INTERNATIONAL JOUNAL OF: SCIENCE RESEARCH AND TECHNOLOGY

TIMBOU-AFRICA ACADEMIC PUBLICATIONS
INTERNATIONAL JOURNAL, NOVEMBER, 2022 EDITIONS
VOL. 11 NO. 9 ISSN: 2623-7861

THE SHORTEST VECTOR PROBLEM: LATTICE BASED APPROACH.

ALIYU DANLADI HINA; MOHAMMED AUWAL ABDULLAHI; USMAN HASSAN

Department of Mathematics & Statistics, The Federal Polytechnic, Bauchi.

ABSTRACT

Abstract: In the field of cryptography, more especially quantum cryptography, lattices have become an indispensable tool. They are widely used as countermeasures during quantum attacks in lattice based cryptography. One of the significant problem in quantum cryptography is the shortest vector problem (SVP). This is the problem of finding the shortest vector in a lattice, which is NP-hard under randomized reductions as

INTRODUCTION

A lattice L of dimension *n* can be defined as the set of all integer linear combinations of *n* linearly independent basis vectors $\mathbf{V} = [\vec{v}_1, \vec{v}_2, \cdots, \vec{v}_n] \in \mathbb{R}^{m \times n}$ where each $\vec{v}_i \in \mathbb{R}^m$. There are many famous algorithmic problems on point lattices, the most important of which are:

- The shortest vector problem (SVP): Given a basis **V**, find a shortest nonzero vector in the lattice generated by **V**.
- The closest vector problem (CVP): Given a basis **V** and a target vector $\vec{u} \in \mathbb{R}^m$, find a lattice vector generated by **V** that is closest to $\vec{u}$.

SVP and CVP have been extensively studied both as purely mathematical problems, being central in the study of the geometry of numbers (Cassels, 2012) and as algorithmic problems, having numerous applications in communication theory (Conway & Sloane, 2013) and computer science. SVP and CVP have been used to solve major algorithmic problems in combinatorial optimization (integer programming (Lenstra Jr, 1983; Kannan, 1987), solving low density subset-sum problems (Coster et al., 1992), algorithmic number theory and geometry of numbers (factoring polynomials over the rationals (Lenstra, Lenstra, & Lova´sz, 1982), checking the solvability by radicals (Landau & Miller, 1983),

proven by Ajtai. With the assumption of the hardness of SVP, many cryptosystems are presumed secure. A new algorithm is proposed in this paper to solve the SVP in polynomial time. We show that the Hemite factor of the proposed algorithm is polynomially baunded.

Keywords: Cryptography, lattices, lattice based cryptography, randomized reductions, quantum cryptography

and cryptanalysis (breaking the Merkle-Hellman cryptosystem (Odlyzko, 1990).

These problems form the basis of the security of lattice-based cryptography, which is a prime candidate for the NIST post-quantum cryptography standardization. The security of lattice-based cryptosystems in postquantum cryptography is mainly based on the difficulty of solving the shortest vector problem (SVP) or the closest vector problem (CVP) (Satılmı¸s & Akleylek, 2020).

There has been interesting development in the development of algorithms for SVP and CVP (Yasuda, 2021). In 1987, Kannan gave a deterministic algorithm that solves *n*dimensional SVP and CVP in $n^{O(n)} = 2^{O(n \ ogn)}$ time and $po\ y(n)$ space (Kannan, 1987). Ajtai, Kumar, and Sivakumar (AKS) gave a randomized “sieve” algorithm that solves SVP and $CVP1_{+}$ (for any constant > 0) in singly exponential $2^{O(n)}$ time and space (Ajtai, Kumar, & Sivakumar, 2002). In 2010, Micciancio and Voulgaris (MV) gave a deterministic algorithm that solves CVP (and hence SVP and other problems) in $2^{O(n)}$ time and space (Micciancio & Voulgaris, 2010).

A genetic algorithm aiming at searching the shortest vector of the random lattices from the SVP is proposed by (Ding, Zhu, & Wang, 2015). There approach has attracted numerous attention in cryptography. An algorithm to solve the approximate Shortest Vector Problem for lattices corresponding to ideals of the ring of integers of an arbitrary number field **F** was considered by (Pellet-Mary, Hanrot, & Stehl´e, 2019). There method includes a pre-processing phase which depends only on **F**. The pre-processing phase outputs an advice, whose bit-size is no more than the run-time of the query phase.

The implementation of of GaussSieve and ProGaussSieve algorithms were adopted to solve the shortest vector problem in(Satılmı¸s & Akleylek, 2020). Inspired by quantum annealing, (Yamaguchi et al., 2022) propose methods for generating an Ising model and solving the Ising model on annealing computers with a bit representation as the input, which represents encodings to map each integer variable in the SVP into binary variables. A comprehensive survey on solving the SVP can be found in (Yasuda, 2021; Asif, 2021; Biasse, Bonnetain, Kirshanova, Schrottenloher, & Song, 2022).

Preliminaries

Lattices

A lattice is a regular arrangement of points in n-dimensional Euclidean space. The set of points can be described by using a set of *n* linearly independent vectors, $\vec{v}_1, \vec{v}_2, \cdots, \vec{v}_n$, such that $\vec{v}_i \in \mathbb{R}^m$. A lattice is formally defined as the set of all integer combinations of those *n* linearly independent vectors. These linearly independent vectors $\mathbf{V} = \{\vec{v}_1, \vec{v}_2, \cdots, \vec{v}_n\}$ are known as the basis of lattice. The lattice L can be represented as

$$\mathcal{L}(\mathbf{V}) = \left\{ \sum_{i=1}^{n} \alpha_i \vec{v}_i \mid \alpha_i \in Z \right\} \quad (1)$$

One will see that equation (1) shows that L is the integer combinations of the *n* linearly independent vectors of the basis $^{\mathrm{R}n}$. We should however note that, the lattice is not the vector space spanned by the basis, but rather the set of all combinations that has an integer coe cients. This therefore makes a lattice to be a discrete set. Thus, points in a lattice cannot be too close to each other, since the distance between points are represented by integer values. There is a minimum distance between points in each lattice, where the minimum distance *d* of points in a lattice is *d* > 0 (Micciancio, 2011).

The simplest example of a lattice is the set of all *n*-dimensional vectors with integer entries $\mathbf{Z}^n$.

The set of vectors $\{\vec{v}_1, \vec{v}_2, \cdots, \vec{v}_n\} \in \mathbb{Z}^m$ is called the basis for the lattice. This basis can be expressed as $\mathbf{V} = \{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n\} \in \mathbb{Z}^{m \times n}$. This basis can be expresed in matrix form as:

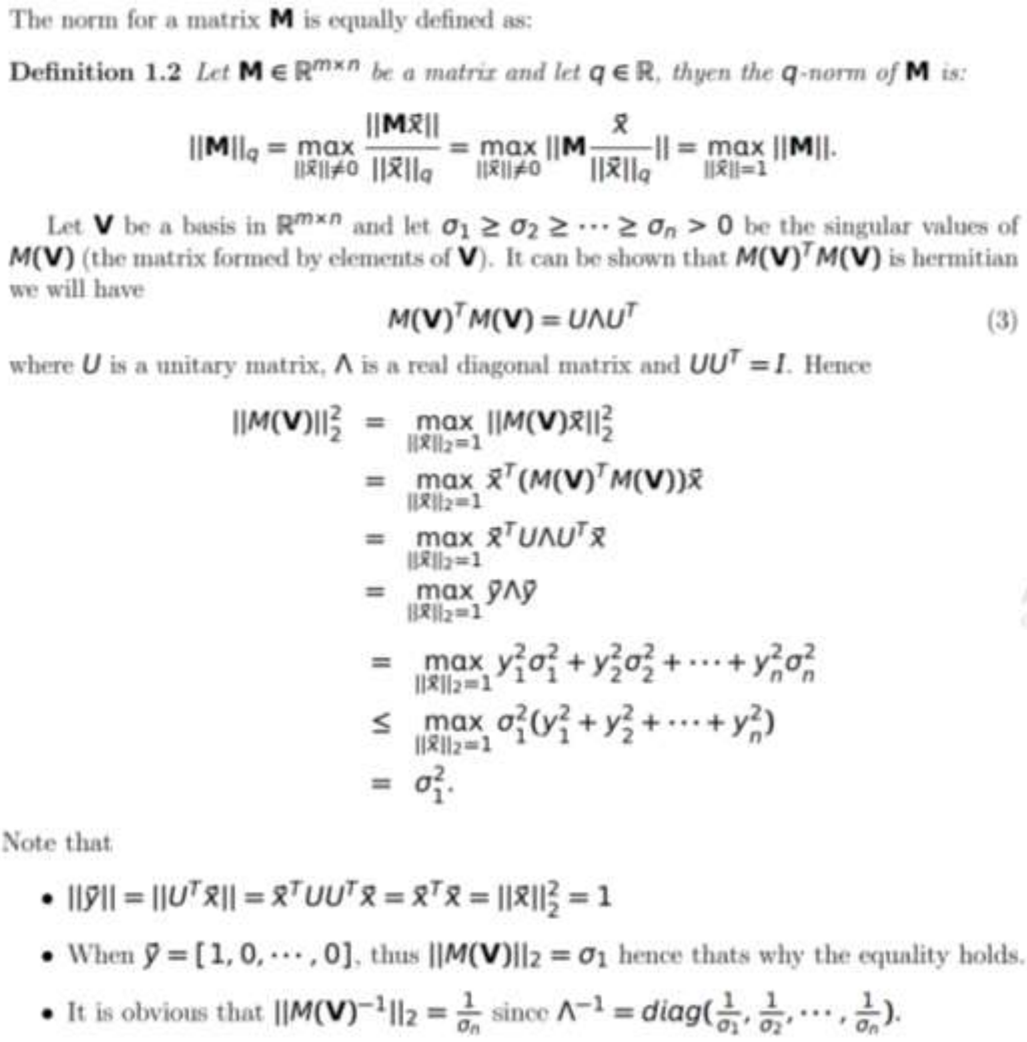
$$M(\mathbf{V}) = [\,\vec{v}_1\ \vec{v}_2\ \ldots\ \vec{v}_n\,] \quad (2)$$

where each $\vec{v}_i$ is a collumn vector of dimension $(m \times 1)$.

Normed Spaces

Definition 1.1 *Let $\vec{v} = (v_1, v_2, \cdots, v_n)$ be a vector in $\mathbb{R}^n$ and $q \in \mathbb{R}$ then the q norm and the infinity norm of the vector are respectively defined thus:*

$$||\vec{v}||_q = \sqrt{v_1^q + v_2^q + \cdots + v_n^q}, \qquad ||\vec{x}||_\infty = \max_i \{|x_i| \mid i = 1, 2, \cdots, n\}.$$



The norm for a matrix $\mathbf{M}$ is equally defined as:

Definition 1.2 *Let* $\mathbf{M} \in \mathbb{R}^{m\times n}$ *be a matrix and let* $q \in \mathbb{R}$*, thyen the* q*-norm of* $\mathbf{M}$ *is:*

$$||\mathbf{M}||_q = \max_{||\bar{x}||\neq 0} \frac{||\mathbf{M}\bar{x}||}{||\bar{x}||_q} = \max_{||\bar{x}||\neq 0} ||\mathbf{M}\frac{\bar{x}}{||\bar{x}||_q}|| = \max_{||\bar{x}||=1} ||\mathbf{M}||.$$

Let $\mathbf{V}$ be a basis in $\mathbb{R}^{m\times n}$ and let $\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_n > 0$ be the singular values of $M(\mathbf{V})$ (the matrix formed by elements of $\mathbf{V}$). It can be shown that $M(\mathbf{V})^T M(\mathbf{V})$ is hermitian we will have

$$M(\mathbf{V})^T M(\mathbf{V}) = U\Lambda U^T \tag{3}$$

where U is a unitary matrix, Λ is a real diagonal matrix and $UU^T = I$. Hence

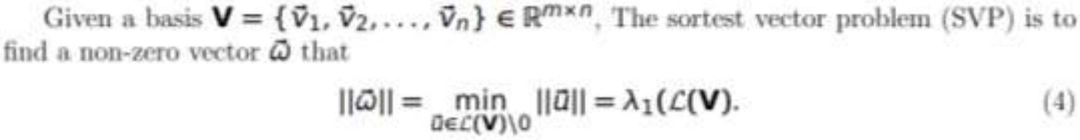
$$\begin{aligned} ||M(\mathbf{V})||_2^2 &= \max_{||\bar{x}||_2=1} ||M(\mathbf{V})\bar{x}||_2^2 \\ &= \max_{||\bar{x}||_2=1} \bar{x}^T(M(\mathbf{V})^T M(\mathbf{V}))\bar{x} \\ &= \max_{||\bar{x}||_2=1} \bar{x}^T U\Lambda U^T \bar{x} \\ &= \max_{||\bar{x}||_2=1} \bar{y}\Lambda\bar{y} \\ &= \max_{||\bar{x}||_2=1} y_1^2\sigma_1^2 + y_2^2\sigma_2^2 + \cdots + y_n^2\sigma_n^2 \\ &\leq \max_{||\bar{x}||_2=1} \sigma_1^2(y_1^2 + y_2^2 + \cdots + y_n^2) \\ &= \sigma_1^2. \end{aligned}$$

Note that

- $||\bar{y}|| = ||U^T\bar{x}|| = \bar{x}^T UU^T\bar{x} = \bar{x}^T\bar{x} = ||\bar{x}||_2^2 = 1$
- When $\bar{y} = [1, 0, \cdots, 0]$, thus $||M(\mathbf{V})||_2 = \sigma_1$ hence thats why the equality holds.
- It is obvious that $||M(\mathbf{V})^{-1}||_2 = \frac{1}{\sigma_n}$ since $\Lambda^{-1} = diag(\frac{1}{\sigma_1}, \frac{1}{\sigma_2}, \cdots, \frac{1}{\sigma_n})$.

The Shortest Vector Problem

The shortest vector problem (SVP) asks to find a nonzero vector in a lattice. The problem can be defined with respect to any norm, but the Euclidean norm is the most common. In the approximation version of SVP, the goal is to find a nonzero lattice vector of length at most g times the length of the optimal solution, where the approximation factor g is usually a function of the lattice dimension.

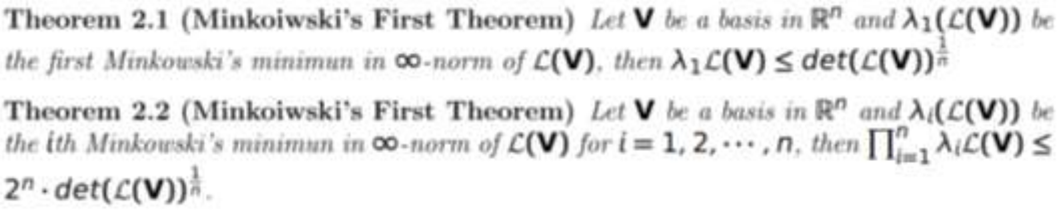


Given a basis $\mathbf{V} = \{\bar{v}_1, \bar{v}_2, \ldots, \bar{v}_n\} \in \mathbb{R}^{m\times n}$, The sortest vector problem (SVP) is to find a non-zero vector $\bar{\omega}$ that

$$||\bar{\omega}|| = \min_{\bar{u}\in\mathcal{L}(\mathbf{V})\backslash 0} ||\bar{u}|| = \lambda_1(\mathcal{L}(\mathbf{V})). \tag{4}$$

In (Ajtai, 1996), it has been proven that the SVP is a NP-hard under the randomized reductions. To date, there has not been a polynomial time algorithm to verify wether a vector is the solution of an SVP problem. However, to test for the solution, one will use the Minkowski's theorem or the Hermite factor.

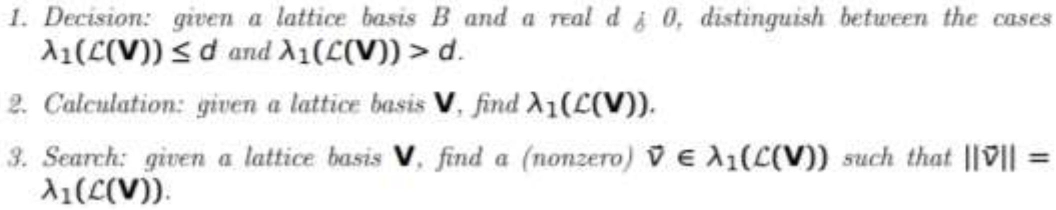
Minkowski Theorem



Theorem 2.1 (Minkoiwski's First Theorem) *Let* $\mathbf{V}$ *be a basis in* $\mathbb{R}^n$ *and* $\lambda_1(\mathcal{L}(\mathbf{V}))$ *be the first Minkowski's minimun in* ∞*-norm of* $\mathcal{L}(\mathbf{V})$*, then* $\lambda_1\mathcal{L}(\mathbf{V}) \leq det(\mathcal{L}(\mathbf{V}))^{\frac{1}{n}}$

Theorem 2.2 (Minkoiwski's First Theorem) *Let* $\mathbf{V}$ *be a basis in* $\mathbb{R}^n$ *and* $\lambda_i(\mathcal{L}(\mathbf{V}))$ *be the ith Minkowski's minimun in* ∞*-norm of* $\mathcal{L}(\mathbf{V})$ *for* $i = 1, 2, \cdots, n$*, then* $\prod_{i=1}^{n} \lambda_i\mathcal{L}(\mathbf{V}) \leq 2^n \cdot det(\mathcal{L}(\mathbf{V}))^{\frac{1}{n}}$.

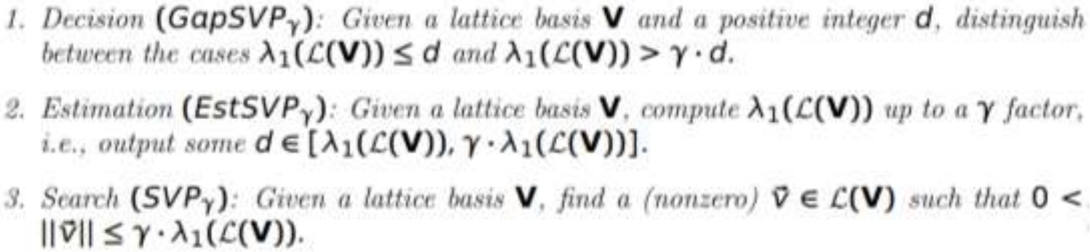
Definition 2.1 (Shortest Vector Problem, Exact Form.) *The exact form of SVP has three common variants, which we restrict to integer lattices (and so integral bases) without loss of generality:*



1. *Decision: given a lattice basis B and a real d ¿ 0, distinguish between the cases* $\lambda_1(\mathcal{L}(\mathbf{V})) \leq d$ *and* $\lambda_1(\mathcal{L}(\mathbf{V})) > d$.
2. *Calculation: given a lattice basis* $\mathbf{V}$*, find* $\lambda_1(\mathcal{L}(\mathbf{V}))$.
3. *Search: given a lattice basis* $\mathbf{V}$*, find a (nonzero)* $\vec{v} \in \lambda_1(\mathcal{L}(\mathbf{V}))$ *such that* $||\vec{v}|| = \lambda_1(\mathcal{L}(\mathbf{V}))$.

The approximate version of the SVP is also of great interest and wide applicabilition.

Definition 2.2 (Approximate SVP.) *The -approximate Shortest Vector Problem, where* = (*n*) 1 *is a function of the dimension n, has the following variants (again restricted to integer lattices):*



1. *Decision* $(GapSVP_\gamma)$*: Given a lattice basis* $\mathbf{V}$ *and a positive integer* d*, distinguish between the cases* $\lambda_1(\mathcal{L}(\mathbf{V})) \leq d$ *and* $\lambda_1(\mathcal{L}(\mathbf{V})) > \gamma \cdot d$.
2. *Estimation* $(EstSVP_\gamma)$*: Given a lattice basis* $\mathbf{V}$*, compute* $\lambda_1(\mathcal{L}(\mathbf{V}))$ *up to a* γ *factor, i.e., output some* $d \in [\lambda_1(\mathcal{L}(\mathbf{V})), \gamma \cdot \lambda_1(\mathcal{L}(\mathbf{V}))]$.
3. *Search* (SVP_γ)*: Given a lattice basis* $\mathbf{V}$*, find a (nonzero)* $\vec{v} \in \mathcal{L}(\mathbf{V})$ *such that* $0 < ||\vec{v}|| \leq \gamma \cdot \lambda_1(\mathcal{L}(\mathbf{V}))$.

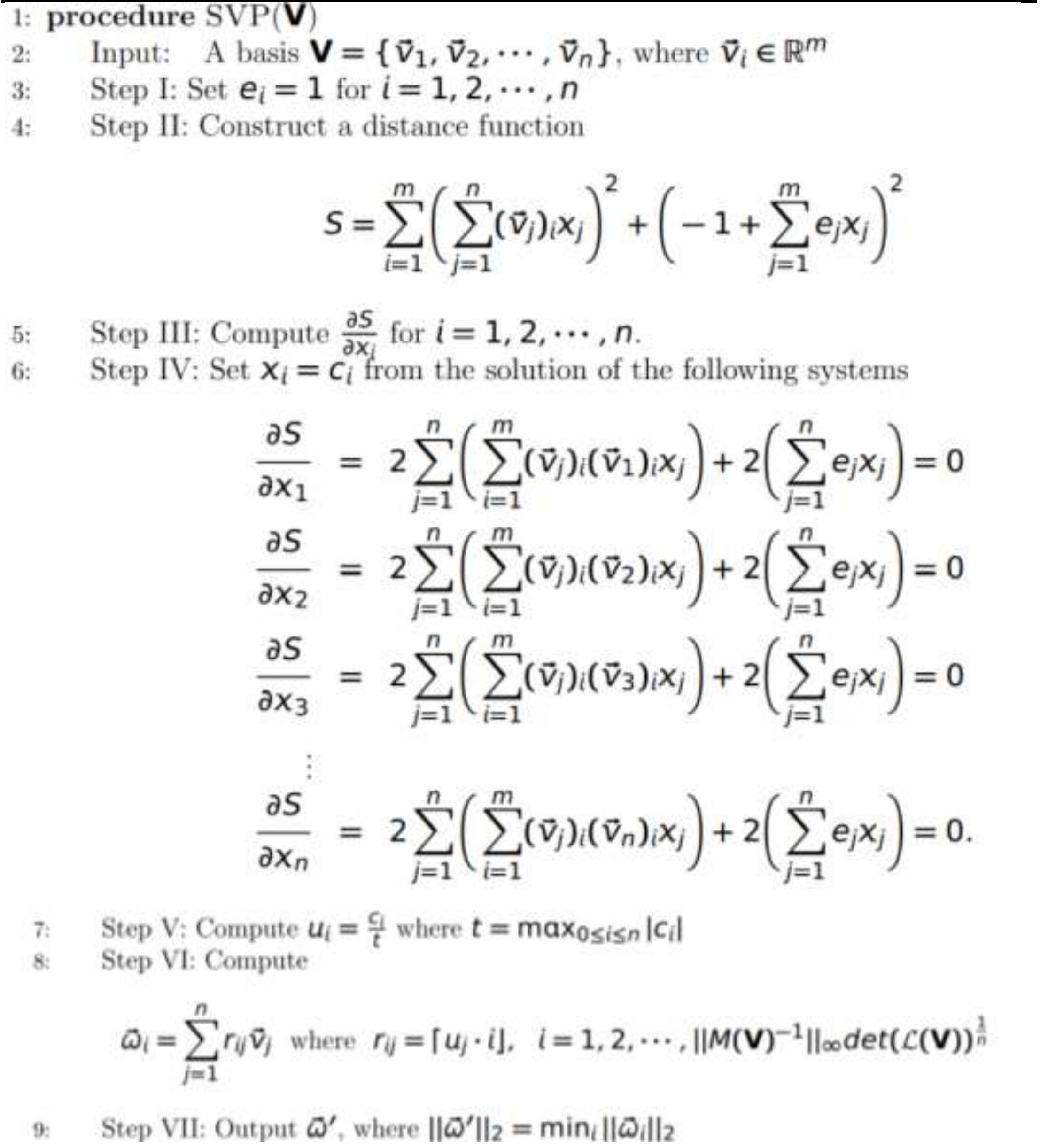
Note that the approximation becomes the exact version with = 1.

The Proposed Algorithm

In this section we propose an algorithm that will compute the shortest vector problem (SVP). We initialize by adding some noise $e_i = 1$ to each of the vectors. For some c_i to be computed, $\sum_{i=1}^{n} c_i e_i \approx 1$.

The Algorithm

Algorithm 1 Shotest Vector Problem



```
procedure SVP($\mathbf{V}$)
    Input: A basis $\mathbf{V} = \{\vec{v}_1, \vec{v}_2, \cdots, \vec{v}_n\}$, where $\vec{v}_i \in \mathbb{R}^m$
    Step I: Set $e_i = 1$ for $i = 1, 2, \cdots, n$
    Step II: Construct a distance function
        $$S = \sum_{i=1}^{m}\Big(\sum_{j=1}^{n}(\vec{v}_j)_i x_j\Big)^2 + \Big(-1 + \sum_{j=1}^{m} e_j x_j\Big)^2$$
    Step III: Compute $\frac{\partial S}{\partial x_i}$ for $i = 1, 2, \cdots, n$.
    Step IV: Set $x_i = c_i$ from the solution of the following systems
        $$\frac{\partial S}{\partial x_1} = 2\sum_{j=1}^{n}\Big(\sum_{i=1}^{m}(\vec{v}_j)_i(\vec{v}_1)_i x_j\Big) + 2\Big(\sum_{j=1}^{n} e_j x_j\Big) = 0$$
        $$\frac{\partial S}{\partial x_2} = 2\sum_{j=1}^{n}\Big(\sum_{i=1}^{m}(\vec{v}_j)_i(\vec{v}_2)_i x_j\Big) + 2\Big(\sum_{j=1}^{n} e_j x_j\Big) = 0$$
        $$\frac{\partial S}{\partial x_3} = 2\sum_{j=1}^{n}\Big(\sum_{i=1}^{m}(\vec{v}_j)_i(\vec{v}_3)_i x_j\Big) + 2\Big(\sum_{j=1}^{n} e_j x_j\Big) = 0$$
        $\vdots$
        $$\frac{\partial S}{\partial x_n} = 2\sum_{j=1}^{n}\Big(\sum_{i=1}^{m}(\vec{v}_j)_i(\vec{v}_n)_i x_j\Big) + 2\Big(\sum_{j=1}^{n} e_j x_j\Big) = 0.$$
    Step V: Compute $u_i = \frac{c_i}{t}$ where $t = max_{0 \le i \le n}|c_i|$
    Step VI: Compute
        $$\vec{\omega}_i = \sum_{j=1}^{n} r_{ij}\vec{v}_j \text{ where } r_{ij} = \lceil u_j \cdot i \rfloor, \quad i = 1, 2, \cdots, ||M(\mathbf{V})^{-1}||_\infty det(\mathcal{L}(\mathbf{V}))^{\frac{1}{n}}$$
    Step VII: Output $\vec{\omega}'$, where $||\vec{\omega}'||_2 = min_i ||\vec{\omega}_i||_2$
```

If we consider the distance function in Step II:

$$S = \sum_{i=1}^{m}\Big(\sum_{j=1}^{n}(\vec{v}_j)_i x_j\Big)^2 + \Big(-1 + \sum_{j=1}^{m} e_j x_j\Big)^2$$

Let $\vec{v}'_t = [\vec{v}_t, e_t]$ for $t = 1, 2, \cdots, n$. Then the corresponding partial derivative for $i = t$ will be (Step III):

$$\begin{aligned}
\frac{\partial S}{\partial x_t} &= \sum_{i=1}^{m} 2\Big(\sum_{j=1}^{n} (\vec{v}_j)_i) x_j\Big) \cdot (\vec{v}_t)_i + 2\Big(-1 + \sum_{j=1}^{n} e_j x_j\Big) \cdot e_t \\
&= 2\sum_{j=1}^{n}\Big(\sum_{i=1}^{m} (\vec{v}_j)_i (\vec{v}_t)_i x_j\Big) + 2\Big(\sum_{j=1}^{n} e_j e_t x_j\Big) - 2e_t \\
&= 2\Big[\sum_{j=1}^{n}\Big(\sum_{i=1}^{m} (\vec{v}_j)_i (\vec{v}_t)_i + e_j e_t\Big) x_j - e_t\Big] \\
&= 2\Big[\sum_{j=1}^{n} (\vec{v}'_j, \vec{v}'_t) x_j - e_t\Big]
\end{aligned}$$

Now each component of the matrix $M = [a_{ij}]$ where $a_{ij} = \langle \vec{v}_i, \vec{v}_j \rangle + e_i e_j$ can be computed by performing the inner product $\langle \vec{v}'_j, \vec{v}'_t \rangle$.

We have in the algorithm that $\vec{\omega} = \sum_{i=1}^{n} f_i \vec{v}_i$ is the shortest vector in $\mathcal{L}(\mathbf{V})$ where f_i is the coefficient of the vector $\vec{v}_i$. The vector $\vec{f} = [f_1, f_2, f_3, \cdots, f_n]$ which can be expressed as

$$\vec{f} = \Big[\vec{v}_1 \,\Big|\, \vec{v}_2 \,\Big|\, \vec{v}_3 \,\Big|\, \cdots \,\Big|\, \vec{v}_n\Big]^{-1} \begin{bmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{bmatrix}. \tag{5}$$

Taking the norm

$$\begin{aligned}
||\vec{f}||_\infty &= ||M(\mathbf{V})^{-1}\vec{\omega}||_\infty \\
&\leq ||M(\mathbf{V})^{-1}||_\infty ||\vec{\omega}||_\infty \\
&\leq ||M(\mathbf{V})^{-1}||_\infty \cdot det\Big(\mathcal{L}(\mathbf{V})\Big)^{\frac{1}{n}}.
\end{aligned}$$

which gives the upper bound of the coefficient vector $\vec{f}$ using the Minkowski's first theorem $||\vec{\omega}||_\infty \leq det\Big(\mathcal{L}(\mathbf{V})\Big)^{\frac{1}{n}}$.

Correctness of the Algorithm

In the proposed algorithm presented above, we now test its correctness. Let $\vec{\omega}' = \sum_{i=1}^{n} u_i k \vec{v}_i$ and $\vec{F} = \sum_{i=1}^{n} f_i \vec{v}_i$ be the shortest vector of $\mathcal{L}(\mathbf{V})$ for some vector $\vec{f} = [f_i]_n$. We claim that there exist a constant k such that for all i,

$$|u_i \cdot k - f_i| \leq \eta = \frac{\sigma_1}{\sigma_n}\sqrt{n}.$$

where σ_1 and σ_n are respectively, the maximum and minimum singular values of $M(\mathbf{V})$.

Let

$$k = \frac{\sum_{i=1}^{n} f_i}{\sum_{i=1}^{n} u_i}, \quad \text{and} \quad r_i = u_i \cdot k. \tag{6}$$

thus, $\sum_{i=1}^{n} r_i - \sum_{i=1}^{n} f_i = 0$. Let

$$\sum_{i=1}^{n} r_i\vec{v}_i - \sum_{i=1}^{n} f_i\vec{v}_i = \sum_{i=1}^{n} z_i\vec{v}_i, \quad \text{where} \quad z_i = r_i - vf_i. \qquad (7)$$

Hence,

$$\begin{aligned} \sum_{i=1}^{n} z_i\vec{v}_i &= \sum_{i=1}^{n} r_i - \sum_{i=1}^{n} f_i = \sum_{i=1}^{n} u_i \cdot k \\ &= \frac{\sum_{i=1}^{n} f_i}{\sum_{i=1}^{n} u_i} \sum_{i=1}^{n} u_i - \sum_{i=1}^{n} f_i \\ &= 0. \end{aligned}$$

We have seen from the algorithm that some ratios of $(c_1, c_2, \cdots, c_n)$ can be found such that $|ku_i - f_i| < \eta$ for some k, from whichnthe shortest vector is $\bar{\omega} = \sum_{i=1}^{n} f_i\vec{v}_i$.

Let the equare roots of the eigenvalues of $M(\mathbf{V})^T M(\mathbf{V})$ be $\sigma_1 \geq \sigma_2 \geq \sigma_3 \geq \cdots \geq \sigma_n \geq 0$, the following holds:

$$\sigma_1 \leq \sigma_1 \left(\frac{\sigma_1}{\sigma_n}\frac{\sigma_2}{\sigma_n}\frac{\sigma_3}{\sigma_n}\cdots\frac{\sigma_n}{\sigma_n}\right)^{\frac{1}{n}} \leq \frac{\sigma_1}{\sigma_n} det\left(\mathcal{L}(\mathbf{V})\right)^{\frac{1}{n}}$$

Therefore;

$$\begin{aligned} \left\|\bar{\omega} + \sum_{i=1}^{n}(ku_i - f_i)\bar{v}_i\right\|_2 &\leq \|\bar{\omega}\|_2 + \left\|\sum_{i=1}^{n}(ku_i - f_i)\bar{v}_i\right\|_2 \\ &\leq \sqrt{n} \cdot det\left(\mathcal{L}(\mathbf{V})\right)^{\frac{1}{n}} + \|M(\mathbf{V})\|_2 \left\|\sum_{i=1}^{n}(ku_i - f_i)\right\|_2 \\ &\leq \sqrt{n} \cdot det\left(\mathcal{L}(\mathbf{V})\right)^{\frac{1}{n}} + \sigma_1\left(\frac{\sigma_1}{\sigma_n}\right)n \\ &\leq \sqrt{n} \cdot det\left(\mathcal{L}(\mathbf{V})\right)^{\frac{1}{n}} + n\left(\frac{\sigma_1}{\sigma_n}\right)^2 det\left(\mathcal{L}(\mathbf{V})\right)^{\frac{1}{n}} \\ &= \left(\sqrt{n} + n\left(\frac{\sigma_1}{\sigma_n}\right)^2\right) det\left(\mathcal{L}(\mathbf{V})\right)^{\frac{1}{n}}. \end{aligned}$$

Space Complexity

The proposed algorithm has the space complexity of $O(n^2)$. This implies that it needs n^2 numbers to store $M(\mathbf{V})$, the basis in matris form, and needs n numbers to store the initial valu of $e - i,\ i = 1, 2, \cdots, n.$. The system $\frac{\partial S}{\partial x_i}$ generated from $M(\mathbf{V})^T M(\mathbf{V})$ has space complexity of $O(n^2)$. The vector $\vec{u}$ will require n numbers to be stored whereas the vector $\vec{\omega}$ will require $2n$ numbers to be stored.. Totally the space requirements for the algorithm is thus: $n^2 + n + n^2 + n + 2n = 2n^2 + 4n$ numbers.

Conclusion

An algorithm for the approximate computation of SVP which uses the Hermite factor of at-most $(\sqrt{n}+(\frac{a_1}{a_n})^2 n)$ is proposed. It was shown that the length of the vector $\sum_{i=1}^{n} c_i\vec{v}_i$ has a minimum value provided that $\sum_{i=1}^{n} c_i \approx 1$ for some non-zero critical point $(c_1, c_2, \cdots, c_n)$.

References

Ajtai, M. (1996). Generating hard instances of lattice problems. In *Proceedings of the twenty-eighth annual acm symposium on theory of computing* (pp. 99–108).

Ajtai, M., Kumar, R., & Sivakumar, D. (2002). Sampling short lattice vectors and the closest lattice vector problem. In *Proceedings 17th ieee annual conference on computational complexity* (pp. 53–57).

Asif, R. (2021). Post-quantum cryptosystems for internet-of-things: a survey on lattice-based algorithms. *IoT*, 2(1), 71–91.

Biasse, J.-F., Bonnetain, X., Kirshanova, E., Schrottenloher, A., & Song, F. (2022). Quantum algorithms for attacking hardness assumptions in classical and post-quantum cryptography. *IET Information Security*.

Cassels, J. W. S. (2012). *An introduction to the geometry of numbers*. Springer Science & Business Media.

Conway, J. H., & Sloane, N. J. A. (2013). *Sphere packings, lattices and groups* (Vol. 290). Springer Science & Business Media.

Coster, M. J., Joux, A., LaMacchia, B. A., Odlyzko, A. M., Schnorr, C.-P., & Stern, J. (1992). Improved low-density subset sum algorithms. *Computational complexity*, 2(2), 111–128.

Ding, D., Zhu, G., & Wang, X. (2015). A genetic algorithm for searching the shortest lattice vector of svp challenge. In *Proceedings of the 2015 annual conference on genetic and evolutionary computation* (pp. 823–830).

Kannan, R. (1987). Minkowski's convex body theorem and integer programming. *Mathematics of operations research*, 12(3), 415–440.

Landau, S., & Miller, G. L. (1983). Solvability by radicals is in polynomial time. In *Proceedings of the fifteenth annual acm symposium on theory of computing* (pp. 140– 151).

Lenstra, A. K., Lenstra, H. W., & Lov´asz, L. (1982). Factoring polynomials with rational coefficients. *Mathematische annalen*, 261(ARTICLE), 515–534.

Lenstra Jr, H. W. (1983). Integer programming with a fixed number of variables. *Mathematics of operations research*, 8(4), 538–548.

Micciancio, D. (2011). The geometry of lattice cryptography. In *International school on foundations of security analysis and design* (pp. 185–210).

Micciancio, D., & Voulgaris, P. (2010). A deterministic single exponential time algorithm for most lattice problems based on voronoi cell computations. In *Proceedings of the forty-second acm symposium on theory of computing* (pp. 351–358).

Odlyzko, A. M. (1990). The rise and fall of knapsack cryptosystems. *Cryptology and computational number theory*, 42(2).

Pellet-Mary, A., Hanrot, G., & Stehl´e, D. (2019). Approx-svp in ideal lattices with preprocessing. In *Annual international conference on the theory and applications of cryptographic techniques* (pp. 685–716).

Satılmı¸s, H., & Akleylek, S. (2020). Efficient implementations of gauss-based sieving algorithms. In *2020 28th signal processing and communications applications conference (siu)* (pp. 1–4).

Yamaguchi, J., Shimizu, T., Furukawa, K., Ohori, R., Shimoyama, T., Mandal, A., ... Takuya, O. (2022). Annealing-based algorithm for solving cvp and svp. *Journal of the Operations Research Society of Japan*, 65(3), 121–137.

Yasuda, M. (2021). A survey of solving svp algorithms and recent strategies for solving the svp challenge. In *International symposium on mathematics, quantum theory, and cryptography* (pp. 189–207).