An Introduction to Lenstra-Lenstra-Lovasz Lattice Basis Reduction Algorithm

Xinyue Deng

77 Massachusetts Avenue

Cambridge, MA, 02139

Massachusetts Institute of Technology

Abstract

Lenstra-Lenstra-Lovasz (LLL) Algorithm is an approximation algorithm of the shortest vector problem, which runs in polynomial time and finds an approximation within an exponential factor of the correct answer. It is a practical method with enough accuracy in solving integer linear programming, factorizing polynomials over integers and breaking cryptosystems. In this paper, we introduce its background and implementation, analyze its correctness and performance and discuss its applications.

Keywords: LLL-algorithm, Lattice basis reduction

1. Introduction

A lattice is formed by all linear combinations with integer coefficients of the subgroup of any basis in $\mathbb{R}^n$, as formulated in Definition 1.1.

Definition 1.1 (Lattice)**.** A lattice $\mathcal{L}$ is a discrete subgroup of H generated by all the integer combinations of the vectors of some basis B :

$$\mathcal{L} = \sum_{i=1}^{m} \mathbb{Z}\mathbf{b_i} = \left\{ \sum_{i=1}^{m} z_i \mathbf{b_i}, \text{where } z_i \in \mathbb{Z}, \mathbf{b_i} \in B \right\}.$$

Lattices have many significant applications in mathematics, and cryptography. The Shortest vector problem (SVP) is the most famous and widely studied lattice problem, which consists in finding the shortest nonzero vector, $\lambda(\mathcal{L})$ in a given lattice $\mathcal{L}$. The length of the vector can be defined with any norm, but most frequently with Euclidean norm. Another variant of SVP is finding the length of the shortest non-zero vector without finding the vector.

SVP has been studied since 19th century due to its connectivity with many problems, like integer linear programming and number theory. The average hardness of SVP made it also an attractive topic in cryptography. In 1910s, mathematician Minowski proved an upper bound of SVP in n-dimensions, which is stated in Theorem 1.1.

Theorem 1.1 (Minowski's Theorem). *Any convex, centrally symmetric body S of volume $vol(S) > 2^n det(\mathcal{L})$ contains a non-zero lattice point. $det(\mathcal{L})$ is the determinant of a lattice $\mathcal{L}$.*

Proof. Let $S' = S/2$, and we have $vol(S') > det(\mathcal{L})$. We claim that there are distinct points $\mathbf{x}, \mathbf{y} \in S'$, such that $x - y \in \mathcal{L}$. To see this, we need to introduce the definition of fundamental region.

Definition 1.2 (Foundamental Region). A set $\mathcal{F} \subseteq \mathbb{R}^n$ of a lattice $\mathcal{F}$ if its translation $\mathbf{x} + \mathcal{F} = \{\mathbf{x} + \mathbf{y} : \mathbf{y} \in \mathcal{F}\}$, taken over all $\mathbf{x} \in \mathcal{L}$, form a partition of $\mathbb{R}^n$.

Consider any fundamental region $\mathcal{F}$ of lattice $\mathcal{L}$, S' can be partitioned into sets $S'_{\mathbf{v}} = S' \cap (\mathbf{v} + \mathcal{F})$ for each $\mathbf{v} \in \mathcal{L}$. Then, the translates $S'_{\mathbf{v}} - \mathbf{v} \subseteq \mathcal{F}$, and $vol(S') > vol(\mathcal{F})$, so it means some regions must overlap. This indicates that there must exist $\mathbf{z} \in (S'_{\mathbf{v}} - \mathbf{v}) \cap (S'_{\mathbf{u}} - \mathbf{u})$ for some distinct $\mathbf{u}, \mathbf{v} \in \mathcal{L}$. Therefore, we have $\mathbf{x} = \mathbf{z} + \mathbf{u}$ and $\mathbf{y} = \mathbf{z} + \mathbf{v} \in S'$, and difference $\mathbf{x} - \mathbf{y} = \mathbf{u} - \mathbf{v} \in \mathcal{L}$ is a lattice point.

Finally, we have $2\mathbf{x}, -2\mathbf{y} \in S$ by the definition and central symmetry of S and S'. Followed by convexity, the midpoint $\frac{2\mathbf{x} - 2\mathbf{y}}{2} = \mathbf{x} - \mathbf{y} \in S$. □

Corollary 1.1.1. *For any n-dimensional lattice $\mathcal{L}$, we have the length of shortest vector $\lambda(\mathcal{L}) > \sqrt{n} \cdot det(\mathcal{L})^{1/n}$.*

Proof. For simplicity, we assume $det(\mathcal{L}) = 1$ by scaling with the factor $det(\mathcal{L})^{-1/n}$. Let S be a n-dimensional sphere with radius $\sqrt{n}$ at the origin, and S strictly contains a $[-1, 1]^n$ cube with side length 2, and volume 2^n. Therefore, we have $vol(S) > 2^n$. With Theorem 1.1, we conclude there is a non-zero lattice point inside S. Multiplying the scale factor, we have $\lambda(\mathcal{L}) > \sqrt{n} \cdot det(\mathcal{L})^{1/n}$. □

However, Minowski's theorem only gives a upper bound of SVP, but we still have no clue on how to find the shortest vector. Finding shortest non-zero vector in 2-dimensional lattices was solved by Gauss in the 19th century, but there was not efficient algorithm of solving SVP in higher dimensions until 1980s. In 1981, mathematician Perter van Emde Boas conjectured that SVP is a NP-hard problem[1].

Up to date, there is no algorithm can solve SVP exactly and run efficiently, but Arjen Lenstra, Hendrik Lenstra and László Lovász posted a well-known approximation algorithm of SVP in 1982, which can approximate a non-zero lattice vector in n-dimension lattice $\mathcal{L}$ of length at most $2^{(n-1)/2}$ times $\lambda(\mathcal{L})$ in polynomial time [1]. Although the approximation factor seems too large at the first glance, it is actually better than the Minowski's bound, because it only depends on the number of dimensions, while Minowski's bound depends on the determinant of lattice as well. Practically, LLL algorithm can give a good approximation in reasonable time.

2. Basis Reduction

Basis reduction is a process of reducing the basis $\mathbf{B}$ of a lattice $\mathcal{L}$ to a shorter basis $\mathbf{B}'$ while keeping $\mathcal{L}$ the same. Figure 1 shows a reduced basis in two dimensional space. Common ways to change the basis but keep the same lattice include:

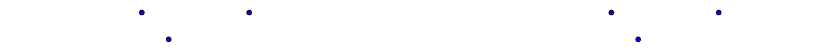

Figure 1: A lattice with two different basis in 2 dimension. The determinant of the basis is shaded. The right basis is reduced and orthogonal.

1. Swap two vectors in the basis.
2. For a vector $\mathbf{b_i} \in \mathbf{B}$, use $-\mathbf{b_i}$ instead.

[1] The approximation factor can be reduced to $(\frac{2}{\sqrt{3}})^n$ if the algorithm is tuned, but it is still exponential in n

3. For a vector $\mathbf{b_i} \in \mathbf{B}$, add a linear combination of other basis vectors to it. For any vector $\mathbf{v}$ in lattice, it can be expressed as

$$\mathbf{v} = \sum_{i=0}^{m} z_i \mathbf{b_i}.$$

After addition, we have a new basis vector $\mathbf{b_j}$, where

$$\mathbf{b_j} = \mathbf{b_j} + \sum_{i \neq j} y_i \mathbf{b_i}, y_i \in \mathbb{Z}.$$

We can still express lattice $\mathcal{L}$ with the new basis,

$$\mathbf{v} = \sum_{i \neq j} z_i \mathbf{b_i} + z_j(\mathbf{b_j} + \sum_{i \neq j} y_i \mathbf{b_i}).$$

Therefore, the lattice remains the same after changing the basis.

Basis reduction can help solving SVP, because if we cannot reduce a basis anymore, the shortest basis vector should be the shortest vector of the lattice. We start by solving the SVP in 2-dimentional case.

Definition 2.1 (Two dimensional reduced basis)**.** A basis $(\mathbf{b_1}, \mathbf{b_2})$ is said to be reduced if it satisfies following condition:

$$\begin{aligned} ||\mathbf{b_1}|| &\leq ||\mathbf{b_2}|| \\ u = \frac{\mathbf{b_1} \cdot \mathbf{b_2}}{||\mathbf{b_1}||^2} &\leq \frac{1}{2}. \end{aligned}$$

u is called the orthogonal projection coefficient, and Figure 2 shows a process of projection. Figure 2 shows the process of orthogonal projection. Based on this definition, we have following theorems.

Theorem 2.1. *Given a two dimensional lattice $\mathcal{L}$ with basis rank 2, if λ is the length of the shortest vector in $\mathcal{L}$, then*

$$\lambda \leq \sqrt{\frac{2}{\sqrt{3}} det(\mathcal{L})}.$$

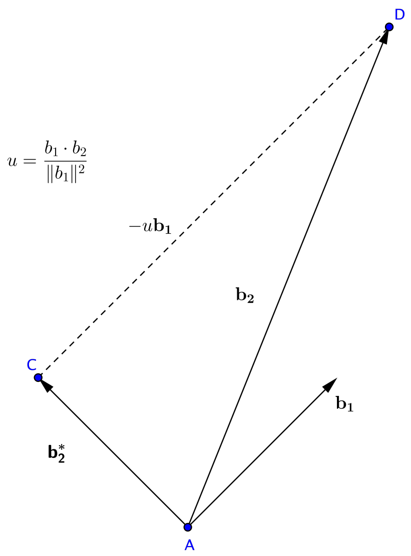

Figure 2: Orthogonal projection. The set $\{\mathbf{b_1}, \mathbf{b_2^*}\}$ is the orthogonal basis for the lattice generated by basis $\{\mathbf{b_1}, \mathbf{b_2}\}$

Proof. Suppose we have a reduced basis $\{\mathbf{b_1}, \mathbf{b_2}\}$, and its orthogonal basis is $\{\mathbf{b_1}, \mathbf{b_2^*}\}$.Based on the orthogonal process, we have

$$\mathbf{b_2} = \mathbf{b_2^*} + u\mathbf{b_1}$$

$$\|\mathbf{b_2}\|^2 = \|\mathbf{b_2^*}\|^2 + u^2\|\mathbf{b_1}\|^2$$

$$\|\mathbf{b_2^*}\|^2 = \|\mathbf{b_2}\|^2 - u^2\|\mathbf{b_1}\|^2 \geq \|\mathbf{b_1}\|^2 - \frac{1}{4}\|\mathbf{b_1}\|^2 = \frac{3}{4}\|\mathbf{b_1}\|^2$$

$$\|\mathbf{b_2^*}\| \geq \frac{\sqrt{3}}{2}\|\mathbf{b_1}\|$$

$$\|\mathbf{b_2^*}\|\|\mathbf{b_1}\| = det(\mathcal{L}) \geq \frac{\sqrt{3}}{2}\|\mathbf{b_1}\|^2$$

$$\|\mathbf{b_1}\| \leq \sqrt{\frac{2}{\sqrt{3}}det(\mathcal{L})}$$

λ is smaller or equal to $\|\mathbf{b_1}\|$, so the theorem is proved. □

Theorem 2.2. *If a basis $\{\mathbf{b_1}, \mathbf{b_2}\}$ is reduced, then $\mathbf{b_1}$ is the shortest vector.*

Proof. Let $\mathbf{x}$ is the shortest vector in lattice $\mathcal{L}$, so we have $\mathbf{x} = z_1\mathbf{b_1} + z_2\mathbf{b_2}$.

Then,

$$\begin{aligned}
\|\mathbf{x}\|^2 &= \|z_1\mathbf{b_1} + z_2\mathbf{b_2}\|^2 \\
&= \|z_1\mathbf{b_1} + z_2(\mathbf{b_2^*} + u\mathbf{b_1})\|^2 \\
&= (z_1 + z_2u)^2\|\mathbf{b_1}\|^2 + z_2^2\|\mathbf{b_2^*}\|^2 \\
&\geq (z_1 + z_2u)^2\|\mathbf{b_1}\|^2 + z_2^2\frac{3}{4}\|\mathbf{b_1}\|^2 \\
&= \|\mathbf{b_1}\|^2
\end{aligned}$$

As $\mathbf{x}$ is the shortest vector, it is only possible that $\|\mathbf{x}\|^2 = \|\mathbf{b_1}\|^2$, so $\mathbf{b_1}$ is the shortest vector. □

Gauss solved SVP in 2-dimensional lattice in 19th century, and the description of his algorithm is following:

1. Start with basis $\{\mathbf{b_1}, \mathbf{b_2}\}$, if $\|\mathbf{b_1}\| > \|\mathbf{b_2}\|$, swap $\mathbf{b_1}$ and $\mathbf{b_2}$.
2. Compute $u = \frac{\mathbf{b_1}\cdot\mathbf{b_2}}{\|\mathbf{b_1}\|^2}$. If $u > \frac{1}{2}$, let m be the biggest integer that is smaller than u, and let $\mathbf{b_2} = \mathbf{b_2} - m\mathbf{b_1}$.
3. If $\|\mathbf{b_1}\| > \|\mathbf{b_2}\|$, then swap $\mathbf{b_1}$ and $\mathbf{b_2}$, and repeat step 2. Otherwise, output $\mathbf{b_1}$.

3. Gram-Schmidt Orthogonalization

The idea of basis reduction in two dimensional lattice is to find the orthogonal basis based on the given basis. The basis we found in Gauss algorithm is not exactly orthogonal, but it is the nearest basis we can get. To generalize the algorithm to n-dimensions, we need to find a way to construct n-dimensional orthogonal basis based on the given basis, which leads us to Gram-Schmidt Orthogonalization.

Theorem 3.1 (Gram-Schmidt Orthogonalization method)**.** *Given a basis $\{\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_m}\}$ of a subspace H_m of $\mathbb{R}^n$, we define*

$$\begin{aligned}
&\mathbf{b_1}^* = \mathbf{b_1}, \\
&\mathbf{b_2}^* = \mathbf{b_2} - u_{1,2}\mathbf{b_1}, && \text{where } u_{1,2} = \frac{\mathbf{b_2}\cdot\mathbf{b_1}^*}{\mathbf{b_1}^*\cdot\mathbf{b_1}^*} \\
&\vdots \\
&\mathbf{b_m}^* = \mathbf{b_m} - \sum_{i<m} u_{i,m}\mathbf{b_i}, && \text{where } u_{i,m} = \frac{\mathbf{b_m}\cdot\mathbf{b_i}^*}{\mathbf{b_i}^*\cdot\mathbf{b_i}^*}
\end{aligned}$$

Then, $\{\mathbf{b_1}^*, \mathbf{b_2}^*, \cdots, \mathbf{b_m}^*\}$ is an orthogonal basis of H_m.

Proof. This theorem can be proved by induction on the dimension of the vector space.

1. For $k = 1$, $\mathbf{b_1}^* = \mathbf{b_1}$.
2. For $k = 2$: $\{\mathbf{b_1}^*, \mathbf{b_2}^*\}$ is orthogonal, because $\mathbf{b_2}^*$ is constructed by orthogonal projection of $\mathbf{b_2}$ onto $\mathbf{b_1}^*$. Figure 2 shows this process. Also, $\mathbf{b_2}^*$ is constructed by subtracting a linear combination of other basis vector, so $\{\mathbf{b_1}^*, \mathbf{b_2}^*\}$ is a basis of H_2.
3. For $2 < k \leq m$:
   - $\{\mathbf{b_1}^*, \mathbf{b_2}^*, \cdots, \mathbf{b_k}^*\}$ is orthogonal because $\{\mathbf{b_1}^*, \mathbf{b_2}^*, \cdots, \mathbf{b_{k-1}}^*\}$ is orthogonal based on the induction hypothesis, and $\mathbf{b_k}^*$ is constructed by orthogonal projection of $\mathbf{b_k}$ onto every other vectors.
   - $\mathbf{b_k}^*$ is constructed by subtracting a linear combination of other basis vectors, so $\{\mathbf{b_1}^*, \mathbf{b_2}^*, \cdots, \mathbf{b_k}^*\}$ is a basis of H_k.

□

Based on the Theorem 3.1, if we set $u_{m,m} = 1$, then we have

$$\mathbf{b_m} = \sum_{i=1}^{m} u_{i,m} \mathbf{b_i}.$$

Therefore, we can write the above formula in matrix form, $B = B^*U$, where basis vectors are columns in B and B^*. Thus, we have

$$U = \begin{pmatrix} u_{1,1} & u_{1,2} & \cdots & u_{1,n} \\ 0 & u_{2,2} & \cdots & u_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & u_{n,n} \end{pmatrix} = \begin{pmatrix} 1 & u_{1,2} & \cdots & u_{1,n} \\ 0 & 1 & \cdots & u_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

U is a upper trianglar matrix with 1s on the diagonal, so $det(U) = 1$. We can then factoring B^* by $B^* = QD$,

$$D = \begin{pmatrix} \|\mathbf{b_1}^*\| & & & \\ & \|\mathbf{b_2}^*\| & & \\ & & \ddots & \\ & & & \|\mathbf{b_m}^*\| \end{pmatrix}$$

where Q is an orthogonal matrix. Thus, we have

$$B = QDU.$$

Lemma 3.2. *For any n-dimensional lattice $\mathcal{L}$ with basis B, we have $det(\mathcal{L}) = \Pi_{i=1}^{n}\mathbf{b_i}\|$.*

Proof.

$$det(\mathcal{L}) = det(B) = det(Q)det(D)det(U) = det(D) = \Pi_{i=1}^{n}\|\mathbf{b_i}\|.$$

□

Lemma 3.3. *For any n-dimensional lattice $\mathcal{L}$ with basis B, we have the length of shortest vector $\lambda(\mathcal{L}) \geq \min_i \|\mathbf{b_i}^*\|$.*

Proof. For any non-zero lattice vector $\mathbf{v}$,

$$\begin{aligned}\mathbf{v} &= \sum_{i=1}^{k} z_i\mathbf{b_i}\\ &= \sum_{i=1}^{k} z_i \sum_{j=1}^{i} u_{j,i}\mathbf{b_j}^*\\ &= z_k\mathbf{b_k}^* + \sum_{j=1}^{k-1}\sum_{i=1}^{k} z_i u_{j,i}\mathbf{b_j}^*\end{aligned}$$

Thus,

$$\|\mathbf{v}\| \geq \|z_k\mathbf{b_k}^*\| \geq \|\mathbf{b_k}^*\|.$$

□

4. LLL Basis Reduction

In Section 2, we have introduced a two dimensional reduced basis, and the way to solve the SVP in two-dimension with Gauss algorithm. However, the real interesting SVP still remains unsolved in the higher dimension. In 1997, Ajtai proved SVP is NP-hard to solve exactly under randomized reduction [2], and later, Micciancio proved that SVP is NP-hard to approximate with any factor less than $\sqrt{2}$ [3]. Although the SVP is proved unsolvable within realistic time, a good approximation of the SVP would be useful in practical problems. By observing in the two dimensional case, we found that in the process of reducing the basis, we want to make the basis vectors as the most orthogonal as possible. The orthogonal basis cannot be reduced any more. With the Gram-Schmidt orthogonalization in higher dimensions, A. Lenstra, H. Lenstra, and L. Lovász proposed an approximation algorithm of basis reduction in higher dimensions in 1982 [4], which is called LLL basis reduction algorithm. To begin with, they defined LLL reduced basis.

Definition 4.1 (LLL reduced basis)**.** Let $\{\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_n}\}$ be a basis for a n-dimensional Lattice $\mathcal{L}$, and $\{\mathbf{b_1}^*, \mathbf{b_2}^*, \cdots, \mathbf{b_n}^*\}$ be the orthogonal basis generated in Theorem 3.1, and we have $u_{i,k} = \frac{\mathbf{b_k}\cdot\mathbf{b_i}^*}{\mathbf{b_i}^*\cdot\mathbf{b_i}^*}$. We say $\{\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_n}\}$ is a LLL reduced basis if it satisfies two conditions:

(1) $\forall i \neq k, u_{i,k} \leq \frac{1}{2}$,
(2) For each i, $\|\mathbf{b_{i+1}}^* + u_{i,i+1}\mathbf{b_i}^*\|^2 \geq \frac{3}{4}\|\mathbf{b_i}^*\|^2$.

Remark. The constant $\frac{3}{4}$ is chosen for the simplicity of the paper. Any constant between $\frac{1}{4}$ and 1 can guarantee that the algorithm terminates in polynomial time.

Remark. The condition 2 emphasizes the ordering of the basis, like what we did in two dimensional case.

Given a basis $\{\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_n}\}$ in n-dimension, to get a LLL reduced basis, the LLL algorithm works as below.

Algorithm 1: LLL Algorithm

```
Input: $\{\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_n}\}$
Repeat two steps until find the LLL reduced basis
Step 1: Gram-Schmidt orthogonalization
for $i = 1$ to $n$ do
    for $k = i - 1$ to $1$ do
        $m \leftarrow$ nearest integer of $u_{k,i}$
        $\mathbf{b_i} \leftarrow \mathbf{b_i} - m\mathbf{b_k}$
    end
end
Step 2: Check Condition 2, and swap
for $i = 1$ to $n - 1$ do
    if $\|\mathbf{b_{i+1}}^* + u_{i,i+1}\mathbf{b_i}^*\|^2 < \frac{3}{4}\|\mathbf{b_i}^*\|^2$ then
        swap $\mathbf{b_{i+1}}$ and $\mathbf{b_i}$
        go to step 1
    end
end
```

In step 1, we computed the most orthogonal basis based on Gram-Schmidt orthogonalization, and we check our second condition in step 2. If any basis violates the order, we swap them and repeat step 1.

The LLL algorithm gives us an approximation within an exponential factor of the actual shortest vector in polynomial time. First, we show that the reduced basis produced from LLL Algorithm gives a short vector within an exponential faction of the actual shortest vector.

Claim 4.1. *If $\{\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_n}\}$ is a n-dimensional LLL reduced basis of Lattice $\mathcal{L}$, then $\|\mathbf{b_1}\| \leq 2^{\frac{n-1}{2}}\lambda(\mathcal{L})$, where $\lambda(\mathcal{L})$ is the length of the shortest vector of $\mathcal{L}$.*

Proof. Based on our definition of LLL reduced basis, we have

$$\|\mathbf{b_i}^*\|^2 \leq \frac{4}{3}\|\mathbf{b_{i+1}}^* + u_{i,i+1}\mathbf{b_i}^*\|^2$$

By expanding the right hand side,

$$= \frac{4}{3}\|\mathbf{b_{i+1}}^*\|^2 + \frac{4}{3}u_{i,i+1}^2\|\mathbf{b_i}^*\|^2$$

With $u_{i,i+1} \leq \frac{1}{2}$, we get

$$\leq \frac{4}{3}\|\mathbf{b_{i+1}}^*\|^2 + \frac{1}{3}\|\mathbf{b_i}^*\|^2,$$

which gives us $\|\mathbf{b_{i+1}}^*\|^2 \geq \|\mathbf{b_i}\|^2$. By induction on i, we have

$$\|\mathbf{b_i}^*\|^2 \geq \frac{1}{2^{i-1}}\|\mathbf{b_1}^*\|^2 = \frac{1}{2^{i-1}}\|\mathbf{b_1}\|^2.$$

Based on Lemma 3.3, we have $\lambda(\mathcal{L}) \geq \min_i \|\mathbf{b_i}^*\|$. Therefore, by combining it with inequality above, we get

$$\|\mathbf{b_i}\|^2 \leq \min_i\{2^{i-1}\|\mathbf{b_i}^*\|^2\} \leq 2^{n-1}\lambda(\mathcal{L})^2.$$

Thus, we prove the claim. □

Second, we show that the LLL algorithm terminates in polynomial time of n. Note that the step 1 takes polynomial time, and step 2 takes linear time, so we need to show that we only repeat step 1 and step 2 a polynomial number of times. To show this, we define a function:

$$F(\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_n}) = \Pi_{i=1}^{n} \|\mathbf{b_i}^*\|^2.$$

In step 1, we do not change $\mathbf{b_i}^*$, so F does not change.

In step 2, we swap $\mathbf{b_i}$ and $\mathbf{b_{i+1}}$ only when $\|\mathbf{b_i}^*\|^2 > \frac{4}{3}\|\mathbf{b_{i+1}}^* + u_{i,i+1}\mathbf{b_i}^*\|^2 \geq \frac{4}{3}\|\mathbf{b_{i+1}}^*\|^2$. By swapping, we reduce F by at lease a factor of $\frac{2}{\sqrt{3}}$.

Let $\|\mathbf{b_{max}}\| = \max_i \|\mathbf{b_i}\|, \forall i$, we get an upper bound of F, which is $\|\mathbf{b_{max}}\|^{n(n-1)/2}$. Thus, we can only decrease F $\log_{2/\sqrt{3}}(\|\mathbf{b_{max}}\|^{n(n-1)/2})$ times, which is in polynomial time of n.

5. Conclusion

In this paper, we introduced an algorithm, LLL basis reduction algorithm, for approximating the shortest vector in higher dimensional space in polynomial time. Although the algorithm was developed in early 1980s, it still has various applications in number theory, integer programming and cryptography because of its performance and accuracy. The appearance of LLL algorithm inspired new development of cryptography since the existing encryption systems can be easily broken by LLL algorithm. Also, it is a fundamental algorithm for solving lattice problems.

References

[1] P. van Emde Boas, Another np-complete problem and the complexity of computing short vectors in a lattice, Technical Report 81 (04).

[2] M. Ajtai, The shortest vector problem in l_2 is np-hard for randomized reductions (extended abstract), Proceedings of the thirties Annial ACM Symposium on Theory of Computing -STOC (1998) 10–19.

[3] D. Micciancio, The shortest vector problem is NP-hard to approximate to within some constant, SIAM Journal on Computing 30 (6) (2001) 2008–2035, preliminary version in FOCS 1998. doi:10.1137/S0097539700373039.

[4] A. K. Lenstra, H. W. Lenstra, L. Lovász, Factoring polynomials with rational coefficients, Mathematische Annalen 261 (4) (1982) 515–534. doi:10.1007/BF01457454. URL http://dx.doi.org/10.1007/BF01457454