New Results and Proofs in Lattice Theory

A thesis submitted

in Partial Fulfillment of the Requirements

for the Degree of

Master of Technology

by

Mahesh Sreekumar Rajasree

17111273

to the

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

INDIAN INSTITUTE OF TECHNOLOGY KANPUR

May, 2022

CERTIFICATE

It is certified that the work contained in the thesis titled **New Results and Proofs in Lattice Theory**, by **Mahesh Sreekumar Rajasree**, has been carried out under my supervision and that this work has not been submitted elsewhere for a degree.

Prof. Manindra Agrawal
Department of Computer Science & Engineering
IIT Kanpur

May, 2022

DECLARATION

This is to certify that the thesis titled **New Results and Proofs in Lattice Theory** has been authored by me. It presents the research conducted by me under the supervision of **Prof. Manindra Agrawal**. To the best of my knowledge, it is an original work, both in terms of research content and narrative, and has not been submitted elsewhere, in part or in full, for a degree. Further, due credit has been attributed to the relevant state-of-the-art and collaborations (if any) with appropriate citations and acknowledgements, in line with established norms and practices.

Name: Mahesh Sreekumar Rajasree
Programme: Master of Technology
Department: Computer Science & Engineering
Indian Institute of Technology Kanpur
Kanpur 208016

May, 2022

ABSTRACT

Name of student: **Mahesh Sreekumar Rajasree** Roll no: **17111273**

Degree for which submitted: **Master of Technology**

Department: **Computer Science & Engineering**

Thesis title: **New Results and Proofs in Lattice Theory**

Name of Thesis Supervisor: **Prof. Manindra Agrawal**

Month and year of thesis submission: **May, 2022**

In this thesis, we give an alternate reduction between Closest Vector Problem (CVP) and a problem which we call Maximum Distance Sublattice Problem (MDSP). We show that the problem of solving an instance of CVP in a lattice $\mathcal{L}$ is the same as solving an instance of MDSP in the dual lattice of $\mathcal{L}$. We also show that the set of Voronoi relevant vectors contains a set of linearly independent vectors whose norms are equal to the Successive Minima, i.e., λ_i. This shows that the algorithm given by Micciancio and Voulgaris [1] to compute the set of all Voronoi relevant vectors can be extended to an $\widetilde{\mathrm{O}}(2^{2n})$-time $\widetilde{\mathrm{O}}(2^n)$-space algorithm for solving Successive Minima Problem (SMP) and Successive Independent Vector Problem (SIVP) without using the reductions from Closest Vector Problem (CVP) to these problems [2]. We also show that the length of the longest Voronoi relevant vector is bounded by $\frac{n^{3/2}}{2}\lambda_n$.

To my grandmother.

Acknowledgements

First and foremost, I would like to thank my advisor, Prof. Manindra Agrawal, for introducing me to the area of lattice theory. He was always able to make me believe in me and build confidence to work in the field of theoretical computer science. I want to express my deepest gratitude to Prof. Shashank K. Mehta for his constant guidance and support. His enthusiasm and perseverance in solving problems motivated me to become a better researcher. Apart from being a great teacher, Prof. Mehta is a fantastic person who has always been concerned about my well-being throughout my research life. This work was done in collaboration with him. I'm fortunate that Rajendra Kumar was a part of my MTech journey and has also contributed to the results of section 3.

I would like to thank my friends Sumanta, Amit, Ramaiah, Pranjal, Prateek, Bhargav, Priyanka, Krishnaprasad, Parvathy, Telma, Smriti and Aditi for the amazing discussions and wonderful friendship which made my life in IITK peaceful. Last but not least, I am extremely thankful to my parents and brother for bearing with me, helping me during my troubled times and having faith in me.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

A *lattice* generated by a set of linearly independent vectors $\{\vec{b_1}, \ldots, \vec{b_n}\}$ is defined to be the set of all integer combinations of $\{\vec{b_1}, \ldots, \vec{b_n}\}$, i.e.,

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

It is a discretization of a vector space and finds applications in number theoretic algorithms and cryptography. One of the most interesting applications of lattices is to build post-quantum cryptosystems. Many powerful cryptographic primitives like fully homomorphic encryption [3], functional encryption [4], etc. can be based on the hardness of certain lattice problems.

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 $\mathcal{L}$, Shortest Vector problem is to find the shortest non-zero vector in the lattice. In the Closest Vector problem we are given a basis of a lattice, a target vector $\vec{t}$ and asked to find the closest lattice vector to the target $\vec{t}$. CVP and SVP are shown to be NP-hard even to approximate within an approximation factor under $n^{\mathcal{O}(1/\log\log n)}$ [9, 8, 5, 11, 10, 7, 6, 1] (for SVP only randomized reduction is known). Recently, there are also results on the fine grained hardness of CVP [12, 13] and SVP [14]. Among these two problem, CVP is harder than SVP as there is an approximation factor preserving reduction from SVP to CVP[15]. Very recently, Divesh et al.[16] showed dimension preserving reduction between SVP and CVP in different p-norms.

All the known algorithms for solving the exact SVP and CVP take exponential time. Kannan [17] gave an enumeration based algorithm for CVP which takes $n^{\mathcal{O}(n)}$ time and polynomial space. There are also some improvements on runing time of Kannan's algorithm [18, 19]. In 2001, Ajtai, Kumar and Sivakumar gave the first $2^{\mathcal{O}(n)}$ time and space sieving algorithm for SVP [20] and CVP [21]. There is a lot of work in the sieving algorithm for SVP and CVP [26, 22, 23, 25, 27, 24]. The fastest known algorithm to solve SVP and CVP is due to Micciancio and Voulgaris [1] which uses the concept of Voronoi relevant vectors. Fastest know algorithm for SVP and CVP takes $2^{n+o(n)}$ time and space, which is based on Discrete Gaussian Sampling [29, 28].

Algorithm	Time complexity	Space Complexity
Enumeration	$n^{O(n)}$	$\mathsf{poly}(n)$
Sieving	$2^{O(n)}$	$2^{O(n)}$
Voronoi	$\tilde{O}(2^{2n})$	$\tilde{O}(2^{n})$
Gaussian	$2^{n+o(n)}$	$2^{n+o(n)}$

Table 1.1: Algorithms for CVP

In 1982, Lenstra et al. [30] 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 [31, 33, 32]. Babai [34] gave a polynomial time algorithm for approximating CVP with exponential approximation factor which uses LLL. Schnorr has given improvements over the LLL algorithm [36, 35].

1.1 Our Contributions

The first part of this thesis focuses on CVP and Maximum Distance Sublattice Problem (MDSP). We give an alternate reduction between CVP and a problem which we call MDSP. It can be shown that the problem of solving an instance of CVP in a lattice $\mathcal{L}$ is the same as solving an instance of MDSP in the dual lattice of $\mathcal{L}$.

The second part of the thesis deals with the Voronoi relevant vectors and the Successive Minima. We show that the set of Voronoi relevant vectors contains a set of linearly independent vectors whose norms are equal to the Successive Minima, i.e., λ_i. This shows that the algorithm given by Micciancio and Voulgaris [1] to compute the set of all Voronoi relevant vectors can be extended to an $\tilde{O}(2^{2n})$-time $\tilde{O}(2^n)$-space algorithm for solving Successive Minima Problem (SMP) and Successive Independent Vector Problem (SIVP) without using the reductions from CVP to these problems [2]. We also show that the length of the longest Voronoi relevant vector is bounded by $\frac{n^{3/2}}{2}\lambda_n$.

Chapter 2

Preliminaries and notations

2.1 Notations

In this thesis, $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{Q}$ will denote the sets of integers, reals and rationals respectively. For any positive integer $n > 0$, $[n]$ denotes the set $\{1, 2, 3, \ldots, n\}$. Vectors will be denoted by small case and matrices and basis sets will be denoted in capital letters. Let $B = \{\vec{b_1}, \ldots, \vec{b_k}\}$ be a set of vectors in $\mathbb{R}^n$. The subspace of $\mathbb{R}^n$ spanned by B will be denoted by $\mathsf{span}(B)$. The norm of a vector $\vec{v} = [v_1, \ldots, v_n]$ is the normal Euclidean norm, i.e, $||\vec{v}|| = \sqrt{\sum_i v_i^2}$. The norm of B is defined as $||B|| = \max_{i \in [n]} ||\vec{b_i}||$. For any two sets of vectors U and V, $U + V$ will denote the set $\{\vec{u} + \vec{v} \mid \vec{u} \in U,\ \vec{v} \in V\}$.

2.2 Lattice

Definition 2.1 (Lattice) *Given a set of linearly independent vectors $B = \{\vec{b_1}, \ldots, \vec{b_m}\}$, the lattice spanned by B is the set $\mathcal{L}(B) = \{B \cdot \vec{z} \mid \forall \vec{z} \in \mathbb{Z}^m\}$.*

In other words, a lattice is an integral-span of B where B is called a *basis* of the lattice. The *rank* of the lattice is the number of independent vectors in the basis B and the dimension of a lattice is the dimension of the ambient space containing the lattice. We also represent B by a matrix in which the columns are vectors of B. In the matrix representation, rank of the lattice is the same as the rank of matrix B.

Similar to a vector space, a lattice contains infinitely many bases. If B and B' are two bases of the same lattice, then $B' = B \cdot U$ where U is a unimodular matrix.

Theorem 2.2 *Let B (in matrix form) be a basis of a rank-n lattice $\mathcal{L}$ in $\mathbb{R}^n$. Then B' is also a basis of $\mathcal{L}$ if and only if there exists an $n \times n$ unimodular matrix U such that $B' = B \cdot U$.*

Let $\vec{v}$ be an arbitrary vector. Then $\mathcal{L}(B)+\vec{v}$ denotes the shifted lattice $\{\sum_{i=1}^{n} z_i.\vec{b}_i + \vec{v} \mid \forall z_i \in \mathbb{Z}\}$. Observe that if $\vec{v}$ belongs to $\mathcal{L}(B)$, then $\mathcal{L}(B) + \vec{v} = \mathcal{L}(B)$.

A lattice $\mathcal{L}'$ is said to a sublattice of $\mathcal{L}$ if $\mathcal{L}' \subseteq \mathcal{L}$. Observe that the lattice denoted by $2\mathcal{L}(\vec{b}_1, \ldots, \vec{b}_n)$ which is $\{\sum_{i=1}^{n} 2z_i\vec{b}_i \mid z_i \in \mathbb{Z}\}$ is a sublattice of $\mathcal{L}(\vec{b}_1, \ldots, \vec{b}_n)$. Further, the shifted lattice $2\mathcal{L}(\vec{b}_1, \ldots, \vec{b}_n) + \vec{v}$ is a subset of $\mathcal{L}(\vec{b}_1, \ldots, \vec{b}_n)$ for any $\vec{v} \in \mathcal{L}(\vec{b}_1, \ldots, \vec{b}_n)$. For each $\vec{v} \in \mathcal{L}(\vec{b}_1, \ldots, \vec{b}_n)$, $2\mathcal{L}(\vec{b}_1, \ldots, \vec{b}_n) + \vec{v}$ is called a coset of $2\mathcal{L}(\vec{b}_1, \ldots, \vec{b}_n)$. Each vector of $\mathcal{L}(\vec{b}_1, \ldots, \vec{b}_n)$ belongs to either $2\mathcal{L}(\vec{b}_1, \ldots, \vec{b}_n)$ or to one of its cosets. Hence they partition the entire lattice.

Claim 2.3 *Let an $n \times n$ matrix B be a basis matrix of a lattice. Then there are 2^n distinct cosets of $2\mathcal{L}(B)$, given by $2\mathcal{L}(B) + B \cdot \vec{z}$ for all $\vec{z} \in \{0, 1\}^n$.*

Definition 2.4 (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*

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

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

Definition 2.6 (Shortest Vector Problem (SVP)) *Given a basis B, find a shortest non-zero vector $\vec{v}$ in the lattice $\mathcal{L}(B)$, i.e., $||\vec{v}|| \leq ||\vec{u}||$ for all $\vec{u} \in \mathcal{L}(B) \setminus \{\vec{0}\}$.*

Definition 2.7 (Closest Vector Problem (CVP)) *Given a basis B and a vector $\vec{t}$, find the vector $\vec{v}$ in the lattice $\mathcal{L}(B)$ which is closest from $\vec{t}$, i.e., $||\vec{v}-\vec{t}|| \leq ||\vec{u}-\vec{t}||$ for all $\vec{u} \in \mathcal{L}(B)$.*

Definition 2.8 (Shortest Basis Problem (SBP)) *Given a basis of a lattice $\mathcal{L}$, find a basis C of $\mathcal{L}$ such that $||C|| \leq ||D||$ for all bases D of $\mathcal{L}$.*

Definition 2.9 (Successive Minima) *The i^{th} successive minimum $\lambda_i(\mathcal{L})$ for a lattice $\mathcal{L}$ of rank n is the radius of the smallest sphere centered at the origin containing at least i independent lattice vectors.*

$$\lambda_i(\mathcal{L}) = inf\,\{r \mid dim(\mathsf{span}(\mathcal{L} \cap \mathcal{B}(0,r))) \geq i\}$$

where $\mathcal{B}(0,r)$ denotes the set of vectors with norm at most r.

A direct consequence of this definition is as follows.

Lemma 2.10 *Let $S = \{\vec{v}_1, \ldots, \vec{v}_k\}$ be a linearly independent set of vectors of a lattice $\mathcal{L}$. Then there exists a $\vec{v} \in S$ such that $||\vec{v}|| \geq \lambda_k$.*

A non-trivial relation between the norm of a shortest basis of a lattice and the λ_n of the lattice is given in lemma 2.11.

Lemma 2.11 (Corollary 7.2, [37]) *For any lattice $\mathcal{L}$, there exists a basis B such that $||B|| \leq \sqrt{n}\lambda_n/2$.*

Definition 2.12 (Successive Minima Problem (SMP)) *Given a basis B of a lattice, find linearly independent vectors $\vec{s}_1, \vec{s}_2, \ldots, \vec{s}_n$ such that $||\vec{s}_i|| = \lambda_i(\mathcal{L}(B))$ for all i.*

Definition 2.13 (Shortest Independent Vector Problem (SIVP)) *Given a basis B of a lattice, find n linearly independent vectors $\vec{s}_1, \ldots, \vec{s}_n$ such that $||\vec{s}_i|| \leq ||\vec{s}_{i+1}||$ for all i and $||\vec{s}_n|| = \lambda_n(\mathcal{L}(B))$.*

Observe that a solution to SMP is also a solution to SIVP.

Theorem 2.14 (Corollary 4, [2]) *There is a dimension and rank preserving reduction from* SMP *and* SIVP *to* CVP*. The reduction calls the* CVP *oracle* $\mathsf{poly}(n, b)$ *times where b is the number of input bits.*

Definition 2.15 (Shortest Vector Problem in Shifted Lattice (SVPS)) *Given a lattice basis $B = \{\vec{b_1}, \ldots, \vec{b_n}\}$ in the $\mathbb{R}^n$ space and $\vec{t} \in \mathbb{R}^n$, find a shortest vector $\vec{v}$ in the shifted lattice $\vec{t} + \mathcal{L}(B)$, i.e*

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

Observe that SVPS and CVP are equivalent problems because $\mathsf{CVP}(B, \vec{t}) = \vec{t} - \mathsf{SVPS}(B, \vec{t})$.

Definition 2.16 *Given a basis $B = \{\vec{b_1}, \ldots, \vec{b_k}\}$ of a subspace in $\mathbb{R}^n$, this subspace also has an orthogonal basis $B^* = \{\vec{b_1^*}, \ldots, \vec{b_k^*}\}$ given by $\vec{b_i}^* = \vec{b_i} - \sum_{j=1}^{i-1} \mu_{ij} \vec{b_j}^*$ where $\mu_{ij} = \vec{b_i}^T \cdot \vec{b_j}^* / (\vec{b_j}^*)^2$. This transformation of the basis is called* Gram Schmidt orthogonalization*.*

Definition 2.17 *Let $B = \{\vec{b_1}, \ldots, \vec{b_k}\}$ 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 $S =$ $\mathsf{span}(B)$ is its component in S. If B^* is an orthogonal basis of $\mathsf{span}(B)$ (such as the one computed by Gram Schmidt orthogonalization), then the projection of $\vec{v}$ on S is*

$$proj_S(\vec{v}) = \sum_{i=1}^{k} (\vec{v}^T \cdot \vec{b_i^*} / \vec{b_i^*}^2).\vec{b_i^*}.$$

The subspace orthogonal to S is given by $S^{\perp} = \{\vec{x} \in \mathbb{R}^n \mid v^t \cdot y = 0 \, \forall y \in S\}$. 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*

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

Definition 2.18 (Maximum Distance Sublattice Problem(MDSP)) *Given a basis* $\{\vec{v}, \vec{b_1}, \ldots, \vec{b_n}\}$ *for an* $n+1$ *dimensional lattice* $\mathcal{L}$*, find* $B' = \{\vec{b'_1}, \ldots, \vec{b'_n}\}$ *such that* $\{\vec{v}, \vec{b'_1}, \ldots, \vec{b'_n}\}$ *is also a basis for* $\mathcal{L}$ *and the distance* $dist(\vec{v}, \mathsf{span}(B'))$ *is maximum.* $\vec{v}$ *is called the* fixed vector.

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

Theorem 2.19 *There exist polynomial time reductions between* SVPS *and* MDSP*.*

Proof. We now show the trivial reduction between MDSP and SVPS. Let the input to MDSP be $B = [\vec{v}, \vec{b}_1, \ldots, \vec{b}_n]$ with $\vec{v}$ being the fixed vector and let its dual basis be $D = [\vec{u}, \vec{d}_1, \ldots, \vec{d}_n]$. In Theorem 3.1, we will show that a solution $B' = [\vec{v}, \vec{b}'_1, \ldots, \vec{b}'_n]$ to MDSP can be written as $B' = BU = [\vec{v}, \vec{b}_1 + \alpha_1\vec{v}, \ldots, \vec{b}_n + \alpha_n\vec{v}]$, i.e

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

where $\vec{\alpha}^T = [\alpha_1, \ldots, \alpha_n]$. From claim 2.5, we know that the dual basis D' of B' is $D(U^{-1})^T$ where

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

Therefore, $D' = [\vec{u} - \sum \alpha_i \vec{d_i}, \vec{d_1}, \ldots, \vec{d_n}]$. Also, from the definition of dual basis, we have $(D')^T B' = I$, therefore,

$$\vec{v}.\left(\vec{u} - \sum \alpha_i \vec{d_i}\right) = 1 \tag{2.1}$$

$$||\vec{v}||\ cos(\theta) = \frac{1}{||\vec{u} - \sum \alpha_i \vec{d_i}||} \tag{2.2}$$

where θ is the angle between $\vec{v}$ and $\vec{u} - \sum \alpha_i \vec{d_i}$. Again, from the definition of dual basis, we know that $\vec{u} - \sum \alpha_i \vec{d_i}$ is perpendicular to all $\vec{b'_i}$, therefore $\vec{u} - \sum \alpha_i \vec{d_i}$ is perpendicular to $\mathsf{span}(\vec{b'_1}, \ldots, \vec{b'_n})$. Therefore, $90 - \theta$ is the angle between $\vec{v}$ and

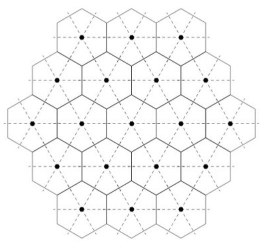

Figure 2.1: Voronoi cells

$\mathsf{span}(\vec{b}'_1, \ldots, \vec{b}'_n)$. Hence, $||\vec{v}||\ \sin(90-\theta)$ is the perpendicular distance between $\vec{v}$ and $\mathsf{span}(\vec{b}'_1, \ldots, \vec{b}'_n)$ which is maximized. Since, B' is the solution of MDSP, the term $||\vec{v}||\ sin(90-\theta)$ is maximized. Therefore, $||\vec{u} - \sum \alpha_i \vec{d}_i||$ is minimized due to (2.2) which is SVPS in the dual lattice. □

Definition 2.20 (Voronoi Cell) *Let $\mathcal{L}$ be a lattice. The Voronoi cell of the lattice is*

$$\mathcal{V}(\mathcal{L}) = \{\vec{x} \in \mathbb{R}^n \mid \forall \vec{v} \in \mathcal{L} \setminus \{0\}, ||\vec{x}|| < ||\vec{x} - \vec{v}||\}.$$

The halfspace for a non-zero lattice vector $\vec{v}$ is defined as

$$H(\vec{v}) = \{\vec{x} \in \mathbb{R}^n \mid ||\vec{x}|| < ||\vec{x} - \vec{v}||\}.$$

Observe that $\mathcal{V}(\mathcal{L}) = \bigcap\limits_{\vec{v} \in \mathcal{L} \setminus \{\vec{0}\}} H(\vec{v})$. In fact, there is a minimal set of lattice vectors called the set of Voronoi relevant vectors, denoted by $V(\mathcal{L})$, such that $\mathcal{V}(\mathcal{L}) = \bigcap\limits_{\vec{v} \in V(\mathcal{L})} H(\vec{v})$.

Theorem 2.21 (Voronoi, [38]) *Let $\mathcal{L}$ be a lattice and $\vec{v} \in \mathcal{L}$ be any lattice vector. Then $\vec{v}$ is a Voronoi relevant vector if and only if $\pm\vec{v}$ are the only shortest vectors in the coset $2\mathcal{L} + \vec{v}$.*

Corollary 2.22 *The number of Voronoi relevant vectors is upper bounded by $2(2^n - 1)$.*

Proof. According to Theorem 2.21 if coset has a unique (along with its negative) minimum vector, then that vector and its negative are Voronoi relevant vectors. Therefore the total number of Voronoi relevant vectors depends on the number of cosets of $2\mathcal{L}$, not including $2\mathcal{L}$ itself, because $\vec{0}$ is not a Voronoi relevant vector. So the number of Voronoi relevant vectors is at most $2(2^n - 1)$ (See Claim 2.3). $\square$

Chapter 3

New Reduction between MDSP and CVP

In this section, we present a new reduction between MDSP and CVP. Let $\{\vec{v}, \vec{b_1}, \ldots, \vec{b_n}\}$ be an input to the MDSP. Let us denote it by $[\vec{v} \mid B]$ where B denotes $\{\vec{b_1}, \ldots, \vec{b_n}\}$. 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 3.1 *Let $[\vec{v} \mid B]$ be a basis of an $n+1$ dimensional lattice $\mathcal{L}$ in $\mathbb{Z}^{n+1}$. Then for any lattice basis of the form $[\vec{v} \mid B'']$, there exists a basis $[\vec{v} \mid B']$ such that $\langle B'' \rangle = \langle B' \rangle$ and*

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

where $\alpha_i \in \mathbb{Z}$.

Proof. Since $[\vec{v} \mid B'']$ and $[\vec{v} \mid B]$ generate the same lattice, there exists a unimodular matrix U', see Theorem 2.2, such that

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

where U is given below. The determinant $det(U') = 1 \times det(U) = \pm 1$, so $det(U) = \pm 1$. Observe that $U' \in \mathbb{Z}^{n+1 \times n+1}$ which implies $U \in \mathbb{Z}^{n \times n}$ and it is unimodular.

Therefore, U^{-1} exists and it is also unimodular.

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

Let us denote vector $(\beta_1, \beta_2, \dots, \beta_n)$ by $\vec{\beta}^T$. Then

$$[v \mid B''] \begin{bmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & & & & & \\ \vdots & & & U^{-1} & & \\ 0 & & & & & \end{bmatrix} = [v \mid B] \cdot \begin{bmatrix} 1 & \vec{\beta}^T \\ 0 & \\ \vdots & U \\ 0 & \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & & & & & \\ \vdots & & & U^{-1} & & \\ 0 & & & & & \end{bmatrix}$$

$$= [\vec{v} \mid B] \cdot \begin{bmatrix} 1 & \vec{\beta}^T \cdot U^{-1} \\ 0 & \\ \vdots & UU^{-1} \\ 0 & \end{bmatrix}$$

$$= [\vec{v} \mid B] \cdot \begin{bmatrix} 1 & \vec{\beta}^T \cdot U^{-1} \\ 0 & \\ \vdots & I \\ 0 & \end{bmatrix}$$

$$= [\vec{v} \mid B] + [\vec{0} \mid \alpha_1 \vec{v}, \dots, \alpha_n \vec{v}]$$

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

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

Keeping Theorem 3.1 in consideration, the maximum distance sublattice problem can be stated as follows. Given an $(n + 1)$-dimensional lattice with basis

$\{\vec{v}, \vec{b_1}, \ldots, \vec{b_n}\}$. Compute a basis $\{\vec{v}, \vec{b_1} + j_1\vec{v}, \ldots, \vec{b_n} + j_n\vec{v}\}$ such that the distance of point $\vec{v}$ from the subspace spanned by $\{\vec{b_1} + j_1\vec{v}, \ldots, \vec{b_n} + j_n\vec{v}\}$ is maximum, where $j_i \in \mathbb{Z}\ \forall i$.

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

Lemma 3.2 *Let $\{\vec{v}, \vec{b_1}, \ldots, \vec{b_n}\}$ be an orthonormal basis of $\mathbb{R}^{n+1}$. Then the distance of point $\vec{v}$ from $P_{x_1,\ldots,x_n}$ is $1/\sqrt{1 + \sum_i x_i^2}$ 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. Then $\vec{w}^T.(\vec{b_i}+x_i\vec{v}) = 0$,$\forall i \in [n]$. These equations simplify to $c_i = -x_i.t$ where $t = \sum_j c_j x_j - 1$. The square of the distance of $\vec{v}$ from the plane is $\vec{w}^2 = \sum_i c_i^2 + (\sum_i c_i x_i - 1)^2 = \sum_i c_i^2 + t^2 = t^2(1 + \sum_i x_i^2)$.

We have $t = \sum_i x_i c_i - 1 = -t\sum_i x_i^2 - 1$. So $t = -1/(1 + \sum_i x_i^2)$. Plugging it in the expression for $\vec{w}^2$ we get $\vec{w}^2 = 1/(1 + \sum_i x_i^2)$. □

The distance from a plane is the projection on its orthogonal plane and projection is directly proportional to the length of the vector. Hence we have a trivial consequence.

Corollary 3.3 *Let $\{\vec{v}, \vec{b_1}, \ldots, \vec{b_n}\}$ be an orthogonal basis of $\mathbb{R}^{n+1}$ in which all but $\vec{v}$ are unit vectors. Then the distance of point $\vec{v}$ from $P_{x_1,\ldots,x_n}$ is $|\vec{v}|/\sqrt{1 + \sum_i x_i^2}$ for any $(x_1, \ldots, x_n) \in \mathbb{R}^n$.*

Consider an arbitrary basis $\{\vec{v}, \vec{b_1}, \ldots, \vec{b_n}\}$ of $\mathbb{R}^{n+1}$. 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 $\gamma_i = \vec{b_i}^T \cdot \vec{v}/\vec{v}^2$ 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. A lattice point $\vec{b_i} + j_i \cdot \vec{v}$ is the same 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, it is spanned by $\vec{b'_1} + (\gamma_1 + x_1)\vec{v}, \ldots, \vec{b'_n} + (\gamma_n + x_n)\vec{v}$.

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 $B'' = B' \cdot L$ 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. So $\vec{b''_i} = \sum_k L_{ki} \cdot \vec{b'_k}$. The new basis $\{\vec{b''_1}, \ldots, \vec{b''_n}\}$ spans the same subspaceas $\vec{b'_1}, \ldots, \vec{b'_n}$. Now $\{\vec{v}/|\vec{v}|, \vec{b''_1}, \ldots, \vec{b''_n}\}$ forms an orthonormal basis for the entire $\mathbb{R}^{n+1}$.

The plane $P_{x_1,\ldots,x_n}$ is spanned by $\vec{b'_1} + (\gamma_1 + x_1)\vec{v}, \ldots, \vec{b'_n} + (\gamma_n + x_n)\vec{v}$. If we extend a line parallel to $\vec{v}$ from the point $\vec{b''_i}$, 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.

We have $\vec{b''_i} + y_i\vec{v} = \sum_k L_{ki}(\vec{b'_k} + (\gamma_k + x_k)\vec{v}) - \sum_k L_{ki}(\gamma_k + x_k)\vec{v} + y_i\vec{v}$. By the choice of y_i, $\vec{b''_i} + y_i\vec{v}$ belongs to $P_{x_1,\ldots,x_n}$. 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. From the linear independence $-\sum_k L_{ki}(\gamma_k + x_k)\vec{v} + y_i\vec{v} = 0$. So $y_i = \sum_k L_{ki}(\gamma_k + x_k)$, i.e., $\vec{y} = L^T \cdot \vec{\gamma} + L^T \cdot \vec{x}$.

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 3.3, the square of the distance of $\vec{v}$ from the plane $P_{x_1,\ldots,x_n}$ is $|\vec{v}|^2/(1 + \sum_i y_i^2)$. 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 maximum. Equivalently we want to find a sublattice plane such that $\sum_i y_i^2$ $(= \vec{y}^2)$ is minimum, i.e., our goal is to minimize the length of the vector $\vec{y}$.

If $\vec{x} = \vec{j} \in \mathbb{Z}^n$, then corresponding $\vec{y} = L^T \cdot \vec{\gamma} + L^T \cdot \vec{j}$. Define a lattice $\mathcal{L}_1$ generated by the basis L^T, i.e., the row vectors of L are basis vectors. 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 the lattice point of $\mathcal{L}_1$ closest to the point $\vec{z}$. This is an instance of CVP where $\{\vec{r_1}, \ldots, \vec{r_n}\}$ is the lattice basis and $\vec{z}$ is the fixed point.

Lemma 3.4 *Given a lattice basis* $\{\vec{v}, \vec{b_1}, \ldots, \vec{b_n}\}$ *as an instance of* MDSP. *Let* $\vec{b'_i} = \vec{b_i} - \gamma_i\vec{v}$ *for all* $1 \leq i \leq n$ *where* $\gamma_i = \vec{b_i}^T \cdot \vec{v}/\vec{v}^2$. *Let* L *be a linear transformation* *such that $B'' = B' \cdot L$ is an orthonormal basis of $\mathbb{R}^{n+1}$. 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 the optimal lattice vertex 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 3.5 *Let the basis $\{\vec{s_1}, \ldots, \vec{s_n}\}$ and the fixed point $\vec{t} \in \mathbb{R}^n$ be an instance of* CVP*. L denotes the matrix in which i-th row is $\vec{s_i}$ for all $1 \leq i \leq n$. Define $\gamma = -(L^T)^{-1} \cdot \vec{t}$. 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 $\vec{e''_1}, \ldots, \vec{e''_n}$ and $B' = B'' \cdot L^{-1}$. The i-th column of B' is denoted by $\vec{e'_i}$. Let $\vec{e_i} = \vec{e'_i} + \gamma_i \vec{e_0}$. If $\{\vec{e_1} + j_1\vec{e_0}, \ldots, \vec{e_n} + j_n\vec{e_0}\}$ is a solution of* MDSP *instance $\{\vec{e_0}, \vec{e_1}, \ldots, \vec{e_n}\}$, then $\sum_i j_i \vec{s_i}$ is the solution of the given* CVP *instance.*

Thus we have the following theorem.

Theorem 3.6 *There is a polynomial time reduction between* MDSP *and* CVP*.*

Chapter 4

Successive Minima from Voronoi Relevant Vectors

In this section, we will show that all solutions to SMP is contained in the set of Voronoi relevant vectors. We also show that $\lambda_n(\mathcal{L})$ can be used to bound $||V(\mathcal{L})||$. We present a few interesting observations on $V(\mathcal{L})$ and show that the set of Voronoi relevent vectors generate the entire lattice. We start by proving some claims regarding the vectors in a solution to the SMP problem.

4.1 Relation between Solutions to SMP and Voronoi Relevant Vectors

Claim 4.1 *Let $S = \{\vec{s}_1, \ldots, \vec{s}_n\}$ be a solution to* SMP *of a lattice $\mathcal{L}$, i.e., S is a set of n linearly independent lattice vectors such that $||\vec{s}_i|| = \lambda_i(\mathcal{L})$. If $\vec{w} \in \mathcal{L}$, $||\vec{w}|| < \lambda_j$ and $\lambda_{j-1} < \lambda_j$, then $\vec{w} \in \mathsf{span}(\vec{s}_1, \ldots, \vec{s}_{j-1})$.*

Proof. Since, $\lambda_{j-1} < \lambda_j$, there are exactly $j-1$ linearly independent vectors whose norms are strictly less than λ_j. If $\vec{w} \notin \mathsf{span}(\vec{s}_1, \ldots, \vec{s}_{j-1})$, then $\vec{s}_1, \ldots, \vec{s}_{j-1}, \vec{w}$ are linearly independent. Since $\lambda_{j-1} < \lambda_j$, the norms of each of these j vectors is strictly less than λ_j. This contradicts Lemma 2.10. □

An obvious corollary of Claim 4.1 is as follows.

Corollary 4.2 *Let* $S = \{\vec{s}_1, \ldots, \vec{s}_n\}$ *and* $S' = \{\vec{s'}_1, \ldots, \vec{s'}_n\}$ *be any two solutions of* SMP. *If* $\lambda_i < \lambda_{i+1}$, *then* $\mathsf{span}(\vec{s}_1, \ldots, \vec{s}_i) = \mathsf{span}(\vec{s'}_1, \ldots, \vec{s'}_i)$.

We will show in the main result of this chapter that if $S = \{\vec{s}_1, \vec{s}_2, \ldots, \vec{s}_n\}$ is a solution to SMP, then S will be contained in the set of Voronoi relevant vectors of the lattice. From theorem 2.21, if $\vec{v} \in \mathcal{L}$ is not a Voronoi relevant vector, then there exist $\vec{w} \in \mathcal{L} \setminus \{0, \vec{v}\}$ such that $||\vec{v}/2 - \vec{w}|| \leq ||\vec{v}/2||$. We will use this criterion to prove this result.

(Remarks: We first show that all the shortest vectors of $\mathcal{L}$ are Voronoi relevant.) If $\vec{s}_1$ is not Voronoi relevant, then applying above criterion for $\vec{v} = \vec{s}_1$, we consider two cases.

- $\left|\left|\frac{\vec{s}_1}{2} - \vec{w}\right|\right| < \left|\left|\frac{\vec{s}_1}{2}\right|\right|$: In this case $||\vec{s}_1 - 2\vec{w}|| < ||\vec{s}_1||$ which is a contradiction because $\vec{s}_1$ is the shortest vector in $\mathcal{L}$.

- $\left|\left|\frac{\vec{s}_1}{2} - \vec{w}\right|\right| = \left|\left|\frac{\vec{s}_1}{2}\right|\right|$: It implies that $cos(\theta) = ||\vec{w}||/||\vec{s}_1||$ where θ is the angle between $\vec{s}_1$ and $\vec{w}$. Since $||\vec{w}|| \geq ||\vec{s}_1||$, we have $cos(\theta) \geq 1$. Therefore $\theta = 0$ and $\vec{w} = \vec{s}_1$, which contradicts the way $\vec{w}$ was chosen.

This implies that $\vec{s}_1 \in V(\mathcal{L})$. Now to argue using induction assume that $\vec{s}_1, \ldots, \vec{s}_{i-1}$ belong to $V(\mathcal{L})$ and $\vec{s}_i \notin V(\mathcal{L})$, for some i. Again we consider two cases based on the criterion.

- $||\vec{s}_i - 2\vec{w}|| < ||\vec{s}_i||$: From the Claim 4.1 $\vec{s}_i - 2\vec{w}$ belongs to $X = \mathsf{span}(\vec{s}_1, \ldots, \vec{s}_{i-1})$. Due to triangular inequality, we have $||\vec{w}|| = ||\vec{w} - \vec{s}_i/2 + \vec{s}_i/2|| < ||\vec{s}_i||$. So $\vec{w} \in X$. Combining the two facts we get that $\vec{s}_i$ also belongs to X. But that is impossible because $||\vec{s}_i|| = \lambda_i$.

- $||\vec{s}_i - 2\vec{w}|| = ||\vec{s}_i||$: This implies that $||\vec{w}||^2 = \vec{s}_i.\vec{w} \implies cos(\theta) = ||\vec{w}||/||\vec{s}_i||$.

  If $\theta = 0$ then $\vec{w} = \vec{s}_i$ which contradicts the fact that $\vec{w} \notin \{0, \vec{v} = \vec{s}_i\}$. So, we consider the case when $||\vec{s}_i|| > ||\vec{w}||$. In this case w belongs to

$X = \mathsf{span}(\vec{s}_1, \ldots, \vec{s}_{i-1})$. We get an inequality as follows.

$$\begin{aligned} ||\vec{s}_i - \vec{w}||^2 &= ||\vec{s}_i||^2 + ||\vec{w}||^2 - 2\vec{s}_i.\vec{w} \\ &= ||\vec{s}_i||^2 + ||\vec{w}||^2 - 2||\vec{w}||^2 \\ &= ||\vec{s}_i||^2 - ||\vec{w}||^2 \\ &< ||\vec{s}_i||^2 \end{aligned}$$

This implies that $\vec{s}_i - \vec{w}$ also belongs to X. Thus we deduce that $\vec{s}_i$ must also belong to X, which is absurd because $||\vec{s}_i|| = \lambda_i$.

Therefore, we have the following theorem.

Theorem 4.3 *If $S = \{\vec{s}_i, \ldots, \vec{s}_n\}$ is a solution to* SMP *for a lattice $\mathcal{L}$, then $S \subseteq V(\mathcal{L})$.*

Corollary 4.4 *For any lattice $\mathcal{L}$*

$$\lambda_n(\mathcal{L}) \leq ||V(\mathcal{L})|| \leq \frac{n^{3/2}}{2}\lambda_n(\mathcal{L})$$

.

Proof. The lower bound is obvious due to Theorem 4.3. Let B be a shortest basis of $\mathcal{L}$. Using Lemma 2.11, we know that $||B|| \leq \sqrt{n}\lambda_n(\mathcal{L})/2$. Also, the norm of the shortest vector in the coset $2\mathcal{L} + \vec{v}$, where $\vec{v} \in \mathcal{L}$, is at most $||\vec{v}||$. We know that all possible cosets are given by $2\mathcal{L} + B\vec{z}$ where $\vec{z} \in \{0,1\}^n$. Therefore, the norm of the shortest vector in $2\mathcal{L} + B\vec{z}$, for any $\vec{z}$, is at most $n.||B||$. Thus $||V(\mathcal{L})|| \leq n^{3/2}\lambda_n(\mathcal{L})/2$. □

The algorithm given by Micciancio et al. [1] computes all the Voronoi relevant vectors, then Algorithm 1 computes a solution of SMP.

Let us now prove the correctness of the algorithm.

Theorem 4.5 *Algorithm 1 computes a solution of* SMP.

Input: A basis $B = [\vec{b}_1, \ldots, \vec{b}_n]$ for $\mathcal{L}$.
Run the algorithm given by Micciancio et al. to compute the set of all Voronoi relevant vector V;
Sort V in the order of non-decreasing norm;
$S := \{\}$;
$i = 1$;
while $|S| < n$ **do**
    if $V[i] \notin \mathsf{span}(S)$ **then**
        $S = S \cup \{V[i]\}$;
    end
end
Return S.

Algorithm 1: Algorithm for solving SMP

Proof. From Theorem 4.3 we know that the list of Voronoi relevant vectors contain all the solutions of SMP. It is obvious that the algorithm will compute n linearly independent lattice vectors. Let the sorted sequence of the vectors of $V(\mathcal{L})$ be $\{\vec{v}_1, \vec{v}_2, \ldots\}$. Let $\{\vec{v}_{j_1}, \ldots, \vec{v}_{j_n}\}$ be any arbitrary solution of SMP in the increasing order of norm. Suppose the algorithm computes the set $S = \{\vec{v}_{i_1}, \ldots, \vec{v}_{i_n}\}$ where $i_1 < i_2 < \ldots i_n$. Next we will show that $i_p \leq j_p$.

Assume that $i_p > j_p$. So we have $i_q \leq j_p < i_{q+1}$ for some $q < p$. From the algorithm we know that each of the vectors $\vec{v}_{j_1}, \vec{v}_{j_2}, \ldots, \vec{v}_{j_p}$ can be spanned by $\{\vec{v}_{i_1}, \ldots, \vec{v}_{i_q}\}$. So $\mathsf{span}(\vec{v}_{j_1}, \ldots, \vec{v}_{j_p}) \subseteq \mathsf{span}(\vec{v}_{i_1}, \ldots, \vec{v}_{i_q})$. Thus $p \leq q$, which is a contradiction!

From Lemma 2.10 $||\vec{v}_{i_p}|| \geq \lambda_p$ for all p. Also from the above result $||\vec{v}_{i_p}|| \leq ||\vec{v}_{j_p}|| = \lambda_p$ for all p. Hence $||\vec{v}_{i_p}|| = \lambda_p$ for all p. □

As the number of Voronoi relevant vectors is at most $2(2^n - 1)$, see Corollary 2.22, the sorting would take time $\tilde{O}(2^n)$. The number of iterations in the while loop is $O(2^n)$ and in each iteration, the amount of time required to check whether a vector is to be included in the set S is polynomial. Therefore, the entire running time of the algorithm is $\tilde{O}(2^{2n})$ because this is also the time complexity of Micciancio's algorithm to compute $V(\mathcal{L})$.

It is easy to see that Algorithm 1 computes a solution of SMP because set V is the set of all Voronoi relevant vectors and it contains every solution to SMP.

Corollary 4.6 *Let V be any set of lattice vectors that contains all vectors with norm λ_i for all i. Then Algorithm 1 computes a solution of* SMP *on input V.*

4.2 More Observations on $V(\mathcal{L})$

In this section we give some facts which bring more light into the relationship between Voronoi relevant vectors and the vectors belonging to some SMP solution. We begin with two examples.

Following lattice has a vector with norm λ_3 but it does not belong to any SMP solution. It also does not belong to $V(\mathcal{L})$. The basis of the lattice is

$$B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \sqrt{2} \end{bmatrix}$$

Observe that $[1,1,0]^T$ is a lattice vector with norm equal to $\lambda_3 = \sqrt{2}$ but does not form a part of any solution to SMP.

Next example shows a vector that belongs to $V(\mathcal{L})$ while its norm is not equal to λ_i for any i. Consider the lattice $\mathcal{L}$ spanned by the basis.

$$B = \begin{bmatrix} 1 & 5 \\ 5 & 1 \end{bmatrix}$$

In this case, $V(\mathcal{L}) = \{\pm[1,5]^T, \pm[5,1]^T, \pm[-4,4]^T\}$ whereas $\lambda_1 = \lambda_2 = \sqrt{26}$ while $||[-4,4]^T|| = \sqrt{32} > \lambda_2$.

Following is a consequence of Corollary 4.6 and Theorem 4.3.

Corollary 4.7 *Let $\vec{v} \in \mathcal{L}$ such that $||\vec{v}|| = \lambda_i$ for some i and $\vec{v} \notin \mathsf{span}(\{\vec{x} \mid ||\vec{x}|| < \lambda_i\}$. Then $\vec{v}$ belongs to at least one solution of* SMP*. Consequently $\vec{v}$ also belongs to $V(\mathcal{L})$.*

Proof. We prove this claim by constructing an SMP solution which contains $\vec{v}$. Without loss of generality, we can assume that $\lambda_{i-1} < \lambda_i$. This is because there will always exist an index j such that $\lambda_j < \lambda_i$ and $\lambda_k = \lambda_i, \forall k \in \{j+1, \ldots, i-1\}$. Therefore, we can assume that $i = j+1$ and the conditions in the theorem are still satisfied.

From Corollary 4.6, if V is ordered in such a way that the first vector with norm equal to λ_i is $\vec{v}$, then the algorithm will pick $\vec{v}$ as the i^{th} vector. Therefore, $\vec{v}$ will be a part of some solution to SMP. □

Above proof describes a class of vectors which belong to at least one SMP solution and hence belong to $V(\mathcal{L})$. The next result identifies a class of short vectors which do not belong to any SMP solution.

Lemma 4.8 *Let $\vec{v}$ be a lattice vector with $||\vec{v}|| = \lambda_i$ for some i. Let j be an index with $\lambda_j < \lambda_i$ and $\vec{v} \in \mathsf{span}(\{\vec{x} \mid ||\vec{x}|| \leq \lambda_j\})$. Then $\vec{v}$ does not belong to any* SMP *solution.*

Proof. Define $Q = \{\vec{v}' \in \mathcal{L} \mid ||\vec{v}'|| \leq \lambda_j\}$. Then $dim(\mathsf{span}(Q)) \geq j$. Without loss of generality we assume that $j = dim(\mathsf{span}(Q))$, i.e., j is the largest index with norm λ_j.

Assume that there is an SMP solution $X = \{\vec{s}_1, \vec{s}_2, \ldots, \vec{s}_n\}$, where $||\vec{s}_k|| = \lambda_k \forall k$ and which contains $\vec{v}$. Then $\{\vec{s}_1, \ldots, \vec{s}_j\}$ is a basis of the space $\mathsf{span}(Q)$. We are given that $\vec{v}$ belongs to $\mathsf{span}(Q)$ and it also belongs X so $\vec{v} \in \{\vec{s}_1, \ldots, \vec{s}_j\}$. Thus $\lambda_i = ||\vec{v}|| \leq ||\vec{s}_j|| = \lambda_j$. This contradicts the fact that $\lambda_i > \lambda_j$.

Thus $\vec{v}$ cannot belong to any SMP solution. . □

These two results give a complete characterization of vectors that belong to at least one SMP solution..

Theorem 4.9 *A lattice vector $\vec{v}$ belongs to at least one* SMP *solution if and only if $||\vec{v}|| = \lambda_i$ for some i and it does not belong to $\mathsf{span}(\{\vec{v}' \mid ||\vec{v}'|| < \lambda_i\})$.*

We now show that the set of Voronoi relevant vector $V(\mathcal{L})$ can generate $\mathcal{L}$, i.e $\mathcal{L} = \{\sum_i \vec{v}_i z_i \mid \vec{v}_i \in V(\mathcal{L}), z_i \in \mathbb{Z}\}$.

Definition 4.10 *The closed Voronoi cell of a lattice $\mathcal{L}$ is*

$$\overline{\mathcal{V}}(\mathcal{L}) = \{\vec{x} \in \mathbb{R}^n | \forall \vec{v} \in \mathcal{L}, ||\vec{x}|| \leq ||\vec{x} - \vec{v}||\}$$

Observe that all Voronoi relevant vectors are on the boundary of $2\overline{\mathcal{V}}(\mathcal{L})$.

Theorem 4.11 ([39]) *Any $\vec{v} \in \mathcal{L}$ on the boundary of $2\overline{\mathcal{V}}(\mathcal{L})$ can be written as sum of mutually orthogonal Voronoi relevant vectors.*

From theorem 4.11, it can be shown that the set $M = 2\overline{\mathcal{V}}(\mathcal{L}) \cap \mathcal{L}$ generates $\mathcal{L}$. We prove this using the following two claims.

Claim 4.12 *Any non-zero lattice vector $\vec{v}$ lies on the boundary of $2i\overline{\mathcal{V}}(\mathcal{L})$ for some $i \in \mathbb{Z}$.*

Proof. We prove this using induction. For base case, we know that the only lattice vector in $2\mathcal{V}(\mathcal{L})$ is 0 and there exists lattice vectors on the boundary of $2\overline{\mathcal{V}}(\mathcal{L})$. Assume that the claim is true till some $i-1 \in \mathbb{Z}$ and there exists a vector $\vec{v} \in \mathcal{L} \setminus \{0\}$ such that $\vec{v} \in 2i\mathcal{V}(\mathcal{L}) \setminus 2(i-1)\overline{\mathcal{V}}(\mathcal{L})$. This implies that there exists $\vec{w} \in 2(i-1)\overline{\mathcal{V}}(\mathcal{L}) \cap \mathcal{L}$ such that $\vec{v} \in \vec{w} + 2\mathcal{V}$ which is a contradiction because $\vec{w} + 2\mathcal{V}(\mathcal{L})$ contains only one lattice vector which is $\vec{w}$. □

Claim 4.13 *M can generate all vectors in $2i\overline{\mathcal{V}}(\mathcal{L}) \cap \mathcal{L}$ where $i \in \mathbb{Z}$.*

Proof. We prove using induction. Observe that claim is true for $i = 1$ because of the definition of M.
Assume it is true for some $i - 1 \in \mathbb{Z}$. It is easy to see that $2i\overline{\mathcal{V}}(\mathcal{L}) \cap \mathcal{L} = \big(2(i-1)\overline{\mathcal{V}}(\mathcal{L}) \cap \mathcal{L}\big) + M$. By induction hypothesis, vectors in $2(i-1)\overline{\mathcal{V}}(\mathcal{L}) \cap \mathcal{L}$ can be generated by M, therefore $2i\overline{\mathcal{V}}(\mathcal{L}) \cap \mathcal{L}$ can also be generated by M. □

Theorem 4.14 *The set of Voronoi relevant vectors $V(\mathcal{L})$ generates $\mathcal{L}$.*

Proof. We will prove this result using induction on the norm of the vectors of $\mathcal{L}$. Clearly every vector of $V(\mathcal{L})$ belongs to the integer-span of $V(\mathcal{L})$.

Suppose $\vec{v} \in \mathcal{L}$. Induction hypothesis is that all vectors with norm strictly less than $||\vec{v}||$ belong to the integer span of $V(\mathcal{L})$.

The line segment L, from the origin to the lattice point v being the vector $\vec{v}$, the length of the line segment is $||\vec{v}||$. Suppose this line segment intersects the surface of the polytope $\overline{\mathcal{V}}(v)$ (the closed Voronoi cell of lattice point v) at a point p. This point can be either on a facet or a lower dimensional face, F. So F is the intersection of one of more facets. Let one of these facets be F' and it is the border between v and another lattice point u. Then the origin and u must be on the same side of the hyper-plane corresponding to the facet F'. Let point x be the mid-point of the line segment $\overline{uv}$ and let $\vec{d} = \vec{v} - \vec{u}$. Then x is on the hyper-plane corresponding to F' and $\vec{x} \cdot \vec{d} > 0$.

We have $\vec{u} = \vec{x} - \vec{d}/2$ and $\vec{v} = \vec{x} + \vec{d}/2$. So $||\vec{v}||^2 = ||\vec{x}||^2 + ||\vec{d}||^2/4 + \vec{x} \cdot \vec{d} = ||\vec{u}||^2 - 2 \cdot \vec{x} \cdot \vec{d}$. So $||\vec{u}||^2 < ||\vec{v}||^2$. From induction hypothesis $\vec{u}$ belongs to the integer span of $V(\mathcal{L})$. Besides, $\vec{d} = \vec{v} - \vec{u} \in V(\mathcal{L})$. Hence $\vec{v} = \vec{u} + \vec{d}$ also belongs to the integer span of $V(\mathcal{L})$. □

Chapter 5

Conclusions

In this thesis, we give an alternate reduction between Closest Vector Problem (CVP) and Maximum Distance Sublattice Problem (MDSP). We also show some interesting relationship between the solutions to SMP and Voronoi relevant vectors.

5.1 Scope for Further Work

The $\mathbb{Z}^n$ isomorphism problem asks whether a given lattice $\mathcal{L}$ is a rotation of $\mathbb{Z}^n$ or not. A trivial solution to this problem is to find the shortest vectors and check whether these vectors are mutually orthogonal unit vectors or not. Since we can solve SVP using a CVP oracle, one direction of research would be to find better algorithms for CVP in such special lattices.

References

[1] Daniele Micciancio and Panagiotis Voulgaris. “A deterministic single exponential time algorithm for most lattice problems based on Voronoi cell computations”. In: *SIAM Journal on Computing* 42.3 (2013), pp. 1364–1391.

[2] Daniele Micciancio. “Efficient reductions among lattice problems”. In: *Proceedings of the nineteenth annual ACM-SIAM symposium on Discrete algorithms*. Society for Industrial and Applied Mathematics. 2008, pp. 84–93.

[3] Craig Gentry. “Fully homomorphic encryption using ideal lattices”. In: *Proceedings of the forty-first annual ACM symposium on Theory of computing*. 2009, pp. 169–178.

[4] Shweta Agrawal, David Mandell Freeman, and Vinod Vaikuntanathan. “Functional encryption for inner product predicates from learning with errors”. In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2011, pp. 21–40.

[5] Jin-Yi Cai and Ajay 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)*. IEEE. 1998, pp. 46–55.

[6] Ishay Haviv and Oded 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*. ACM. 2007, pp. 469–477.

[7] Subhash Khot. “Hardness of approximating the shortest vector problem in lattices”. In: *Journal of the ACM (JACM)* 52.5 (2005), pp. 789–808.

[8] Miklós Ajtai. “The Shortest Vector Problem in L2 is NP-hard for Randomized Reductions (Extended Abstract)”. In: *STOC*. 1998.

[9] Sanjeev Arora et al. “The hardness of approximate optima in lattices, codes, and systems of linear equations”. In: *Journal of Computer and System Sciences* 54.2 (1997), pp. 317–331.

[10] Daniele Micciancio. “The shortest vector in a lattice is hard to approximate to within some constant”. In: *SIAM journal on Computing* 30.6 (2001), pp. 2008–2035.

[11] Irit Dinur, Guy Kindler, and Shmuel Safra. “Approximating-CVP to within almost-polynomial factors is NP-hard”. In: *Foundations of Computer Science, 1998. Proceedings. 39th Annual Symposium on*. IEEE. 1998, pp. 99–109.

[12] Huck Bennett, Alexander Golovnev, and Noah Stephens-Davidowitz. "On the quantitative hardness of CVP". In: *FOCS*. 2017. URL: http://arxiv.org/abs/1704.03928.

[13] Divesh Aggarwal et al. "Fine-grained hardness of CVP(P)— Everything that we can prove (and nothing else)". In: *SODA*. 2021. URL: http://arxiv.org/abs/1911.02440.

[14] Divesh Aggarwal and Noah Stephens-Davidowitz. "(Gap/S)ETH Hardness of SVP". In: *STOC*. 2018. URL: http://arxiv.org/abs/1712.00942.

[15] Oded Goldreich et al. "Approximating shortest lattice vectors is not harder than approximating closest lattice vectors". In: *Information Processing Letters* 71.2 (1999), pp. 55–61.

[16] Divesh Aggarwal et al. "Dimension-preserving reductions between SVP and CVP in different p-norms". In: *SODA*. 2021. URL: http://arxiv.org/abs/2104.06576.

[17] Ravi Kannan. "Minkowski's convex body theorem and integer programming". In: *Mathematics of operations research* 12.3 (1987), pp. 415–440.

[18] Guillaume Hanrot and Damien Stehlé. "Improved analysis of Kannan's shortest lattice vector algorithm". In: *Annual International Cryptology Conference*. Springer. 2007, pp. 170–186.

[19] Daniele Micciancio and Michael Walter. "Fast lattice point enumeration with minimal overhead". In: *Proceedings of the twenty-sixth annual ACM-SIAM symposium on Discrete algorithms*. SIAM. 2014, pp. 276–294.

[20] Miklós Ajtai, Ravi Kumar, and Dandapani Sivakumar. "A sieve algorithm for the shortest lattice vector problem". In: *Proceedings of the thirty-third annual ACM symposium on Theory of computing*. ACM. 2001, pp. 601–610.

[21] Miklós Ajtai, Ravi Kumar, and Dandapani Sivakumar. "Sampling short lattice vectors and the closest lattice vector problem". In: *Proceedings 17th IEEE Annual Conference on Computational Complexity*. IEEE. 2002, pp. 53–57.

[22] Vikraman Arvind and Pushkar 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.

[23] Johannes Blömer and Stefanie Naewe. "Sampling methods for shortest vectors, closest vectors and successive minima". In: *Theoretical Computer Science* 410.18 (2009), pp. 1648–1665.

[24] Guillaume Hanrot, Xavier Pujol, and Damien Stehlé. "Algorithms for the shortest and closest lattice vector problems". In: *International Conference on Coding and Cryptology*. Springer. 2011, pp. 159–190.

[25] Xavier Pujol and Damien Stehlé. "Solving the Shortest Lattice Vector Problem in Time 22.465 n." In: *IACR Cryptology ePrint Archive* 2009 (2009), p. 605.

[26] Phong Q Nguyen and Thomas Vidick. "Sieve algorithms for the shortest vector problem are practical". In: *Journal of Mathematical Cryptology* 2.2 (2008), pp. 181–207.

[27] Daniele Micciancio and Panagiotis Voulgaris. “Faster exponential time algorithms for the shortest vector problem”. In: *Proceedings of the twenty-first annual ACM-SIAM symposium on Discrete Algorithms*. Society for Industrial and Applied Mathematics. 2010, pp. 1468–1480.

[28] Divesh Aggarwal, Daniel Dadush, and Noah Stephens-Davidowitz. “Solving the Closest Vector Problem in 2^ n Time–The Discrete Gaussian Strikes Again!” In: *2015 IEEE 56th Annual Symposium on Foundations of Computer Science*. IEEE. 2015, pp. 563–582.

[29] Divesh Aggarwal et al. “Solving the shortest vector problem in 2 n time using discrete Gaussian sampling”. In: *Proceedings of the forty-seventh annual ACM symposium on Theory of computing*. ACM. 2015, pp. 733–742.

[30] Arjen Klaas Lenstra, Hendrik Willem Lenstra, and László Lovász. “Factoring polynomials with rational coefficients”. In: *Mathematische Annalen* 261.4 (1982), pp. 515–534.

[31] Don Coppersmith. “Finding a small root of a univariate modular equation”. In: *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 1996, pp. 155–165.

[32] Don 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*. Springer. 1996, pp. 178–189.

[33] Adi Shamir. “A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem”. In: *Foundations of Computer Science, 1982. SFCS’08. 23rd Annual Symposium on*. IEEE. 1982, pp. 145–152.

[34] László Babai. “On Lovász’lattice reduction and the nearest lattice point problem”. In: *Combinatorica* 6.1 (1986), pp. 1–13.

[35] Claus-Peter Schnorr and Martin Euchner. “Lattice basis reduction: Improved practical algorithms and solving subset sum problems”. In: *Mathematical programming* 66.1-3 (1994), pp. 181–199.

[36] Claus-Peter Schnorr. “A hierarchy of polynomial time lattice basis reduction algorithms”. In: *Theoretical computer science* 53.2-3 (1987), pp. 201–224.

[37] Daniele Micciancio and Shafi Goldwasser. *Complexity of lattice problems: a cryptographic perspective*. Vol. 671. Springer Science & Business Media, 2012.

[38] John Horton Conway and Neil James Alexander Sloane. *Sphere packings, lattices and groups*. Vol. 290. Springer Science & Business Media, 2013.

[39] Akos G Horváth. “On the Dirichlet—Voronoi cell of unimodular lattices”. In: *Geometriae Dedicata* 63.2 (1996), pp. 183–191.

[40] Ravi Kannan. “Improved algorithms for integer programming and related lattice problems”. In: *Proceedings of the fifteenth annual ACM symposium on Theory of computing*. ACM. 1983, pp. 193–206.

[41] Xiaoyun Wang et al. “Improved Nguyen-Vidick heuristic sieve algorithm for shortest vector problem”. In: *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*. ACM. 2011, pp. 1–9.

[42] Divesh Aggarwal et al. “Solving the shortest vector problem in 2n time via discrete Gaussian sampling. arXiv preprint”. In: *arXiv* 1412 (2014).