Lecture Notes on Lattices, Bases and the Reduction Problem
(Expository Notes)

by

Bud Mishra

Technical Report No. 300
Robotics Report No. 113
June, 1987

New York University
Dept. of Computer Science
Courant Institute of Mathematical Sciences
251 Mercer Street
New York, New York 10012

Work on this paper has been supported by Office of Naval Research Grant N00014-82-K-0381, National Science Foundation CER Grant DCR-83-20085, and by grants from the Digital Equipment Corporation and the IBM Corporation.

ABSTRACT

These sets of notes are somewhat fleshed out version of the Section 1.2. of Lovász's Book "*An Algorithmic Theory of Numbers, Graphs and Convexity*." Both Cassel's and Lekkerkerker's books are excellent texts on Geometry of Numbers. However, we need only a small portion of these books, and we develop the materials *ab initio*.

1 Geometry of Numbers

The subject of "*geometry of numbers*" was developed by Minkowski around the turn of the century. This has been a classical tool in subjects such as *integral quadratic forms*, *diophantine approximations*. However, it occupied its renewed role as a powerful tool in Computer Science, after H.W. Lenstra used it to give a polynomial time algorithm for the *Integer Programming (Feasibility) Problem* for fixed number of variables. Since then it has been used to give efficient algorithms in as diverse areas as *simultaneous diophantine approximations*, *cryptography*, *solvability by radicals*, *low density subset sum problem*, *computing with algebraic numbers*, *factorization of polynomials over finite fields*.

The main approach common to all the algorithms involves reformulating the initial problem as a geometrical problem concerning lattices of points. The geometric insights gained by such representations is a powerful aid to thinking about both classical and algorithmic problems.

Definition 1.1 [LATTICE]
Let $a_1, a_2, \ldots, a_n \in \mathbb{R}^n$ be a set of linearly independent vectors in $\mathbb{R}^n$. Let A be an $n \times n$ matrix with columns $a_1, a_2, \ldots, a_n$,

$$A = (a_1, a_2, \ldots, a_n).$$

The *lattice generated by* A (*by* $a_1, a_2, \ldots, a_n$) is defined to be

$$\Lambda = \Lambda(A) = \mathbb{Z}a_1 + \mathbb{Z}a_2 + \cdots + \mathbb{Z}a_n = \{\lambda_1 a_1 + \lambda_2 a_2 + \cdots \lambda_n a_n \mid \lambda_i \in \mathbb{Z}\},$$

i.e., integer linear combinations of the vectors $a_1, a_2, \ldots, a_n$.

We say that $a_1, a_2, \ldots, a_n$ is a *basis of the lattice* $\Lambda(a_1, a_2, \ldots, a_n)$, and A is its *basis matrix*. We say n is the *dimension of the lattice* Λ. □

The same lattice Λ may have many bases, but they are related to one another.

Definition 1.2 A square matrix U is called *unimodular*, if

$$\det U = \pm 1. \quad \square$$

Theorem 1.1 *Let* $\Lambda_1 = \Lambda(A_1)$ *and* $\Lambda_2 = \Lambda(A_2)$ *be two* n*-dimensional lattices, with basis matrices* A_1 *and* A_2*, respectively. Then* $\Lambda_1 = \Lambda_2$*, if and only if there exists an integer unimodular matrix* U*, such that*

$$A_1 = A_2 U.$$

PROOF.

($\Rightarrow$) Assume $\Lambda_1 = \Lambda_2$. Then the column vectors of A_2 are integer linear combinations of the column vectors of A_1, and *vice versa*. Hence there are integer matrices U_1 and U_2 such that

$$A_2 = A_1 U_1, \quad \text{and} \quad A_1 = A_2 U_2.$$

Hence

$$A_1 = A_1 U_1 U_2.$$

Since A_1 is of full rank,

$$U_1 U_2 = I_n,$$

where I_n is the $n \times n$ identity matrix. This implies

$$\det U_1 \det U_2 = 1, \quad \text{and} \quad \det U_1, \det U_2 \in \mathbb{Z};$$

from which we conclude that

$$|\det U_1| = 1 = |\det U_2|.$$

The matrices U_1 and U_2 are integer unimodular matrices.
($\Leftarrow$) Assume that there is an integer unimodular matrix U such that

$$A_2 = A_1 U.$$

Then

$$U^{-1} = \frac{\operatorname{adj} U}{\det U} = \pm \operatorname{adj} U \in \mathbb{Z}^{n \times n},$$

and

$$\left|\det U^{-1}\right| = \frac{1}{|\det U|} = 1,$$

i.e. U^{-1} is an integer unimodular matrix. Furthermore,

$$A_1 = A_2 U^{-1}.$$

Hence the column vectors of A_2 are integer linear combinations of the column vectors of A_1, and *vice versa*. Thus $\Lambda_1 = \Lambda_2$. □

The transformation corresponding to the integer unimodular matrix, is called an *integer unimodular transformation*. Following three transformations can be easily shown to be integer unimodular:

(A) Multiply some basis vector by -1.

(B) Add an integer multiple of a basis vector to another.

(C) Permute two basis vectors.

It is possible that the same lattice Λ may have two distinct bases A_1 and A_2; however, they are related by an integer unimodular matrix U,

$$A_2 = A_1 U;$$

and thus all the basis matrices have the same determinant (up to their signs), the absolute value of which is a characteristic of the lattice Λ.

Definition 1.3 [DETERMINANT OF A LATTICE]
Let $\Lambda(A)$ be a lattice with basis matrix A. The number

$$\det \Lambda = \sqrt{\det A^{\mathrm{T}} A} = |\det A|$$

is called the *determinant of the lattice.* □

Geometrically, the determinant of the lattice is the common n-volume of those parallelohedra whose vertices are lattice points and which contain no other lattice point; equivalently, *n-volume of those parallelohedra spanned by bases.*

Definition 1.4 [DUAL LATTICE]
Every lattice Λ has a *dual lattice*, called Λ^*,

$$\Lambda^* = \{x \in \mathbb{R}^n \mid y^{\mathrm{T}} x \in \mathbb{Z} \text{ for every } y \in \Lambda\}. \quad \square$$

If $(a_1, a_2, \ldots, a_n)$ is a basis of Λ then the vectors $a_1^*, a_2^*, \ldots, a_n^*$ defined by

$$\langle a_i^*, a_j \rangle = \begin{cases} 1, & \text{if } i = j; \\ 0, & \text{if } i \neq j. \end{cases}$$

form a basis for the dual lattice, called the *dual basis* of $(a_1, a_2, \ldots, a_n)$. That is

$$A^{*\mathrm{T}} A = I_n.$$

Moreover, we have the following properties:

(A) $\Lambda^{**} = \Lambda$.

(B) $(\det \Lambda^*)(\det \Lambda) = 1$, i.e.,

$$\det \Lambda^* = \frac{1}{\det \Lambda}.$$

(C) If Λ_1 and Λ_2 are two lattices then

$$(\Lambda_1 \cap \Lambda_2)^* = \Lambda_1^* + \Lambda_2^*, \quad \text{and} \quad (\Lambda_1 + \Lambda_2)^* = \Lambda_1^* \cap \Lambda_2^*.$$

2 Gram-Schmidt Orthogonalization

Let $(b_1, b_2, \ldots, b_n)$ be a (vector space) basis of $\mathbb{R}^n$. Then an *orthogonal basis* $(b_1^*, b_2^*, \ldots, b_n^*)$ of $\mathbb{R}^n$ can be found by the following simple procedure, known as *Gram-Schmidt Orthogonalization*:

Procedure *GRAM-SCHMIDT*;

INPUT: $(b_1, \ldots, b_n)$: Basis $\in \mathbb{R}^n$
OUTPUT: $(b_1^*, \ldots, b_n^*)$: Basis $\in \mathbb{R}^n$ such that the b_i^*'s are mutually orthogonal;

begin
$b_1^* := b_1$;
for $i := 2$ to n loop

$$b_i^* := b_i - \sum_{j=1}^{i-1} \left(\frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} \right) b_j^*;$$

end{loop }
end{*GRAM-SCHMIDT*}. □

We have used the notation $\langle b_i, b_j \rangle$ to denote the vector dot product of two vectors b_i and b_j.

Hence, we see that

(A) Each b_i can be written in terms of b_j^*'s as follows:

$$b_i = \sum_{j=1}^{i} \mu_{i,j} b_j^*,$$

where

$$\mu_{i,j} = \begin{cases} 0, & \text{if } i < j; \\ 1, & \text{if } i = j; \\ \dfrac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle}, & \text{if } i > j. \end{cases}$$

Hence,

$$B = B^* M^{\mathrm{T}},$$

where M is an $n \times n$ lower triangular matrix with the $(i,j)^{\text{th}}$ entry, $\mu_{i,j}$, and B and B^* are the $n \times n$ matrices with the column vectors b_i's and b_i^*'s, respectively. Note that

$$\det B^{\mathrm{T}} B = \det M (B^*)^{\mathrm{T}} B^* M^{\mathrm{T}} = \det (B^*)^{\mathrm{T}} B^*,$$

since

$$\det M = \prod_{i=1}^{n} \mu_{i,i} = 1.$$

(B) Since the column vectors of B^* are mutually orthogonal,

$$(B^*)^{\mathrm{T}} B^* = \operatorname{diag} \{\langle b_i^*, b_i^* \rangle\}_i = \operatorname{diag} \left\{ \|b_i^*\|^2 \right\}_i,$$

and

$$\det (B^*)^{\mathrm{T}} B^* = \prod_{i=1}^{n} \|b_i^*\|^2.$$

(C) From (A), we know that

$$\|b_i^*\|^2 \leq \|b_i^*\|^2 + \sum_{j=1}^{i-1} \mu_{i,j}^2 \|b_j^*\|^2 = \|b_i\|^2,$$

Since b_i^*'s are mutually orthogonal.

Hence we obtain the following inequality, known as *Hadamard's Inequality*:

$$\det B^{\mathrm{T}} B = \det (B^*)^{\mathrm{T}} B^* = \prod_{i=1}^{n} \|b_i^*\|^2 \leq \prod_{i=1}^{n} \|b_i\|^2.$$

Equivalently,

$$|\det B| \leq \prod_{i=1}^{n} \|b_i\|.$$

Geometrically, this can be interpreted to mean that the n-volume of the parallelohedra spanned by the basis vectors is always bounded from above by the product of the Euclidean lengths of the basis vectors.

(D) Let $(b_1, b_2, \ldots, b_n)$ be a basis of $\mathbb{R}^n$. Let us denote by $b_i(j)$ the component of b_i orthogonal to the linear subspace spanned by the first $j-1$ vectors $b_1, b_2, \ldots, b_{j-1}$.

Observe that

(a) If $i < j$ then $b_i \in \text{span}\,(b_1, b_2, \ldots, b_{j-1})$, and thus, $b_i(j) = 0$ and $\mu_{i,j} = 0$.

(b) If $i = j$ then $b_i(i)$ is the component of b_i orthogonal to the $\text{span}\,(b_1, b_2, \ldots, b_{i-1}) = \text{span}\,(b_1^*, b_2^*, \ldots, b_{i-1}^*)$, and thus, $b_i(i) = b_i^*$ and $\mu_{ii} = 1$.

(c) If $i > j$ then

$$\begin{aligned} b_i(j) &= b_i - \sum_{k=1}^{j-1} \mu_{i,k} b_k^* \\ &= \sum_{k=1}^{i} \mu_{i,k} b_k^* - \sum_{k=1}^{j-1} \mu_{i,k} b_k^* \\ &= \sum_{k=j}^{i} \mu_{i,k} b_k(k) \end{aligned}$$

and

$$\mu_{i,j} = \frac{\|b_i(j) - b_i(j+1)\|}{\|b_j(j)\|}.$$

Hence,

$$b_{i+1}(i) = \sum_{k=i}^{i+1} \mu_{i+1,k} b_k(k) = b_{i+1}(i+1) + \mu_{i+1,i} b_i(i) = b_{i+1}^* + \mu_{i+1,i} b_i^*.$$

(E) Let $(a_1, a_2, \ldots, a_n)$ be a basis of an n-dimensional lattice Λ, and $(a_1^*, a_2^*, \ldots, a_n^*)$ be a Gram-Schmidt Orthogonalization of the basis.

Let ξ_1 be the Euclidean length of a shortest non-zero lattice vector b_1. Then

$$\begin{aligned} b_1 &= \sum_{i=1}^{n} \lambda_i a_i \\ &= \sum_{i=1}^{n} \lambda_i \left(a_i^* + \sum_{j=1}^{i-1} \mu_{i,j} a_j^* \right) \\ &= \sum_{i=1}^{n} \lambda_i a_i^* + \sum_{i=1}^{n} \sum_{j=1}^{i-1} \lambda_i \mu_{i,j} a_j^*. \end{aligned}$$

Hence,

$$\|b_1\|^2 \geq \sum_{i=1}^{n} |\lambda_i|^2 \|a_i^*\|^2 \geq \left(\min_{1 \leq i \leq n} \|a_i^*\| \right)^2.$$

Or,

$$\min_{1 \leq i \leq n} \|a_i^*\| \leq \xi_1. \tag{1}$$

As an immediate corollary of Hadamard's inequality, we see that

Proposition 2.1 *Let Λ be an n-dimensional lattice with the basis matrix*

$$A = (a_1, a_2, \ldots, a_n).$$

Then

$$\|a_1\| \, \|a_2\| \cdots \|a_n\| \geq \det \Lambda.$$

The equality in the above proposition can be guaranteed, if and only if the basis vectors $(a_1, a_2, \ldots, a_n)$ are mutually orthogonal. If the mutual orthogonality of the basis vectors is used as a measure of their goodness, we would like to answer the question of how good a basis can be found for a particular lattice Λ.

To that effect, let us define the ratio

$$\delta = \frac{\|a_1\| \, \|a_2\| \cdots \|a_n\|}{\det \Lambda}$$

to be the *orthogonality defect* of the basis. We know that $\delta \geq 1$. The question is how small a δ can we achieve for a particular lattice Λ.

A closely related problem is that of finding a shortest lattice vector of a lattice Λ. Notice that if v is a shortest vector in the lattice $\Lambda(a_1, \ldots, a_n)$ and

$$v = \lambda_1 a_1 + \cdots + \lambda_n a_n,$$

then

$$\lambda_i = \frac{\det(a_1, \ldots, a_{i-1}, v, a_{i+1}, \ldots, a_n)}{\det(a_1, \ldots, a_{i-1}, a_i, a_{i+1}, \ldots, a_n)}.$$

Hence

$$|\lambda_i| \leq \frac{\|a_1\| \cdots \|a_{i-1}\| \, \|v\| \, \|a_{i+1}\| \cdots \|a_n\|}{|\det \Lambda|}.$$

Since v is by assumption no greater than any of the lattice vector, in particular a_i

$$|\lambda_i| \leq \frac{\|a_1\| \, \|a_2\| \cdots \|a_n\|}{\det(a_1, a_2 \ldots, a_n)} = \delta.$$

Hence a shortest vector of the lattice can be found by searching among a set of $(2\lceil\delta\rceil + 1)^n$ possible values for the λ_i's.

In general, if a lattice Λ is presented with a basis matrix A, whose representation requires at least $\ell(A)$ number of bits, then we can only say that

$$\delta = 2^{O(\ell(A))}.$$

This, however, implies that the above 'generate-and-test' algorithm has a time complexity of $2^{O(n \cdot \ell(A))}$. This algorithm will be considered intractable, and it has been conjectured that the *shortest lattice vector problem* is NP-complete. So far, there is only a proof of NP-completeness, if the length of the vectors are taken to be their ℓ_∞-norms.

Before turning to the algorithmic problems raised by the above discussion, let us first consider the existence of a 'fairly good' bound for the orthogonality defect and the length of a shortest lattice vector.

3 Minkowski's Convex Body Theorem

Theorem 3.1 [MINKOWSKI'S CONVEX BODY THEOREM] *Let Λ be an n-dimensional lattice in $\mathbb{R}^n$. Let S be set in $\mathbb{R}^n$, which is convex and symmetric about the origin, and has n-volume $V(S)$ (not necessarily bounded). If*

$$V(S) > 2^n \det \Lambda,$$

then S contains at least one non-zero lattice vector $u \in \Lambda$.

PROOF.

Define

$$\frac{1}{2}S = \{x \in \mathbb{R}^n \mid 2x \in S\}.$$

Then it is easy to see that

1. $\frac{1}{2}S$ is convex and centrally symmetric, and
2. $V(\frac{1}{2}S) > \det \Lambda$.

For each lattice point v of Λ consider the body $v + \frac{1}{2}S$ obtained by translating $\frac{1}{2}S$ by v:

$$v + \frac{1}{2}S = \left\{x \in \mathbb{R}^n \mid x = v + s \text{ for some } s \in \frac{1}{2}S\right\}.$$

Hence the set of translates of $\frac{1}{2}S$ (one for each lattice point) has the additional property that some two of them must have a non-empty intersection.

This follows from the facts that the n-volume of each fundamental parallelohedra has a volume $\det \Lambda$ and that each of the replicas of $\frac{1}{2}S$ has a volume in excess of $\det \Lambda$.

Without loss of generality, we may assume that $\frac{1}{2}S$ and $v + \frac{1}{2}S$ are two such bodies with a non-empty intersection, i.e.,

$$\exists y \in \mathbb{R}^n \text{ such that } y \in \left(\frac{1}{2}S\right) \cap \left(v + \frac{1}{2}S\right).$$

Hence $y \in \frac{1}{2}S$, and $y - v \in \frac{1}{2}S$, (the later, because $y \in v + \frac{1}{2}S$). By the central symmetry of $\frac{1}{2}S$, we conclude also that $v - y \in \frac{1}{2}S$. By the convexity of $\frac{1}{2}S$, we also know that $\frac{1}{2}v$ (the mid point of y and $v - y$) is in $\frac{1}{2}S$. Hence,

$$v \in S.$$

But v was a lattice point by choice.

Notice that by the central symmetry, we can, in fact, conclude that both $\pm v \in S$. □

In the literature, the Minkowski's Convex Body Theorem is stated as follows. Though this is apparently a stronger theorem, the same proof technique applies and can be found in the standard text books on geometry of numbers.

Theorem 3.2 [MINKOWSKI'S CONVEX BODY THEOREM] *Let Λ be an n-dimensional lattice in $\mathbb{R}^n$. Let S be set in $\mathbb{R}^n$, which is convex and symmetric about the origin, and has n-volume $V(S)$ (not necessarily bounded). Let k be a positive natural number. If*

$$V(S) > k2^n \det \Lambda,$$

or

$$V(S) = k2^n \det \Lambda, \text{ and } S \text{ is compact,}$$

then S contains at least k pairs of distinct non-zero lattice vectors $\pm u_1$, $\pm u_2$, ..., $\pm u_k \in \Lambda$. □

Corollary 3.3 *Let Λ be an n-dimensional lattice in $\mathbb{R}^n$ and let b_1 be a shortest non-zero lattice vector of Λ. Then*

$$\|b_1\| \leq \sqrt{\frac{2}{\pi}} \sqrt{n} \sqrt[n]{\det \Lambda}.$$

PROOF.
Consider an n-dimensional sphere $S_n(r)$ of radius r about the origin. Then

$$V(S_n(r)) = \left(\frac{\pi^{n/2}}{\Gamma(n/2+1)}\right) r^n,$$

and

$$b \in S_n(r) \Rightarrow \|b\| \leq r.$$

Let us choose the radius r large enough so that $S_n(r)$ contains at least one lattice point. By Minkowski's Convex Body Theorem, it suffices to satisfy the following inequality:

$$V(S_n(r)) = \left(\frac{\pi^{n/2}}{\Gamma(n/2+1)}\right) r^n \geq 2^n \det \Lambda.$$

That is

$$r \geq \left(\frac{2}{\sqrt{\pi}}\right) \sqrt[n]{\Gamma(n/2+1)}\, \sqrt[n]{\det \Lambda}.$$

Since $\Gamma(x+1) \leq x^x$, it suffices to choose $r = \rho$ with

$$\rho = \sqrt{\frac{2}{\pi}} \sqrt{n}\, \sqrt[n]{\det \Lambda}$$

in order to guarantee that $S_n(\rho)$ contains a lattice point.

Hence if b_1 is a shortest non-zero lattice vector then $v \in S_n(\rho)$ and

$$\xi_1 = \|b_1\| \leq \rho = \sqrt{\frac{2}{\pi}} \sqrt{n}\, \sqrt[n]{\det \Lambda}.$$

□

Note that in the book, Lovasz has shown that

$$\xi_1 = \|b_1\| \leq \sqrt{n}\, \sqrt[n]{\det \Lambda}$$

using a much simpler argument.

4 Successive Minima and a Bound on the Orthogonality Defect

Definition 4.1 [SUCCESSIVE MINIMA]
Let S be a bounded centrally symmetric convex body in $\mathbb{R}^n$ of n-volume $V(S)$. For each $\xi > 0$, let ξS stand for the following centrally symmetric convex body

$$\xi S = \{\xi x \mid x \in S\}.$$

Let Λ be an n-dimensional lattice in $\mathbb{R}^n$. The quantity

$$\xi_k = \inf\{\xi > 0 \mid \xi S \text{ contains } k \text{ linearly independent vectors from } \Lambda\}$$

is called the k^{th} *successive minimum of* Λ with respect to S (for $k = 1, \ldots, n$).

The set of successive minima $\{\xi_k \mid k = 1, \ldots, n\}$ exist and there are n linearly independent vectors $b_1, b_2, \ldots, b_n$ in Λ, corresponding to the successive minima.

Furthermore

$$\xi_1 \leq \xi_2 \leq \cdots \leq \xi_n. \quad \square$$

By Minkowski's Convex Body Theorem it follows that $\xi_1 S$ has a volume

$$V(\xi_1 S) = \xi_1^n V(S) \leq 2^n \det \Lambda.$$

However by considering the whole set of successive minima $\xi_1, \xi_2, \ldots, \xi_n$, Minkowski could prove a much stronger result;

Theorem 4.1 [MINKOWSKI'S SUCCESSIVE MINIMA THEOREM] *Let Λ be an n-dimensional lattice in $\mathbb{R}^n$. Let S be a bounded set in $\mathbb{R}^n$, which is convex and symmetric about the origin, and has n-volume $V(S)$. Let $\xi_1, \xi_2, \ldots, \xi_n$ be the successive minima of Λ with respect to S. Then*

$$\frac{2^n}{n!} \det \Lambda \leq \xi_1 \xi_2 \cdots \xi_n V(S) \leq 2^n \det \Lambda$$

$\square$

The original proof of the above theorem due to Minkowski is rather lengthy. Subsequently, the proof has been considerably simplified and shortened by Davenport, Eastermann, Weyl and Pipping. We will omit

the proof, since it can be found in Cassels or Lekkerkerker [Cassels 1959], [Lekkerkerker 1969].

We will apply the above theorem to obtain a bound for the orthogonality defect of an n-dimensional lattice. For this purpose, it is sufficient only to consider S to be an n dimensional unit sphere, $S_n(1)$. We refer to the successive minima of Λ with respect to $S_n(1)$ as simply successive minima. In this case, the n linearly independent vectors $b_1, b_2, \ldots, b_n$ (associated with the successive minima) have the following additional property:

$$\|b_k\| = \xi_k.$$

Note that although $b_1, b_2, \ldots, b_n$ are vectors of the lattice Λ, and are linearly independent, they may not form a basis of the lattice. However the following lemma shows that there is a basis $(a_1, a_2, \ldots, a_n)$ of Λ that is 'quite close' to the set of vectors $\{b_1, b_2, \ldots, b_n\}$.

Lemma 4.2 *Let $b_1, b_2, \ldots, b_n$ be the n linearly independent vectors associated with the successive minima of the n-dimensional lattice Λ. Then there exists a basis $(a_1, a_2, \ldots, a_n)$ of Λ such that*

$$\|a_j\| \leq \max\left(1, \frac{j}{2}\right) \xi_j.$$

PROOF SKETCH.

(1) First we claim that there is a basis $(c_1, c_2, \ldots, c_n)$ of Λ such that

$$\begin{aligned} b_1 &= v_{11}c_1 \\ b_2 &= v_{21}c_1 + v_{22}c_2 \\ &\vdots \\ b_n &= v_{n1}c_1 + v_{n2}c_2 + \cdots + v_{nn}c_n \end{aligned}$$

for some integers v_{ij} with $v_{ii} \neq 0$. Roughly speaking, the above set of equations can be constructed by successively building the basis for the lattice

$$\Lambda_j = \Lambda \cap \operatorname{span}(b_1, b_2, \ldots, b_j).$$

We start with a basis for Λ_1, extend it to a basis for Λ_2, and so on, until we have constructed a basis for $\Lambda_n = \Lambda$.

(2) Solving the above set of triangular equations we obtain

$$c_j = \frac{1}{v_{jj}} b_j + \sum_{i=1}^{j-1} \lambda_{ji} b_i$$

where λ_{ji}'s are real. Let the notation $[x]$ stand for x rounded to the nearest integer:

$$|x - [x]| \leq \frac{1}{2},$$

and $\{x\}$ for $x - [x]$.

(3) Let

$$a_j = \begin{cases} b_j, & \text{if } |v_{jj}| = 1; \\ c_j - \sum_{i=1}^{j-1} [\lambda_{ji}] b_i, & \text{if } |v_{jj}| \geq 2. \end{cases}$$

Notice that a_j's are linear integer combination of the c_j's, and in fact the transformation is integer unimodular. Hence $(a_1, a_2, \ldots, a_\pi)$ is in fact a basis of Λ.

(4) Now to get the bounds, we consider two cases separately:

1. $a_j = b_j$. Then
$$\|a_j\| = \|b_j\| = \xi_j.$$
2. $a_j = c_j - \sum_{i=1}^{j-1} [\lambda_{ji}] b_i$. Then
$$\|a_j\| = \left\| \frac{1}{v_{jj}} b_j + \sum_{i=1}^{j-1} \{\lambda_{ji}\} b_i \right\| \leq \frac{1}{2} \sum_{i=1}^{j} \xi_j.$$

Hence

$$\|a_j\| \leq \frac{j}{2} \xi_j.$$

Combining the above argument, we get

$$\|a_j\| \leq \max\left(1, \frac{j}{2}\right) \xi_j.$$

□

Theorem 4.3 *Let Λ be an n-dimensional lattice. Then Λ has a basis $(a_1, a_2, \ldots, a_n)$ such that*

$$\prod_{i=1}^{n} \|a_i\| \leq 2 \frac{n!}{V(S_n(1))} \det \Lambda,$$

where $V(S_n(1))$ is the n-dimensional volume of the n-dimensional unit sphere:

$$V(S_n(1)) = \frac{\pi^{n/2}}{\Gamma(n/2+1)}.$$

PROOF.
Choose the basis $(a_1, a_2, \ldots, a_n)$ of the lattice as in the previous lemma. Then

$$V(S_n(1)) \prod_{i=1}^{n} \|a_i\| \leq \frac{n!}{2^{n-1}} \xi_1 \cdots \xi_n V(S_n(1)) \leq 2n! \det \Lambda.$$

Hence, we get the inequality

$$\prod_{i=1}^{n} \|a_i\| \leq 2 \frac{n!}{V(S_n(1))} \det \Lambda.$$

□

The above theorem shows that the orthogonality defect of an n-dimensional lattice are bounded from above and below:

$$1 \leq \delta_n \leq 2 \frac{n!\Gamma(n/2+1)}{\pi^{n/2}} = 2^{O(n \lg n)}.$$

Recall that our discussion from the previous section on computing a shortest vector in a lattice implies that if we know a basis of the lattice whose orthogonality defect δ is 'small' (i.e., bounded by $2^{O(n \lg n)}$) then a shortest vector can be computed in time

$$(2\lceil \delta \rceil + 1)^n \text{poly}(\ell(A)) = 2^{O(n^2 \lg n)} \text{poly}(\ell(A)).$$

For a fixed dimension lattice, a shortest vector of the lattice can be computed in polynomial time.

5 The Reduction Problem

In this chapter we turn to the algorithmic problems raised by the discussion of the previous chapter. In particular, we recall that every n-dimensional lattice Λ has a basis $(b_1, b_2, \ldots, b_n)$ such that

$$\det \Lambda \leq \|b_1\| \, \|b_2\| \cdots \|b_n\| \leq C_n \det \Lambda,$$

where C_n is a constant depending only on n. This result was proven by Hermite. We also showed that it is possible to achieve a $C_n = 2^{O(n \lg n)}$. In other words, for each n-dimensional lattice Λ theres exists a basis whose *orthogonality defect* satisfy the following inequalities:

$$1 \leq \frac{\|b_1\| \, \|b_2\| \cdots \|b_n\|}{\det \Lambda} \leq C_n = 2^{O(n \lg n)}.$$

Hermite's result suggests the following algorithmic problem:

Problem 5.1 [Basis Reduction Problem].

- Input: An n-dimensional lattice $\Lambda = \Lambda(B)$, and an integer $C \geq 1$.
- Output: A basis $(b_1, b_2, \ldots, b_n)$ such that

$$\|b_1\| \, \|b_2\| \cdots \|b_n\| \leq C \det \Lambda.$$

- Note: This problem has a solution if $C \geq n^n$; but, it is not known how to find such a basis. The problem of finding a basis which minimizes the product $\|b_1\| \, \|b_2\| \cdots \|b_n\|$, is NP-hard.
  Hence we relax the constrains to find a basis for which the orthogonality defect compares favourably with the Hermite's bound; that is we will consider a $C = C_n = 2^{O(\text{poly}n)}$ (single-exponential in n) as an acceptable bound. Note that this guarantees that, for a fixed dimension n, the shortest non-zero lattice vector can be found in polynomial time, with the dependence on n still being single exponential. We will call a basis satisfying the above bound, a *reduced basis* [1].

A related problem is the following:

Problem 5.2 [Short Vector Problem].

- Input: An n-dimensional lattice $\Lambda = \Lambda(B)$, and a number $\xi > 0$.
- Output: A vector $b \in \Lambda$, $b \neq 0$ such that

$$\|b\| \leq \xi.$$

[1] This definition of *reduced basis* is somewhat non-standard, but is rather clean and satisfies all the various definitions of reduced bases found in the literature.

- **Note:** If there is a polynomial time algorithm for the Short Vector Problem, then there is also a polynomial time algorithm that finds a shortest non-zero vector in the lattice, by a binary search over ξ.
  We showed that if $\xi \geq \gamma_n \sqrt[n]{\det \lambda}$ then such a vector b always exists; here, $\gamma_n \geq \sqrt{\frac{2n}{\pi}}$. Note, however, that a lattice Λ may contain a vector much shorter than $\sqrt[n]{\det \Lambda}$.
  Let $\gamma_n = \|b\| / \sqrt[n]{\det \Lambda}$ denote the smallest constant satisfying the above inequality. It is known that

$$\sqrt{\frac{n}{2e\pi}} \leq \gamma_n \leq \sqrt{\frac{n}{e\pi}}.$$

  It is widely believed that the Short Vector Problem (and hence the related search problem: Shortest Vector Problem) is NP-complete, though no such proof is currently available. It is not known either whether the weaker problem of finding a solution if $\xi = \sqrt{n} \sqrt[n]{\det \lambda}$ is NP-hard.

The above discussion indicates that the best we may hope for is a polynomial time algorithm to find a 'reduced basis.' In the rest of this chapter, we present Lenstra, Lenstra and Lovász's Basis Reduction Algorithm [Lenstra et. al. 1982] that finds a basis $(b_1, b_2, \ldots, b_n)$ of a lattice Λ satisfying the following inequality:

$$\|b_1\| \, \|b_2\| \cdots \|b_n\| \leq 2^{\frac{1}{2}\binom{n}{2}} \det \Lambda.$$

Also we show that if b_1 is the shortest among the vectors of the reduced basis then

$$\|b_1\| \leq 2^{(n-1)/4} \sqrt[n]{\det \Lambda}.$$

This indicates that we have polynomial time algorithms for both of the problems for appropriately large C and ξ. In practice, for many related problems, these are adequate to give polynomial time algorithms.

6 The L^3 Basis Reduction Algorithm

Let $(b_1, b_2, \ldots, b_n)$ be a basis for the n-dimensional lattice Λ, and $(b_1^*, b_2^*, \ldots, b_n^*)$, the Gram-Schmidt orthogonalization of the basis. We also know that each b_i can be written in terms of b_j^*'s as follows:

$$b_i = \sum_{j=1}^{i} \mu_{i,j} b_j^*,$$

where

$$\mu_{i,j} = \begin{cases} 0, & \text{if } i < j; \\ 1, & \text{if } i = j; \\ \dfrac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle}, & \text{if } i > j. \end{cases}$$

Since the orthogonality defect measures how orthogonal the basis vectors are to each other, in order to reduce the orthogonality defect, we will attempt to find a lattice basis close to the Gram-Schmidt vectors. Formally, our first attempt is to find a basis $(\overline{b_1}, \overline{b_2}, \ldots, \overline{b_n})$ from the original basis $(b_1, b_2, \ldots, b_n)$ via a sequence of unimodular integer transformations such that

$$\overline{b_i} = \sum_{j=1}^{i} \overline{\mu_{i,j}} b_j^*,$$

where

$$\overline{\mu_{i,j}} = \begin{cases} 0, & \text{if } i < j; \\ 1, & \text{if } i = j, \end{cases}$$

and

$$|\overline{\mu_{i,j}}| \leq \frac{1}{2}, \quad \text{if } i > j.$$

The basis $(\overline{b_1}, \overline{b_2}, \ldots, \overline{b_n})$ of Λ satisfying the above condition is called a *weakly reduced basis*.

Assume that we have a set of basis vectors $(\widehat{b_1}, \widehat{b_2}, \ldots, \widehat{b_n})$ satisfying the following equations:

$$\begin{aligned}
\widehat{b_1} &= b_1^* \\
\widehat{b_2} &= \widehat{\mu_{2,1}} b_1^* + b_2^* \\
&\vdots \\
\widehat{b_j} &= \widehat{\mu_{j,1}} b_1^* + \cdots + \widehat{\mu_{j,j-1}} b_{j-1}^* + b_j^* \\
&\vdots \\
\widehat{b_i} &= \widehat{\mu_{i,1}} b_1^* + \cdots + \widehat{\mu_{i,j-1}} b_{j-1}^* + \widehat{\mu_{i,j}} b_j^* + \cdots + b_i^* \\
&\vdots \\
\widehat{b_n} &= \widehat{\mu_{n,1}} b_1^* + \cdots + \widehat{\mu_{n,j-1}} b_{j-1}^* + \widehat{\mu_{n,j}} b_j^* + \cdots + \widehat{\mu_{n,i}} b_i^* + \cdots + b_n^*,
\end{aligned}$$

and let (i, j) be the lexicographically largest pair of indices satisfying the following conditions:

$$|\widehat{\mu_{i,j}}| > \frac{1}{2}, \text{ and}$$

$$|\widehat{\mu_{k,l}}| \leq \frac{1}{2}, \text{ for all } k,l \text{ such that } (k > i) \text{ or } (k = i \wedge l > j).$$

Now, let $m = [\widehat{\mu_{i,j}}]$ be the integer nearest to $\widehat{\mu_{i,j}}$. Consider the following new basis of Λ, $(\widehat{b'_1}, \ldots, \widehat{b'_i}, \ldots, \widehat{b'_n}) = (\widehat{b_1}, \ldots, \widehat{b_i} - m \cdot \widehat{b_j}, \ldots, \widehat{b_n})$, obtained by an integer unimodular transformation

$$\begin{aligned}
\widehat{b'_1} &= \widehat{b_1} \\
&= b_1^* \\
&\vdots \\
\widehat{b'_i} &= \widehat{b_i} - m \cdot \widehat{b_j} \\
&= (\widehat{\mu_{i,1}} - m \cdot \widehat{\mu_{j,1}})b_1^* + \cdots + (\widehat{\mu_{i,j}} - m)b_j^* + \widehat{\mu_{i,j+1}}b_{j+1}^* + \cdots + b_i^* \\
&= \widehat{\mu'_{i,1}}b_1^* + \cdots + \widehat{\mu'_{i,j}}b_j^* + \widehat{\mu'_{i,j+1}}b_{j+1}^* + \cdots + b_i^* \\
&\vdots \\
\widehat{b'_n} &= \widehat{b_n} \\
&= \widehat{\mu_{n,1}}b_1^* + \cdots + \widehat{\mu_{n,n-1}}b_{n-1}^* + b_n^* \\
&= \widehat{\mu'_{n,1}}b_1^* + \cdots + \widehat{\mu'_{n,n-1}}b_{n-1}^* + b_n^*.
\end{aligned}$$

Now, let (i', j') be the lexicographically largest pair of indices satisfying the following conditions:

$$\begin{aligned}
|\widehat{\mu'_{i',j'}}| &> \frac{1}{2}, \text{and} \\
|\widehat{\mu'_{k,l}}| &\leq \frac{1}{2}, \text{ for all } k,l \text{ such that } (k > i') \text{ or } (k = i' \wedge l > j').
\end{aligned}$$

It is easy to see that

$$(i', j') <_{\text{lex}} (i, j).$$

It is also easy to see that $(\widehat{b_1}, \widehat{b_2}, \ldots, \widehat{b_n})$ and $(\widehat{b'_1}, \widehat{b'_2}, \ldots, \widehat{b'_n})$ have the same Gram-Schmidt orthogonalization: $(b_1^*, b_2^*, \ldots, b_n^*)$.

Hence by repeating above step at most $\binom{n}{2}$ many times, it is possible to obtain a weakly reduced basis $(\overline{b_1}, \overline{b_2}, \ldots, \overline{b_n})$, starting from the original basis $(b_1, b_2, \ldots, b_n)$. The following algorithm achieves this:

Procedure *WEAK-BASIS-REDUCTION*;

INPUT: $(b_1, \ldots, b_n)$: Basis of an n-dimensional lattice Λ, and
$(b_1^*, \ldots, b_n^*) = GRAM\text{-}SCHMIDT(b_1, \ldots, b_n)$
OUTPUT: $(\overline{b_1}, \ldots, \overline{b_n})$: A weakly reduced basis of Λ;

```
begin
    for i := n down to 2 loop
        for j := i − 1 down to 1 loop
            b_i := b_i − ⌈⟨b_i, b_j^*⟩ / ⟨b_j^*, b_j^*⟩⌋ · b_j
        end{loop };
    end{loop };
end{WEAK-BASIS-REDUCTION}. □
```

The above discussion can be summarized in the following theorem:

Theorem 6.1 *1. Let $(b_1, b_2, \ldots, b_n)$ be any basis of an n-dimensional lattice Λ and $(b_1^*, b_2^*, \ldots, b_n^*)$ be its Gram-Schmidt orthogonalization. Then there is another basis $(\overline{b_1}, \overline{b_2}, \ldots, \overline{b_n})$ with the same orthogonalization $(b_1^*, b_2^*, \ldots, b_n^*)$ such that if we write*

$$\overline{b_i} = \sum_{j=1}^{i} \overline{\mu_{i,j}} b_j^*, \qquad (i = 1, \ldots, n)$$

then $|\overline{\mu_{i,j}}| \leq \frac{1}{2}$ for $1 \leq j < i \leq n$.

2. Hence

$$\begin{aligned} \|\overline{b_i}\|^2 &= \|b_i^*\|^2 + \sum_{j=1}^{i-1} \overline{\mu_{i,j}}^2 \|b_j^*\|^2 \\ &\leq \|b_i^*\|^2 + \frac{1}{4} \sum_{j=1}^{i-1} \|b_j^*\|^2. \end{aligned}$$

3. A weakly reduced basis of Λ as above can be found in $O(n^2)$ arithmetic operations.

Notice that in the absence of any restriction on the relative sizes of the vectors b_i^*'s, the weakly reduced basis can have arbitrarily large orthogonality defect. But if it is known a priori, for instance, that

$$\|b_{i+1}^*\|^2 \geq \frac{1}{2} \|b_i^*\|^2, \qquad \text{for all } i = 1, \ldots, n-1$$

then we know that

$$\|b^*_{i-j}\|^2 \leq 2^{j+1}\|b^*_{i+1}\|^2, \qquad \text{for all } j = 0, \ldots, i-1.$$

Hence, for $i = 1, \ldots, n-1$

$$\begin{aligned} \|\overline{b_{i+1}}\|^2 &\leq \|b^*_{i+1}\|^2 + \frac{1}{4}\sum_{j=0}^{i-1}\|b^*_{i-j}\|^2 \\ &\leq \|b^*_{i+1}\|^2 + \frac{1}{4}\sum_{j=0}^{i-1}2^{j+1}\|b^*_{i+1}\|^2 \\ &\leq 2^i\|b^*_{i+1}\|^2, \end{aligned}$$

and

$$\|\overline{b_1}\|^2 = \|b^*_1\|^2.$$

From which we conclude that

$$\prod_{i=1}^{n}\|\overline{b_i}\|^2 \leq 2^{\binom{n}{2}}\prod_{i=1}^{n}\|b^*_i\|^2.$$

In other word the orthogonality defect of $(\overline{b_1}, \overline{b_2}, \ldots, \overline{b_n})$ is

$$\frac{\|\overline{b_1}\|\cdots\|\overline{b_n}\|}{\det\Lambda} \leq 2^{\frac{1}{2}\binom{n}{2}}.$$

Procedure *LLL-BASIS-REDUCTION*;

INPUT: $(b_1, \ldots, b_n)$: Basis of an n-dimensional lattice Λ;
OUTPUT: $(b'_1, \ldots, b'_n)$: A reduced basis of Λ;

```
begin
    loop
        (b*_1, ..., b*_n) := GRAM-SCHMIDT(b_1, ..., b_n)
        (b_1, ..., b_n) := WEAK-BASIS-REDUCTION (b_1, ..., b_n)
        if for some i ∈ {1, ..., n-1}, ||b*_{i+1}||^2 < (1/2)||b*_i||^2 then   ···(*)
            (b_i, b_{i+1}) := (b_{i+1}, b_i)
        else
            exit loop
        end{if }
    end{loop };
end{LLL-BASIS-REDUCTION}.  □
```

It is easy to see that when the algorithm terminates with a set of vectors $(b'_1, \ldots, b'_n)$, these indeed form a basis, since they ar obtained via a sequence of weak-basis-reduction operations and interchange of two of the basis vectors—all integer unimodular transformations. Furthermore, at termination they satisfy the following condition

$$\|b'^*_{i+1}\|^2 \geq \frac{1}{2}\|b'^*_i\|^2, \qquad \text{for all } i = 1, \ldots, n-1,$$

and hence they form a reduced basis.

What is not clear, from the above discussion, is that the algorithm terminates, and in fact in polynomial time. For the sake of simplicity, let us assume that the original basis vector of the lattice are all integer vectors.

To this end, let us consider the following quantities:

$$\begin{aligned} V_i &= \sqrt{\det\,(b_1, \ldots, b_i)^{\mathrm{T}}\,(b_1, \ldots, b_i)} \\ &= \|b^*_1\| \cdots \|b^*_i\|, \end{aligned}$$

the i-volume of the parallelohedra spanned by the vectors $b_1, \ldots, b_i$.

Let us define the weight function

$$\begin{aligned} D &= D(b_1, \ldots, b_n) \\ &= V_1 V_2 \cdots V_n \\ &= \prod_{i=1}^{n} \|b^*_i\|^{n-i} \\ &\leq (\max_i \|b_i\|)^{\binom{n}{2}}. \end{aligned}$$

Furthermore,

$$D(b_1, \ldots, b_n) \geq 1,$$

since the basis vectors are assumed to be integer vectors.

It is obvious that the weak-basis-reduction step does not change D. However, if in any step b_{i+1} and b_i are swapped changing the value of the weight function from D to D' then we see that

1. $V_1, \ldots, V_{i-1}, V_{i+1}, \ldots, V_n$ remain uncahnged.

2. V_i changes to a new value

$$\begin{aligned} &\sqrt{\det\,(b_1, \ldots, b_{i-1}, b_{i+1})^{\mathrm{T}}\,(b_1, \ldots, b_{i-1}, b_{i+1})} = \\ &\qquad \|b^*_1\| \cdots \|b^*_{i-1}\|\ \|b^*_{i+1} + \mu_{i+1,i} b^*_i\|. \end{aligned}$$

where $b_{i+1}^* + \mu_{i+1,i} b_i^* = b_{i+1}(i)$ is the component of b_{i+1} orthogonal to span $(b_1, \ldots, b_{i-1})$.

Hence

$$\begin{aligned}
\frac{D}{D'} &= \frac{\sqrt{\det(b_1, \ldots, b_{i-1}, b_i)^{\mathrm{T}}(b_1, \ldots, b_{i-1}, b_i)}}{\sqrt{\det(b_1, \ldots, b_{i-1}, b_{i+1})^{\mathrm{T}}(b_1, \ldots, b_{i-1}, b_{i+1})}} \\
&= \left(\frac{\|b_i^*\|^2}{\|b_{i+1}^*\|^2 + \mu_{i+1,i}^2 \|b_i^*\|^2} \right)^{\frac{1}{2}} \\
&> \left(\frac{\|b_i^*\|^2}{\frac{1}{2}\|b_i^*\|^2 + \frac{1}{4}\|b_i^*\|^2} \right)^{\frac{1}{2}} \\
&= \frac{2}{\sqrt{3}}. \qquad (2)
\end{aligned}$$

Hence, the number of swap operations in the LLL-Basis-Reduction is bounded by a number p, where p satisfy the following inequalities:

$$1 \leq D(b_1', \ldots, b_n') \leq \left(\frac{\sqrt{3}}{2}\right)^p D(b_1, \ldots, b_n) \leq \left(\frac{\sqrt{3}}{2}\right)^p (\max_i \|b_i\|)^{\binom{n}{2}}.$$

Hence, we obtain the following bound on p

$$\begin{aligned}
p &\leq \cdot \binom{n}{2} \log_{2/\sqrt{3}}(\max_i \|b_i\|) \\
&= O(n^2 \ell(B)).
\end{aligned}$$

Since each loop performs $O(n^2)$ arithmetic operations in weak-basis-reduction and $O(n^3)$ time in Gram-Schmidt orthogonalization, the time complexity of the algorithm is

$$T_{\text{arith}}(n, \ell(B)) = O(n^5 \ell(B)).$$

We summarize the above results in the following theorem:

Theorem 6.2 *1. Given a non-singular matrix $B = (b_1, b_2, \ldots, b_n) \in \mathbf{Q}^{n \times n}$, a reduced basis $(b_1', b_2', \ldots, b_n')$ of $\Lambda = \Lambda(B)$ can be found in polynomial time, such that*

$$\|b_1'\| \cdots \|b_n'\| \leq 2^{\frac{1}{2}\binom{n}{2}} \det \Lambda.$$

2. *Let b'_1 be the shortest among the vectors $b'_1, b'_2, \ldots b'_n$. Then*
   (a) $\|b'_1\| \leq 2^{(n-1)/4}\sqrt[n]{\det \Lambda}$, *and*
   (b) $\|b'_1\| \leq 2^{(n-1)/2}\xi_1$.

   Hence a short non-zero vector of the lattice can be found in polynomial time.

PROOF.

1. This follows from the previous discussion.
2. $$\begin{aligned} \|b'^*_i\|^2 &\geq 2^{1-i}\|b'^*_1\|^2 = 2^{1-i}\|b'_1\|^2. \\ \|b'_1\|^{2n} &\leq 2^{n(n-1)/2}\prod_{i=1}^{n}\|b'^*_i\|^2 \\ &= 2^{\binom{n}{2}}(\det \Lambda)^2. \end{aligned}$$

   Hence
   $$\|b'_1\| \leq 2^{(n-1)/4}\sqrt[n]{\det \Lambda}.$$

   The second inequality follows from the following two facts:

   - For each $i = 1, \ldots, n$,
     $$\|b'^*_i\|^2 \geq 2^{1-i}\|b'_1\|^2.$$
     i.e.
     $$\begin{aligned} \|b'_1\|^2 &\leq \min_i\{2^{i-1}\|b'^*_i\|^2\} \\ &\leq 2^{n-1}\min_i\|b'^*_i\|^2. \end{aligned}$$
     In other words,
     $$\|b'_1\| \leq 2^{(n-1)/2}\min_i\|b'^*_i\|.$$
   - By equation 1,
     $$\min_i\|b'^*_i\| \leq \xi_1.$$

□

Remark 6.1 Recall that $b_i(j)$ had been defined previously to denote the component of b_i orthogonal to the linear space spanned by the first $j-1$ vectors $b_1, b_2, \ldots, b_{j-1}$. As a result, the condition

$$\frac{1}{2}\|b_i^*\|^2 \leq \|b_{i+1}^*\|^2$$

can be shown to be implied by the weaker condition

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

since

$$\begin{aligned}\|b_i^*\|^2 = \|b_i(i)\|^2 &\leq \frac{4}{3}\|b_{i+1}(i)\|^2 \\ &= \frac{4}{3}\|b_{i+1}^*\|^2 + \frac{4}{3}\mu_{i+1,i}^2\|b_i^*\|^2 \\ &\leq \frac{4}{3}\|b_{i+1}^*\|^2 + \frac{1}{3}\|b_i^*\|^2.\end{aligned}$$

Hence, the if -condition (marked by the $(*)$) in the *LLL-BASIS-REDUCTION*-algorithm can be replaced by the following,

if for some $i \in \{1, \ldots, n-1\}$, $\|b_i(i)\|^2 > \frac{4}{3}\|b_{i+1}(i)\|^2$ then
$\vdots$

Also notice that, for this modified algorithm the complexity analysis remains unchanged, since the equation 2 holds with

$$\begin{aligned}\frac{D}{D'} &= \left(\frac{\|b_i(i)\|}{\|b_{i+1}(i)\|}\right) \\ &> \frac{2}{\sqrt{3}}.\end{aligned}$$

We note that the standard definition of a *Reduced Basis* (L^3-Reduced Basis) is based on this modified algorithm:

Definition 6.2 A basis $(b_1, b_2, \ldots, b_n)$ of a lattice Λ is called *reduced* if it is weakly rdeuced and

$$\|b_i(i)\|^2 \leq \frac{4}{3}\|b_{i+1}(i)\|^2 \quad \text{for } 1 \leq i < n.$$

Remark 6.3 The algorithms *WEAK-BASIS-REDUCTION* and *LLL-BASIS-REDUCTION* are usually combined into the following algorithm:

Procedure *LLL-BASIS-REDUCTION*;

INPUT: $(b_1, \ldots, b_n)$: Basis of an n-dimensional lattice Λ;
OUTPUT: $(b'_1, \ldots, b'_n)$: A reduced basis of Λ;

```
begin
i := 1
while i < n loop
      (b*_1, ..., b*_n) := GRAM-SCHMIDT(b_1, ..., b_n)
      b_{i+1} := b_{i+1} - [μ_{i+1,i}] · b_i
      if ||b_i(i)||^2 > (4/3)||b_{i+1}(i)||^2 then
            (b_i, b_{i+1}) := (b_{i+1}, b_i)
            if i > 1 then i := i - 1 end{if }
      elsif ||b_i(i)||^2 ≤ (4/3)||b_{i+1}(i)||^2 then
            for j := i - 1 down to 1 loop
                  b_{i+1} := b_{i+1} - [μ_{i+1,j}] · b_j
            end{loop }
            i := i + 1
      end{if }
end{loop }
end{LLL-BASIS-REDUCTION}.  □
```

In the above algorithm $\mu_{j,k}$ denotes

$$\frac{\langle b_j, b_k^* \rangle}{\langle b_k^*, b_k^* \rangle}$$

The correctness of the above algorithm follows from the fact that the following loop invariant is satisfied by the main loop:

For each i $(1 \leq i \leq n)$,

$$\begin{aligned} |\mu_{jk}| &\leq \frac{1}{2}, \quad \text{for } 1 \leq k < j \leq i, \\ \|b_j(j)\|^2 &\leq \frac{4}{3}\|b_{j+1}(j)\|^2, \quad \text{for } 1 \leq j < i. \end{aligned}$$

The above algorithm is the usual *LLL-BASIS-REDUCTION* algorithm found in the literature, and is somewhat more efficient (only in terms of the constants) than the algorithm previously presented.

Remark 6.4 By keeping track of the Gram-Schmidt orthogonalizations, the time complexity of the previous algorithm can be improved to

$$T_{\text{arith}}(n, \ell(B)) = O(n^3) + O(n^4\ell(B)) = O(n^4\ell(B)).$$

In order to achieve this time complexity, we only orthogonalize the initial b_j's and then keep track of the scalars $\|b_j^*\|^2$ and μ_{jk}, updating them after each change in the b_j's. Each update can be achieved with only $O(n)$ arithmetic (i.e. rational) operations. Hence the initial Gram-Schmidt computation takes $O(n^3)$ time and the sequence of updates per iteration takes $O(n^2)$ time. The overall complexity of the algorithm is easily seen to be as claimed.

Note that in the algorithm we perform the following two kinds of update operations:

1. $\boxed{b_{i+1} := b_{i+1} - [\mu_{i+1,j}] \cdot b_j}$

and

2. $\boxed{(b_i, b_{i+1}) := (b_{i+1}, b_i)}$

Let b_i' and μ_{ij}' be the updated values of b_i and μ_{ij}, respectively. Then

1. In case of the first kind of update:

$$b_{i+1}' = b_{i+1} - [\mu_{i+1,j}]b_j.$$

Hence

$$\begin{aligned} \|b_{i+1}'^*\|^2 &= \|b_{i+1}^*\|^2, \quad \text{and} \\ \mu_{i+1,k}' &= \frac{\langle b_{i+1}', b_k^* \rangle}{\langle b_k^*, b_k^* \rangle} = \mu_{i+1,k} - [\mu_{i+1,j}]\mu_{j,k}. \end{aligned}$$

2. In case of the second kind of update:

$$b_i' = b_{i+1}, \quad b_{i+1}' = b_i.$$

Observe that

$$\begin{aligned} \|b_i'^*\|^2\|b_{i+1}'^*\|^2 &= \|b_i^*\|^2\|b_{i+1}^*\|^2, \\ b_i'^* &= b_{i+1}^* + \mu_{i+1,i}b_i^*, \\ b_{i+1}'^* &= \frac{\|b_{i+1}^*\|^2}{\|b_i'^*\|^2}b_i^* - \mu_{i+1,i}\frac{\|b_i^*\|^2}{\|b_i'^*\|^2}b_{i+1}^*, \end{aligned}$$

Hence

$$\begin{aligned}
\|b_i'^*\|^2 &= \|b_{i+1}^*\|^2 + \mu_{i+1,i}^2\|b_i^*\|^2, \\
\|b_{i+1}'^*\|^2 &= \frac{\|b_i^*\|^2}{\|b_i'^*\|^2}\|b_{i+1}^*\|^2, \\
\mu'_{i+1,i} &= \frac{\langle b_i, b_i'^*\rangle}{\langle b_i'^*, b_i'^*\rangle} = \mu_{i+1,i}\frac{\|b_i^*\|^2}{\|b_i'^*\|^2}, \\
\text{For } 1 \le j < i & \\
\mu'_{ij} &= \frac{\langle b_{i+1}, b_j^*\rangle}{\langle b_j^*, b_j^*\rangle} = \mu_{i+1,j}, \\
\mu'_{i+1,j} &= \frac{\langle b_i, b_j^*\rangle}{\langle b_j^*, b_j^*\rangle} = \mu_{ij}, \\
\text{For } i+1 < j \le n & \\
\mu'_{ji} &= \frac{\langle b_j, b_i'^*\rangle}{\langle b_i'^*, b_i'^*\rangle} \\
&= \mu_{j,i+1} + \mu'_{j,i+1}\mu'_{i+1,i}, \\
\mu'_{j,i+1} &= \frac{\langle b_j, b_{i+1}'^*\rangle}{\langle b_{i+1}'^*, b_{i+1}'^*\rangle} \\
&= \mu_{ji} - \mu_{j,i+1}\mu_{i+1,i}.
\end{aligned}$$

Only $O(n^2)$ arithmetic operations are required to make the appropriate modifications, presented in the above set of equations.

Remark 6.5 Note that our presentation of the LLL-Basis-Reduction algorithm can be modified so that all the intermediate results have at most $O(n\ell(B))$ bits. Using standard algorithms for arithmetic operations, we see that the algorithm has a bit-complexity of

$$T_{\text{bit}}(n, \ell(B)) = O(n^6\ell(B)^3).$$

Furthermore, if we use fast-multiplication algorithm, then for any $\epsilon > 0$, we can achieve a bit-complexity of

$$T_{\text{bit}}(n, \ell(B)) = O(n^{5+\epsilon}\ell(B)^{2+\epsilon}).$$

However, this improvement is mostly of theoretical interest, since for almost all practical problems, the straight forward algorithm is good enough.

7 Two-Dimensional Lattices

It is somewhat instructive to look at *LLL-BASIS-REDUCTION* algorithm carefully for the special case of two dimensional lattices. The algorithm for the special case is as follows

Procedure *LLL-BASIS-REDUCTION*;

INPUT: (b_1, b_2): Basis of an 2-dimensional lattice Λ;
OUTPUT: (b'_1, b'_2): A reduced basis of Λ;

```
begin
    loop
        b_2 := b_2 - ⌈⟨b_2, b_1⟩ / ⟨b_1, b_1⟩⌋ · b_1

        if ||b_1||^2 > (4/3)||b_2||^2 then    ···(**)
            (b_1, b_2) := (b_2, b_1)
        else
            exit loop
        end{if }
    end{loop };
end{LLL-BASIS-REDUCTION}. □
```

The correctness and polynomial time complexity of the above algorithm follows from the general results. However it is also known that if the step, marked $(**)$ is replaced by

```
if ||b_1||^2 > ||b_2||^2 then
    ⋮
```

then the time complexity of the modified algorithm can be shown to be also polynomial, and the resulting reduced basis, superior. Notice that if the algorithm terminates with the basis (b_1, b_2) then

$$|\cos\phi(b_1, b_2)| = \frac{|\langle b_2, b_1\rangle|}{\|b_2\|\|b_1\|} \leq \frac{1}{2}\frac{\|b_1\|}{\|b_2\|} \leq \frac{1}{2}.$$

hence the basis vectors form an acute angle of 60° or more. For this reason this modified algorithm is known as the "60°-algorithm." This algorithm is usually attributed to Gauss [Gauss 1801] and has a close similarity to Euclid's algorithm for GCD of two numbers.

The orthogonality defect of the basis produced by the 60° algorithm is

$$\delta = \frac{\|b_1\|\|b_2\|}{\det \Lambda} = \frac{1}{\sin \phi(b_1, b_2)} \leq \sqrt{\frac{4}{3}}.$$

This bound is optimally achieved by a lattice of an equilateral triangle with a vertex at the origin. Furthermore, it can be shown that if (b_1, b_2) is a basis of the lattice Λ produced by the 60° algorithm (with $\|b_1\| \leq \|b_2\|$) then $b - 1$ is a shortest nonzero vector of Λ.

Gauss' algorithm originally motivated the development of the more general polynomial time algorithm for higher dimensional lattices, and hence of historical importance. It is not known, however, if the factor 4/3 can be replaced by 1 in the more general *LLL-BASIS-REDUCTION* algorithm (as in the case of two-dimensional lattices) without sacrificing the polynomial time complexity of the algorithm.

References

[Cassels 1959] J. W. S. Cassels, *An Introduction to the Geometry of Numbers*, **Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen**, Vol. 99, Springer-Verlag, Heidelberg, 1959.

[Gauss 1801] C. F. Gauss, *Disquisitiones Arithmaticae*, **apud Gerh.Fleischer**, Lipsiae 1801.

[Kannan 1984] R. Kannan, "*Lattices, Basis Reduction and the Shortest Vector Problem*," **Colloquia Mathematica Societatis János Bolyai**, 44, Theory of Algorithms, Pécs, Hungary 1984.

[Lekkerkerker 1969] C. G. Lekkerkerker, *Geometry of Numbers*, **Bibliotheca mathematica**, Vol. 8, Wolters-Noordhoff Publishing and North-Holland Publishing Company, 1969.

[Lenstra et. al. 1982] A. K. Lenstra, H. W. Lenstra and L. Lovász, "*Factoring Polynomials with Rational Coefficients*," **Mathematische Annalen**, Vol. 261, 513–534, 1982

[Lovász 1984] L. Lovász, "*Some Algorithmic Problems in Lattices*," **Colloquia Mathematica Societatis János Bolyai**, 44, Theory of Algorithms, Pécs, Hungary 1984.

[Lovász 1984] L. Lovász, *An Algorithmic Theory of Numbers Graphs and Connectivity*, **50, CBMS-NSF, Regional Conference Series in applied Mathematics**, Society for Industrial and Applied Mathematics, Philadelphia, Pennsylvania, 1986.

[Petkovšek 1985] M. Petkovšek, *Reduction Algorithms for Lattices and Quadratic Forms*, Carnegie-Mellon University, Pittsburgh, June 1985.