On LLL lattice basis reduction over imaginary quadratic fields by introducing reduction parameters

Koichi Arimoto
Kurashiki City Gonai Junior High School
Okayama 710–0142, Japan
email: te27212@kurashiki.oky.ed.jp

(Received December 1, 2019, Accepted January 2, 2020)

Abstract

The author has generalized the LLL reduction algorithm so that it can be applied to obtain a LLL reduced basis over imaginary quadratic field by introducing a reduction parameter. The termination of the generalized algorithm is guaranteed by showing that a quantity which strictly decreases during the execution of the algorithm has a positive lower bound.

1 Introduction

In 1982, Lenstra et al. presented the LLL reduction algorithm [7]. It was meant to find "short" vectors in lattices, i.e. to determine a so called reduced basis for a given lattice. Arimoto and Hirano generalized the LLL basis reduction over imaginary quadratic fields([3]). However, the existence of an LLL reduced basis remains an open question in the generalized case. In the paper [2], we considered the conditions under which this reduced basis always existed, and modified the definition of an LLL reduced basis in the case of the Gaussian number field \( \mathbb{Q}(\sqrt{-1}) \). In the paper [1] we defined a quasi LLL reduced basis, and proved the existence of the basis by indicating that the algorithm is guaranteed by showing that there exists a quantity \( D \)

Key words and phrases: basis reduction, LLL-algorithm, imaginary quadratic fields, quadratic forms.

AMS (MOS) Subject Classifications: Primary 11E04, 11R04; Secondary 11Y40.

ISSN 1814-0432, 2020, http://ijmcs.future-in-tech.net
which strictly decreases during the execution of the LLL algorithm and has a positive lower bound.

In this paper, we generalize a LLL reduced basis reduction over imaginary quadratic fields whose ring of the integers are principal ideal domain by introducing the reduction parameter.

2 LLL reduced basis over Gaussian number fields

In this section, we state the definition of LLL reduced basis over an imaginary quadratic field defined by Arimoto [1, 2].

Let $F$ be an imaginary quadratic field and $\mathcal{O}_F$ the ring of integers in $F$. Let $n$ be a positive integer, we consider a lattice in the $n$-dimensional linear space $V = F^n$.

For given an imaginary quadratic field $\mathbb{Q}(\sqrt{m}) := \{a + b\sqrt{m} \mid a, b \in \mathbb{Q}\}$, where $m$ is a square free negative integer, $\mathcal{O}_F$ the ring of integers in $\mathbb{Q}(\sqrt{m})$ is the following:

(i) If $m \not\equiv 1 \pmod{4}$, then $\mathcal{O}_F = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\},$
(ii) If $m \equiv 1 \pmod{4}$, then $\mathcal{O}_F = \left\{a + b \cdot \frac{1 + \sqrt{m}}{2} \mid a, b \in \mathbb{Z}\right\}.$

A subset $\Lambda$ of $V$ is called an $\mathcal{O}_F$-lattice if there exists an $\mathcal{O}_F$-basis $b_1, \ldots, b_n$ of $V$ such that

$$\Lambda = \sum_{i=1}^{n} \mathcal{O}_F b_i = \left\{ \sum_{i=1}^{n} r_i b_i \mid r_i \in \mathcal{O}_F \ (1 \leq i \leq n) \right\}.$$ 

For an $\mathcal{O}_F$-basis $b_1, \ldots, b_n$ of $\Lambda$ the discriminant $d(\Lambda)$ of $\Lambda$ is defined by

$$d(\Lambda) = \sqrt{\left| \det(b_i, b_j) \right|_{1 \leq i, j \leq n}}. \hspace{1cm} (2.1)$$

Suppose that $a = (a_1, \ldots, a_n), b = (b_1, \ldots, b_n)$ are vectors in $F^n$. The Hermitian inner product of $a$ and $b$ is defined by

$$(a, b) = a_1 \bar{b}_1 + \cdots + a_n \bar{b}_n, \hspace{1cm} (2.2)$$

where $\bar{b}_i$ is a conjugate of $b_i$.

Suppose that $x = (x_1, \ldots, x_n)$ is a vector in $F^n$. The norm of $x$ is defined by

$$\|x\| = \sqrt{(x, x)} = \sqrt{|x_1|^2 + \cdots + |x_n|^2}, \hspace{1cm} (2.3)$$
where, $x_i \in F$ is the $i$-th coordinate of $x$, and $\|x\| \in \mathbb{R}$.

Let $b_1, \ldots, b_n \in F^n$ be linearly independent. We recall the Gram-Schmidt orthogonalization process. The vectors $b_i^*(1 \leq i \leq n)$ and the complex numbers $\mu_{ij}(1 \leq j < i \leq n)$ are inductively defined by

\begin{align*}
    b_i^* &:= b_i - \sum_{j=1}^{i-1} \mu_{ij}b_j^*, \\
    \mu_{ij} &:= \frac{(b_i, b_j^*)}{(b_j^*, b_j^*)},
\end{align*}

(2.4)

(2.5)

where $(\ , \ )$ denotes the Hermitian inner product on $\mathbb{C}^n$ defined by (2.2). We call a basis $b_1, \ldots, b_n$ for a lattice LLL reduced if it satisfies

\begin{equation}
    |\mu_{ij}| \leq \sqrt{\frac{2}{2}} \quad \text{for } 1 \leq j < i \leq n,
\end{equation}

(2.6)

and

\begin{equation}
    \|b_i^*\|^2 \geq \left( \frac{3}{4} - |\mu_{i,i-1}|^2 \right) \|b_{i-1}^*\|^2 \quad \text{for } 1 < i \leq n.
\end{equation}

(2.7)

The constant $\frac{3}{4}$ in (2.7) is arbitrarily chosen, and may be replaced by any fixed real number $\alpha$ with $\frac{1}{4} < \alpha < 1$. We call a parameter $\alpha$ reduction parameter.

\section{LLL reduction over imaginary quadratic fields}

In the case of the rational integers $\mathbb{Z}$, the distance to an arbitrary real number is less than or equal to $\frac{1}{2}$. But in the case of the ring of integers in an imaginary quadratic field $\mathbb{Q}(\sqrt{m})$, where $m$ is a square free negative integer, the situation is different. In case $m \not\equiv 1 \pmod{4}$, the distance to an arbitrary complex number is less than $\sqrt{\frac{1-m}{2}}$. In case $m \equiv 1 \pmod{4}$, the distance to an arbitrary complex number is less than $\sqrt{\frac{9-m}{4}}$

\subsection{Definition of LLL reduced bases}

Let $F$ be an imaginary quadratic field $\mathbb{Q}(\sqrt{m})$, and $\mathcal{O}_F$ be the ring of integers in $F$. We call a basis $b_1, \ldots, b_n$ for a lattice LLL reduced with parameter $\alpha$ if it satisfies in case of $m \not\equiv 1 \pmod{4}$,

\begin{equation}
    |\mu_{ij}| \leq \frac{\sqrt{1-m}}{2} \quad \text{for } 1 \leq j < i \leq n,
\end{equation}

(3.8)
and
\[ \| b^*_i + \mu_{i,i-1} b^*_{i-1} \| \geq \alpha \| b^*_i \| \quad \text{for } 1 < i \leq n. \] (3.9)

In case of \( m \equiv 1 \) (mod 4),
\[ |\mu_{ij}| \leq \frac{\sqrt{9-m}}{4} \quad \text{for } 1 \leq j < i \leq n, \] (3.10)
and (3.9).

### 3.2 On the termination of the algorithm

We explain the underlying ideas due to [7]. At the start the constants \( \mu_{ij} \) and the orthogonal basis vectors \( b^*_i \) are calculated by (2.4) and (2.5). Then a LLL reduced basis is constructed inductively. The induction is on the number of reduced basis vectors. The initial value of the induction parameter is \( m = 2 \), in case of \( m > n \) the procedure terminates. In case of \( m \not\equiv 1 \) (mod 4) there are three major steps. In case of \( m \equiv 1 \) (mod 4), replace \( \sqrt{\frac{1-m}{2}} \) by \( \sqrt{\frac{9-m}{4}} \).

(A) By subtracting a suitable scalar multiple of \( b_{m-1} \) from \( b_m \), reduce \( \mu_{m,m-1} \) so that \( |\mu_{m,m-1}| \leq \sqrt{\frac{1-m}{2}} \). All \( b^*_i \) remain unchanged.

If \( |\mu_{m,m-1}| > \sqrt{\frac{1-m}{2}} \), set \( r \leftarrow \{\mu_{m,m-1}\} \), \( b_m \leftarrow b_m - rb_{m-1}, \mu_{m,m-1} \leftarrow \mu_{m,m-1} - r \), where \( \{x\} \) denotes one of the integers of \( F \) closest to \( x \). Therefore \( \sqrt{\frac{1-m}{2}} \geq |\mu_{m,m-1} - r| \).

(B) If (3.9) holds for \( i = m \) proceed to (C), else interchange \( b_{m-1} \) and \( b_m \). In case \( m > 2 \) also replace \( m \) by \( m - 1 \). Then go on with (A).

(C) For \( j = m - 2, m - 3, \ldots, 1 \), reduce \( \mu_{mj} \) so that \( |\mu_{mj}| \leq \frac{\sqrt{1-m}}{2} \) (similar to (A)). Then increase \( m \) by 1. For \( m > n \) terminate, else go on with (A).

We briefly explain the reason for the termination. Let
\[ D_i := \det(b_\mu, b_\nu)_{1 \leq \mu, \nu \leq i} \quad (1 \leq i \leq n) \] (3.11)
and
\[ D := \prod_{j=1}^{n} D_j. \]
Because of (2.4) and (2.5), we also have

$$D_i = \prod_{j=1}^{i} \|b_j^*\|^2 \ (1 \leq i \leq n).$$

Each time \(b_{n-1}\) and \(b_m\) are interchanged in (B) the value \(D_{m-1}\) is diminished by a factor \(\alpha(\frac{1}{2} < \alpha < 1)\) whereas all other \(D_i\) remain unchanged. Hence, \(D\) also decreases by a factor \(\alpha\). It is proved that if \(F\) is an imaginary quadratic field, then the ring of integers \(O_F\) has a least element in [3, Theorem 4.4]. This clearly shows that there is a positive lower bound for \(D\).

Using this fact, the quantity \(D\) is proved to strictly decrease during the execution of the algorithm and to have a positive lower bound. Therefore, the algorithm terminates after a finite number of steps.

### 4 Explicit Lower Bound for the Square of Discriminant of Lattice

As shown in the previous section, we proved the existence of a positive lower bound for \(D\) to indicate the existence of a LLL reduced basis. We give another proof of the existence of a positive lower bound for \(D\) by constructing it explicitly using a minimum element of a lattice.

For a given \(O_F\)-lattice \(\Lambda = \sum_{i=1}^{n} O_F b_i\), with a basis \(b_1, \cdots, b_n\), we consider a Hermitian form \(f(x) = \sum_{1 \leq i, j \leq n} b_{ij} x_i \overline{x}_j\), with \(x = (x_1, \cdots, x_n) \in F^n\) and \(b_{ij} = (b_i, b_j)\), where \(\overline{x}_i\) is a conjugate of \(x_i\). For \(x \in \Lambda\), with \(x = x_1 b_1 + \cdots + x_n b_n\), we can easily see \(f(x) = \|x\|^2\). Therefore, \(f\) is positive definite.

We put

$$m(\Lambda) := \min \{\|x\|^2 \mid x \in \Lambda, x \neq 0\}.$$ 

In case of \(m \not\equiv 1\ (\text{mod} \ 4)\), let \(S_i = (\frac{4}{3+m})^{\frac{(1-i)}{2}} \cdot m(\Lambda)^i\), in case of \(m \equiv 1\ (\text{mod} \ 4)\), let \(S_i = (\frac{16}{7+m})^{\frac{(1-i)}{2}} \cdot m(\Lambda)^i\) and \(S = \prod_{i=1}^{n} S_i\). Then we get the following theorem.

**Theorem 4.1.**

$$0 < S \leq D.$$ 

For the proof, we generalize certain classical results of definite quadratic forms to imaginary quadratic fields. We need to consider a Hermitian form. Here we are concerned only with the minima of forms. We reveal an explicit
indication of a lower bound $S_n$ for $D_n$. The idea of the following statement and its proof are due to [1], [5].

By applying the properties of Hermitian inner product, and the basic property of absolute value in the complex number fields, we can easily get the following lemmas.

**Lemma 4.2.** Let

$$f(x_1, x_2) = b_{11}|x_1|^2 + b_{12}x_1\overline{x}_2 + b_{21}\overline{x}_1x_2 + b_{22}|x_2|^2$$

(4.12)

be a positive definite Hermitian form. Then we get

$$f(x_1, x_2) = b_{11} \left| x_1 + \frac{b_{21}}{b_{11}}x_2 \right|^2 + \frac{b_{11}b_{22} - |b_{12}|^2}{b_{11}} |x_2|^2.$$  

(4.13)

**Lemma 4.3.** Let $F$ be an imaginary quadratic field $\mathbb{Q}(\sqrt{m})$, and $\mathcal{O}_F$ be the ring of integers in $F$. For $\alpha \in F$, there exist $u \in \mathcal{O}_F$ such that in case of $m \not\equiv 1 \pmod{4}$,

$$|u + \alpha| \leq \frac{\sqrt{1 - m}}{2},$$

in case of $m \equiv 1 \pmod{4}$,

$$|u + \alpha| \leq \frac{\sqrt{9 - m}}{4}.$$ 

By these lemmas we get the following lemma.

**Lemma 4.4.** Let $f$ be a positive definite Hermitian form given by (4.12). There exist $(u_1, u_2) \neq (0, 0)$ such that in case of $m \not\equiv 1 \pmod{4}$,

$$f(u_1, u_2) \leq \left( \frac{4}{3 + m} D_2 \right)^{\frac{1}{2}},$$

in case of $m \equiv 1 \pmod{4}$,

$$f(u_1, u_2) \leq \left( \frac{16}{7 + m} D_2 \right)^{\frac{1}{2}},$$

where

$$D_2 = b_{11}b_{22} - |b_{12}|^2.$$
Proof. We prove the case of \( m \not\equiv 1 \pmod{4} \). By taking an equivalent form, if it is necessary, we may suppose that

\[
M(f) = \inf_{u_1, u_2 \in \mathcal{O}_F} f(u_1, u_2) = b_{11},
\]

where \((u_1, u_2) \neq (0, 0)\), by the equality (4.13), we have

\[
f(x_1, x_2) = b_{11} \left| x_1 + \frac{b_{21}}{b_{11}} x_2 \right|^2 + \frac{D_2}{b_{11}} |x_2|^2.
\]

Put \( u_2 = 1 \). By Lemma 4.3 we can choose for a \( u_1 \in \mathcal{O}_F \) such that

\[
\left| u_1 + \frac{b_{21}}{b_{11}} \right| \leq \frac{\sqrt{1 - m}}{2}.
\]

Then, on the one hand,

\[
f(u_1, 1) \geq b_{11},
\]

and on the other hand,

\[
f(u_1, 1) \leq \frac{1 - m}{4} b_{11} + \frac{D_2}{b_{11}}.
\]

We get

\[
\frac{D_2}{b_{11}} \geq \frac{3 + m}{4} b_{11},
\]

that is

\[
b_{11}^2 \leq \frac{4}{3 + m} D_2,
\]

as required. And by (4.14), we get \( f(u_1, u_2) \leq \left( \frac{4}{3 + m} D_2 \right)^{1/2} \).

This argument can be extended to prove the following proposition.

**Proposition 4.5.** A positive definite Hermitian form

\[
f(x) = \sum_{1 \leq i, j \leq n} b_{ij} x_i \overline{x_j}
\]

represents a value \( f(u) \) with

\[
|f(u)| \leq \left( \frac{4}{3 + m} \right)^{\frac{n-1}{2}} D_n^{\frac{1}{2}},
\]

for any \( u \in \mathcal{O}_F^n, u \neq 0 \).
Proof. We may suppose, as in the proof of Lemma 4.4, that
\[ b_{11} \leq f(u) \]
for all integrals \( u \neq 0 \). Then
\[ f(x) = b_{11} \left| x_1 + \frac{b_{21}}{b_{11}} x_2 + \cdots + \frac{b_{n1}}{b_{11}} x_n \right|^2 + g(x_2, \ldots, x_n), \]
where \( g(x_2, \ldots, x_n) \) is a definite Hermitian form of determinant \( D_n/b_{11} \).

Since we may suppose the result already proved for forms in \( n-1 \) variables, there are integers \( u_2, \ldots, u_n \) not all 0 such that
\[ g(u_2, \ldots, u_n) \leq \left( \frac{4}{3 + m} \right)^{n-2} \left( \frac{D_n}{b_{11}} \right)^{-\frac{1}{n-1}}. \]

By Lemma 4.3, choose the integer \( u_1 \in \mathcal{O}_F \) so that
\[ \left| u_1 + \frac{b_{21}}{b_{11}} u_2 + \cdots + \frac{b_{n1}}{b_{11}} u_n \right| \leq \frac{\sqrt{1 - m}}{2}, \]
Then
\[ b_{11} \leq f(u) \leq \frac{1 - m}{4} b_{11} + \left( \frac{4}{3 + m} \right)^{n-2} \left( \frac{D_n}{b_{11}} \right)^{-\frac{1}{n-1}}, \]
and so
\[ b_{11} \leq \left( \frac{4}{3 + m} \right)^{\frac{1}{n}} D_n^{\frac{1}{n}}. \]

We indicate \( D_n = \{d(\Lambda)\}^2, d(\Lambda) \) is given by (2.1). In order to prove that \( D_n \) has a lower bound, \( m(\Lambda) \) is a positive real number. For \( i > 0 \), we can interpret \( D_i \) as the square of the discriminant of the \( \mathcal{O}_F \)-lattice of rank \( i \) spanned by \( b_1, \ldots, b_i \) in the vector space \( \sum_{j=1}^i F b_j \).

By Proposition 4, this lattice contains a nonzero vector \( x \) with \( \|x\|^2 \leq \left( \frac{4}{3 + m} \right)^{(n-1)/2} D_n^{1/n} \), therefore we get the theorem.

Acknowledgements. This work was supported by the Research Institute for Mathematical Sciences, a Joint Usage/Research Center located in Kyoto University.
References


