}'_n)$ is maximized. In other words, $||\vec{v}|| \cdot \sin(90 - \theta)$ is maximized. Therefore, $||\vec{u} - \sum \alpha_i \vec{d}_i||$ is minimized due to Equation (2). But, this is essentially computing the shortest vector in the shifted lattice $\vec{u} + \mathcal{L}(\vec{d}_1, \dots, \vec{d}_n)$, which is exactly CVP with the basis $\{\vec{d}_1, \cdots, \vec{d}_n\}$ and target $\vec{u}$. $\square$

III. New Reduction between MDSP and CVP

In this section, we prove our main theorem, i.e., Theorem 1 which is reduction between MDSP and CVP which does not utilize the concept of dual lattices. Let $[\vec{v} \mid B]$ be an input to the MDSP.

Keeping Theorem 3 in consideration, the maximum distance sub-lattice problem can be stated as follows. Given an $(n+1)$-dimensional lattice with basis $\{\vec{v}, \vec{b_1}, \dots, \vec{b_n}\}$, compute an alternative basis $\{\vec{v}, \vec{b_1} + j_1 \vec{v}, \dots, \vec{b_n} + j_n \vec{v}\}$ such that the distance of point v from the subspace spanned by $\{\vec{b_1} + j_1 \vec{v}, \dots, \vec{b_n} + j_n \vec{v}\}$ is maximum, where $j_i \in \mathbb{Z}$ for all $i \in [n]$.

Let $P_{x_1,\dots,x_n}$ denote the subspace spanned by the vectors $\vec{b_1} + x_1 \vec{v}, \dots, \vec{b_n} + x_n \vec{v}$ for $(x_1, \dots, x_n) \in \mathbb{R}^n$. Following result determines the distance of the point $\vec{v}$ from $P_{x_1,\dots,x_n}$ for the special case when $\{\vec{v}, \vec{b_1}, \dots, \vec{b_n}\}$ is an orthonormal basis.

Lemma 5. *Let $\{\vec{v}, \vec{b_1}, \ldots, \vec{b_n}\}$ be an orthonormal basis. Then the distance of point $\vec{v}$ from $P_{x_1,\ldots,x_n}$ is $1/\sqrt{1+\sum_{i=1}^{n} x_i^2}$ for any $(x_1, \ldots, x_n) \in \mathbb{R}^n$.*

Proof. Let $\sum_i c_i(\vec{b_i} + x_i\vec{v})$ be the projection of vector $\vec{v}$ on $P_{x_1,\ldots,x_n}$. Then $\vec{w} = \sum_i c_i(\vec{b_i} + x_i\vec{v}) - \vec{v}$ is the perpendicular drop from point $\vec{v}$ to the plane. This implies that for all $i \in [n]$,

$$\langle \vec{w}, (\vec{b_i} + x_i\vec{v})\rangle = 0 \tag{3}$$

By expanding the $\vec{w}$ term and crucially using the fact that the vectors are orthonormal, we get

$$\begin{aligned}
&\langle \vec{w}, (\vec{b_i} + x_i\vec{v})\rangle \\
&= \langle \sum_{j=1}^{n} c_j(\vec{b_j} + x_j\vec{v}) - \vec{v}, (\vec{b_i} + x_i\vec{v})\rangle \\
&= \langle \sum_{j=1}^{n} c_j(\vec{b_j} + x_j\vec{v}), (\vec{b_i} + x_i\vec{v})\rangle - \langle \vec{v}, (\vec{b_i} + x_i\vec{v})\rangle \\
&= \langle \sum_{j=1}^{n} c_j(\vec{b_j} + x_j\vec{v}), (\vec{b_i} + x_i\vec{v})\rangle - x_i \\
&= \sum_{j=1}^{n} \langle c_j(\vec{b_j} + x_j\vec{v}), (\vec{b_i} + x_i\vec{v})\rangle - x_i \\
&= \sum_{j\neq i} \langle c_j(\vec{b_j} + x_j\vec{v}), (\vec{b_i} + x_i\vec{v})\rangle + c_i(1+x_i^2) - x_i \\
&= \sum_{j\neq i} (c_j x_j x_i) + c_i(1+x_i^2) - x_i \\
&= c_i + x_i \cdot \left(\sum_{j=1}^{n} (c_j x_j) - 1\right)
\end{aligned}$$

By equating the last equation to 0, we get $c_i = -x_i t$ where $t = \sum_{j=1}^{n} c_j x_j - 1$. This gives us

$$\begin{aligned}
\vec{w} &= \sum_{i=1}^{n} c_i(\vec{b_i} + x_i\vec{v}) - \vec{v} \\
&= \sum_{i=1}^{n} (-x_i t) \cdot (\vec{b_i} + x_i\vec{v}) - \vec{v} \\
&= \left(\sum_{i=1}^{n} -x_i t \cdot \vec{b_i}\right) + \left(\sum_{i=1}^{n} -x_i^2 t - 1\right)\vec{v}
\end{aligned}$$

The square of the distance of $\vec{v}$ from the plane $P_{x_1,\ldots,x_n}$ is

$$\begin{aligned}
||\vec{w}||^2 &= \sum_{i=1}^{n} c_i^2 + (\sum_{i=1}^{n} c_i x_i - 1)^2 \\
&= \sum_{i=1}^{n} c_i^2 + t^2 \\
&= t^2(1 + \sum_{i=1}^{n} x_i^2)
\end{aligned}$$

We now focus on expressing t in terms of x_i's. We have

$$\begin{aligned}
t &= \sum_{i=1}^{n} x_i c_i - 1 \\
&= -t\sum_{i=1}^{n} x_i^2 - 1 \\
\implies t &= -1/(1 + \sum_{i=1}^{n} x_i^2)
\end{aligned}$$

Plugging this in the expression for $||\vec{w}||^2$ we get $\vec{w}^2 = 1/(1 + \sum_{i=1}^{n} x_i^2)$. □

The distance of a vector from a plane P is equal to the length of the vector's projection on the orthogonal plane $P^{\perp}$ and projection is directly proportional to the length of the vector. Hence we have a trivial consequence.

Corollary 6. *Let $\{\vec{v}, \vec{b_1}, \ldots, \vec{b_n}\}$ be an orthogonal basis in which all but $\vec{v}$ are unit vectors. Then the distance of point $\vec{v}$ from $P_{x_1,\ldots,x_n}$ is $||\vec{v}||/\sqrt{1+||\vec{v}||^2\sum_{i=1}^{n} x_i^2}$ for any $(x_1, \ldots, x_n) \in \mathbb{R}^n$.*

Proof. In this case $\vec{v}$ is no longer a unit vector. The basis of $P_{x_1,\ldots,x_n}$ is $\{\vec{b}_1 + x_1\vec{v}, \vec{b}_2 + x_2\vec{v}, \ldots\}$. It is same as $\{\vec{b}_1 + x_1'\vec{u}, \vec{b}_2 + x_2'\vec{u}, \ldots\}$ where the additive vector $\vec{u} = \vec{v}/||\vec{v}||$ is a unit vector as required in Lemma 5 and $x_i' = ||\vec{v}||x_i$. From the lemma, the distance of the point $\vec{u}$ from $P_{x_1',\ldots,x_n'}$, is $1/\sqrt{1+\sum_i (x_i')^2} = 1/\sqrt{1+||\vec{v}||^2\sum_i x_i^2}$. Hence the distance from $\vec{v}$ is $||\vec{v}||/\sqrt{1+||\vec{v}||^2\sum_i x_i^2}$. □

We will now focus on the general case in which the vectors $\vec{b_i}$ are not necessarily orthogonal to the vector $\vec{v}$. Let $\vec{b_i'} = \vec{b_i} - \gamma_i\vec{v}$ be perpendicular to $\vec{v}$ for each i, where $\gamma_i \in \mathbb{R}, \forall i$. So $\gamma_i = \langle \vec{b_i}, \vec{v}\rangle/||\vec{v}||^2$ and the plane spanned by $\{\vec{b_1'}, \ldots, \vec{b_n'}\}$ is perpendicular to $\vec{v}$. Note that γ_i need not be an integer. Note that a lattice vector $\vec{b_i} + j_i.\vec{v}$ can now be represented as $\vec{b_i'} + (\gamma_i + j_i)\vec{v}$ in the new reference frame.

Consider the plane $P_{x_1,\ldots,x_n}$ which is spanned by $\vec{b_1} + x_1\vec{v}, \ldots, \vec{b_n} + x_n\vec{v}$. In the new basis, we have

$$P_{x_1,\ldots,x_n} = span(\vec{b_1'} + (\gamma_1 + x_1)\vec{v}, \ldots, \vec{b_n'} + (\gamma_n + x_n)\vec{v}) \tag{4}$$

Let us now transform the basis, $\{\vec{b_1'}, \ldots, \vec{b_n'}\}$, of the n-dimensional subspace into an orthonormal basis. Let B' denote the matrix in which column vectors are $\vec{b_1'}, \vec{b_2'}, \ldots, \vec{b_n'}$. Let L be a linear transformation such that the column vectors of $B'' = B'L$ form an orthonormal basis. Denote the column vectors of B'' by $\vec{b_1''}, \ldots, \vec{b_n''}$ which are unit vectors and mutually orthogonal. Therefore,

$$\vec{b_i''} = \sum_{k=1}^{n} L_{ki} \cdot \vec{b_k'} \tag{5}$$

Note that the new basis $\{\vec{b_1''}, \ldots, \vec{b_n''}\}$ spans the same subspace which is spanned by $\vec{b_1'}, \ldots, \vec{b_n'}$. Now $\{\vec{v}, \vec{b_1''}, \ldots, \vec{b_n''}\}$ forms an orthogonal basis such that all but $\vec{v}$ are unit vectors.

The plane $P_{x_1,\ldots,x_n}$ is spanned by $\vec{b_1'} + (\gamma_1 + x_1)\vec{v}, \ldots, \vec{b_n'} + (\gamma_n + x_n)\vec{v}$. We will now focus on expressing this plane in terms of the unit vectors $\{\vec{b_i''}\}$. If we extend a line parallel to $\vec{v}$ from the point $\vec{b_i''}$ (where $\vec{v}$ and $\vec{b_i''}$ are perpendicular to each other, for all $i \in [n]$), then it must intersect this plane at one point, say, $\vec{b_i''} + y_i\vec{v}$. Then the plane spanned by $\{\vec{b_1''} + y_1\vec{v}, \ldots, \vec{b_n''} + y_n\vec{v}\}$ is $P_{x_1,\ldots,x_n}$ itself.

Using Equation (5), we have

$$\vec{b_i''} + y_i\vec{v} = \sum_{k=1}^{n} L_{ki} \cdot \vec{b_k'} + y_i\vec{v}$$
$$= \sum_{k=1}^{n} L_{ki}(\vec{b_k'} + (\gamma_k + x_k)\vec{v}) - \sum_{k=1}^{n} L_{ki}(\gamma_k + x_k)\vec{v} + y_i\vec{v}$$

By the choice of y_i, $\vec{b_i''} + y_i\vec{v}$ belongs to $P_{x_1,\ldots,x_n}$. From Equation (4), we know that vector $\vec{b_k'} + (\gamma_k + x_k)\vec{v}$ also belongs to the plane for each k. But, v does not belong to the plane because it is linearly independent from the set of vector $\{\vec{b}_k\}$. Thus, from the linear independence, we can conclude that

$$-\sum_{k=1}^{n} L_{ki}(\gamma_k + x_k)\vec{v} + y_i\vec{v} = 0$$

This implies that

$$y_i = \sum_{k=1}^{n} L_{ki}(\gamma_k + x_k)$$
$$\implies \vec{y} = L^T \cdot \vec{\gamma} + L^T \cdot \vec{x}$$

The plane $P_{x_1,\ldots,x_n}$ is spanned by $\vec{b_1''} + y_1\vec{v}, \ldots, \vec{b_n''} + y_n\vec{v}$ where $\{\vec{b_1''}, \ldots, \vec{b_n''}\}$ is an orthonormal basis and $\vec{v}$ is perpendicular to each vector of the set. From Corollary 6, the square of the distance of $\vec{v}$ from the plane $P_{x_1,\ldots,x_n}$ is $||\vec{v}||^2/(1 + ||\vec{v}||^2 \sum_i y_i^2)$.

Recall that our goal is to find a sub-lattice plane $P_{j_1,\ldots,j_n}$, where $\vec{j} \in \mathbb{Z}^n$, such that the distance from $\vec{v}$ is maximized. Equivalently, we want to find a sub-lattice plane such that $\sum_i y_i^2 = ||\vec{y}||^2$ is minimized, i.e., to minimize the length of the vector $\vec{y}$. Let $\vec{x} = \vec{j} \in \mathbb{Z}^n$, then corresponding $\vec{y} = L^T \cdot \vec{\gamma} + L^T \cdot \vec{j}$.

We now proceed to construct a CVP instance that will solve the MDSP instance. We start define a lattice $\mathcal{L}_1$ with basis L^T, i.e., the row vectors of L form a basis of $\mathcal{L}_1$. We denote the rows of L by $\{\vec{r_1}, \ldots, \vec{r_n}\}$. Let $\vec{z} = -L^T \cdot \vec{\gamma} = -\sum_i \gamma_i\vec{r_i}$. Then the length of the vector $\vec{y}$ is equal to the distance between the fixed point $\vec{z}$ and the lattice point $\sum_i j_i\vec{r_i}$ of $\mathcal{L}_1$. Thus the problem reduces to finding a lattice point of $\mathcal{L}_1$ closest to the point $\vec{z}$. Therefore, we have reduced MDSP to an instance of CVP where $\{\vec{r}_1, \ldots, \vec{r}_n\}$ is a lattice basis and $\vec{z}$ is the fixed point.

The following lemma summarises the computations needed to convert a MDSP instance to a CVP instance.

Lemma 7. *Given a basis of an $(n + 1)$-dimensional lattice $\{v, b_1, \ldots, b_n\}$ as an instance of* MDSP. *Let $\vec{b_i'} = \vec{b_i} - \gamma_i\vec{v}$ for all $1 \le i \le n$ where $\gamma_i = \langle\vec{b_i}, \vec{v}\rangle/||\vec{v}||^2$. Let L be a linear transformation such that $B'' = B' \cdot L$ is an orthonormal basis. Equivalently $\{\vec{b_1''}, \ldots, \vec{b_n''}\}$ is an orthonormal basis where $\vec{b_i''} = \sum_k (L^T)_{ik}\vec{b_k'}$. Let $\vec{r_i}$ denote the i-th row of L. Then the sub-lattice plane $P_{j_1,\ldots,j_n}$ has maximum distance from the point $\vec{v}$ if $\sum_i j_i\vec{r_i}$ is a closest lattice vector for the* CVP *instance in which the lattice basis is $\{\vec{r}_1, \ldots, \vec{r}_n\}$ and the fixed point is $-L^T \cdot \vec{\gamma}$.*

The entire transformation involves only invertible steps hence the converse of the above claim also holds.

Lemma 8. *Let the basis $\{\vec{s_1}, \ldots, \vec{s_n}\}$ and the fixed point $\vec{t} \in \mathbb{R}^{n+1}$ be an instance of* CVP. *Let L be the matrix in which i-th row is $\vec{s_i}$ for all $1 \le i \le n$. Let $\gamma = -(L^T)^{-1} \cdot \vec{t}$. Pick an arbitrary orthonormal basis $\{\vec{e_0}, \vec{e_1''}, \ldots, \vec{e_n''}\}$ for $\mathbb{R}^{n+1}$. Let B'' be the matrix with column vectors $\vec{e_1''}, \ldots, \vec{e_n''}$. Let $B' = B'' \cdot L^{-1}$. Let $\vec{e_i'}$ denote the i-th column of B'. Let $\vec{e_i} = \vec{e_i'} + \gamma_i\vec{e_0}$. If the* MDSP *instance $\{\vec{e_0}, \vec{e_1}, \ldots, \vec{e_n}\}$ has an optimum solution sub-lattice plane formed by $\{\vec{e_1} + j_1\vec{e_0}, \ldots, \vec{e_n} + j_n\vec{e_0}\}$, then $\sum_i j_i\vec{s_i}$ is the solution of the given* CVP *instance.*

Finally, Theorem 1 is obtained by combining Lemma 7 and Lemma 8.

REFERENCES

[1] A. K. Lenstra, H. W. Lenstra, and L. Lovász, "Factoring polynomials with rational coefficients," *Mathematische Annalen*, vol. 261, no. 4, pp. 515–534, 1982.

[2] R. Kannan, "Minkowski's convex body theorem and integer programming," *Mathematics of operations research*, vol. 12, no. 3, pp. 415–440, 1987.

[3] A. Frank and É. Tardos, "An application of simultaneous diophantine approximation in combinatorial optimization," *Combinatorica*, vol. 7, pp. 49–65, 1987.

[4] A. Shamir, "A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem," in *Foundations of Computer Science, 1982. SFCS'08. 23rd Annual Symposium on*, pp. 145–152, IEEE, 1982.

[5] E. F. Brickell, "Breaking iterated knapsacks," in *Workshop on the Theory and Application of Cryptographic Techniques*, pp. 342–358, Springer, 1984.

[6] M. Ajtai, "Generating hard instances of lattice problems," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pp. 99–108, 1996.

[7] D. Micciancio and O. Regev, "Worst-case to average-case reductions based on gaussian measures," *SIAM Journal on Computing*, vol. 37, no. 1, pp. 267–302, 2007.

[8] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *Journal of the ACM (JACM)*, vol. 56, no. 6, pp. 1–40, 2009.

[9] O. Regev, "Lattice-based cryptography," in *Annual International Cryptology Conference*, pp. 131–141, Springer, 2006.

[10] S. Arora, L. Babai, J. Stern, and Z. Sweedyk, "The hardness of approximate optima in lattices, codes, and systems of linear equations," *Journal of Computer and System Sciences*, vol. 54, no. 2, pp. 317–331, 1997.

[11] J.-Y. Cai and A. Nerurkar, "Approximating the SVP to within a factor (1-1/dim/sup/spl epsiv//) is NP-hard under randomized conditions," in *Proceedings. Thirteenth Annual IEEE Conference on Computational Complexity (Formerly: Structure in Complexity Theory Conference)(Cat. No. 98CB36247)*, pp. 46–55, IEEE, 1998.

[12] I. Dinur, G. Kindler, and S. Safra, "Approximating-CVP to within almost-polynomial factors is NP-hard," in *Foundations of Computer Science, 1998. Proceedings. 39th Annual Symposium on*, pp. 99–109, IEEE, 1998.

[13] M. Ajtai, "The Shortest Vector Problem in L2 is NP-hard for Randomized Reductions (Extended Abstract)," in *STOC*, 1998.

[14] D. Micciancio, "The shortest vector in a lattice is hard to approximate to within some constant," *SIAM journal on Computing*, vol. 30, no. 6, pp. 2008–2035, 2001.

[15] D. Micciancio and P. Voulgaris, "A deterministic single exponential time algorithm for most lattice problems based on voronoi cell computations," *SIAM Journal on Computing*, vol. 42, no. 3, pp. 1364–1391, 2013.

[16] S. Khot, "Hardness of approximating the shortest vector problem in lattices," *Journal of the ACM (JACM)*, vol. 52, no. 5, pp. 789–808, 2005.

[17] I. Haviv and O. Regev, "Tensor-based hardness of the shortest vector problem to within almost polynomial factors," in *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, pp. 469–477, ACM, 2007.

[18] H. Bennett, A. Golovnev, and N. Stephens-Davidowitz, "On the quantitative hardness of cvp," in *FOCS*, 2017.

[19] D. Aggarwal, H. Bennett, A. Golovnev, and N. Stephens-Davidowitz, "Fine-grained hardness of CVP(P)— Everything that we can prove (and nothing else)," in *SODA*, 2021.

[20] D. Aggarwal and R. Kumar, "Why we couldn't prove SETH hardness of the Closest Vector Problem for even norms!," in *2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS)*, pp. 2213–2230, IEEE, 2023.

[21] D. Aggarwal and N. Stephens-Davidowitz, "(Gap/S)ETH Hardness of SVP," in *STOC*, 2018.

[22] O. Goldreich, D. Micciancio, S. Safra, and J.-P. Seifert, "Approximating shortest lattice vectors is not harder than approximating closest lattice vectors," *Information Processing Letters*, vol. 71, no. 2, pp. 55–61, 1999.

[23] G. Hanrot and D. Stehlé, "Improved analysis of Kannan's shortest lattice vector algorithm," in *Annual International Cryptology Conference*, pp. 170–186, Springer, 2007.

[24] D. Micciancio and M. Walter, "Fast lattice point enumeration with minimal overhead," in *Proceedings of the twenty-sixth annual ACM-SIAM symposium on Discrete algorithms*, pp. 276–294, SIAM, 2014.

[25] M. Ajtai, R. Kumar, and D. Sivakumar, "A sieve algorithm for the shortest lattice vector problem," in *Proceedings of the thirty-third annual ACM symposium on Theory of computing*, pp. 601–610, ACM, 2001.

[26] M. Ajtai, R. Kumar, and D. Sivakumar, "Sampling short lattice vectors and the closest lattice vector problem," in *Proceedings 17th IEEE Annual Conference on Computational Complexity*, pp. 53–57, IEEE, 2002.

[27] P. Q. Nguyen and T. Vidick, "Sieve algorithms for the shortest vector problem are practical," *Journal of Mathematical Cryptology*, vol. 2, no. 2, pp. 181–207, 2008.

[28] V. Arvind and P. S. Joglekar, "Some sieving algorithms for lattice problems," in *IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science*, Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2008.

[29] J. Blömer and S. Naewe, "Sampling methods for shortest vectors, closest vectors and successive minima," *Theoretical Computer Science*, vol. 410, no. 18, pp. 1648–1665, 2009.

[30] X. Pujol and D. Stehlé, "Solving the Shortest Lattice Vector Problem in Time 22.465 n.," *IACR Cryptology ePrint Archive*, vol. 2009, p. 605, 2009.

[31] D. Micciancio and P. Voulgaris, "Faster exponential time algorithms for the shortest vector problem," in *Proceedings of the twenty-first annual ACM-SIAM symposium on Discrete Algorithms*, pp. 1468–1480, Society for Industrial and Applied Mathematics, 2010.

[32] G. Hanrot, X. Pujol, and D. Stehlé, "Algorithms for the shortest and closest lattice vector problems," in *International Conference on Coding and Cryptology*, pp. 159–190, Springer, 2011.

[33] D. Aggarwal, D. Dadush, O. Regev, and N. Stephens-Davidowitz, "Solving the shortest vector problem in 2n time using discrete gaussian sampling," in *Proceedings of the forty-seventh annual ACM symposium on Theory of computing*, pp. 733–742, ACM, 2015.

[34] D. Aggarwal, D. Dadush, and N. Stephens-Davidowitz, "Solving the Closest Vector Problem in 2ˆ n Time–The Discrete Gaussian Strikes Again!," in *2015 IEEE 56th Annual Symposium on Foundations of Computer Science*, pp. 563–582, IEEE, 2015.

[35] D. Aggarwal, Y. Chen, R. Kumar, and Y. Shen, "Improved classical and quantum algorithms for the shortest vector problem via bounded distance decoding," *arXiv preprint arXiv:2002.07955*, 2020.

[36] D. Coppersmith, "Finding a small root of a univariate modular equation," in *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 155–165, Springer, 1996.

[37] D. Coppersmith, "Finding a small root of a bivariate integer equation; factoring with high bits known," in *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 178–189, Springer, 1996.

[38] L. Babai, "On Lovász lattice reduction and the nearest lattice point problem," *Combinatorica*, vol. 6, no. 1, pp. 1–13, 1986.

[39] C.-P. Schnorr, "A hierarchy of polynomial time lattice basis reduction algorithms," *Theoretical computer science*, vol. 53, no. 2-3, pp. 201–224, 1987.

[40] C.-P. Schnorr and M. Euchner, "Lattice basis reduction: Improved practical algorithms and solving subset sum problems," *Mathematical programming*, vol. 66, no. 1-3, pp. 181–199, 1994.

APPENDIX

PROOF OF THEOREM 3

In this section, we provide a proof for Theorem 3.

Proof. Since $[\vec{v} \mid B'']$ and $[\vec{v} \mid B]$ generate the same lattice, there exists a unimodular matrix U' (refer Theorem 2) such that

$$[\vec{v} \mid B''] = [\vec{v} \mid B]U'$$

where

$$U' = \begin{bmatrix} 1 & \beta_1 & \beta_2 & \dots & \beta_{n-1} & \beta_n \\ 0 & & & & & \\ \vdots & & & U & & \\ 0 & & & & & \end{bmatrix}$$

The determinant $det(U') = 1 \times det(U) = \pm 1$, so $det(U) = \pm 1$. Observe that $U' \in \mathbb{Z}^{(n+1)\times(n+1)}$, so $U \in \mathbb{Z}^{n\times n}$ and is unimodular. So U^{-1} exists and it is also unimodular. Let us denote $[\beta_1, \beta_2, \dots, \beta_n]$ by $\vec{\beta}^T$. Then

$$\begin{aligned}
&[v \mid B''] \begin{bmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & & & & & \\ \vdots & & & U^{-1} & & \\ 0 & & & & & \end{bmatrix} \\
&= [v \mid B] \begin{bmatrix} 1 & \vec{\beta}^T \\ 0 & \\ \vdots & U \\ 0 & \end{bmatrix} \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & U^{-1} & \\ 0 & & & \end{bmatrix} \\
&= [\vec{v} \mid B] \begin{bmatrix} 1 & \vec{\beta}^T U^{-1} \\ 0 & \\ \vdots & UU^{-1} \\ 0 & \end{bmatrix} \\
&= [\vec{v} | B] \begin{bmatrix} 1 & \vec{\beta}^T U^{-1} \\ 0 & \\ \vdots & \mathbb{I}_n \\ 0 & \end{bmatrix} \\
&= [\vec{v} \mid B] + [\vec{0} \mid \alpha_1\vec{v}, \dots, \alpha_n\vec{v}]
\end{aligned}$$

where $\vec{\beta}^T U^{-1} = (\alpha_1, \dots, \alpha_n)^T$. The left-hand side in the above equation is equal to $[\vec{v} \mid B''U^{-1}]$. So $B''U^{-1} = B + [\alpha_1\vec{v}, \dots, \alpha_n\vec{v}]$.

The matrix U^{-1} is unimodular so B'' and $B' = B''U^{-1}$ span the same sub-lattice and $B' = B + [\alpha\vec{v}, \dots, \alpha_n\vec{v}]$. $\square$