数理解析研究所講究録
第2051巻 2017年 9-13

A generalization of LLL lattice basis reduction over imaginary quadratic fields *

Koichi ARIMOTO[1] and Yasuyuki HIRANO[2]
[1]The Joint Graduate School (Ph.D. Program) in Science of School Education, Hyogo University of Teacher Education
[2]Naruto University of Education

1 Introduction

Among all the $\mathbb{Z}$ bases of a lattice, some are better than others. The ones whose elements are the shortest are called *reduced*. Since the bases all have the same discriminant, to be reduced implies also that a basis is not too far from being orthogonal.

In 1982 A.K.Lenstra, H.W.Lenstra, Jr., and L.Lovász presented the LLL reduction algorithm. It was originally meant to find "short" vectors in lattices, i.e. to determine a so called reduced basis for a given lattice. H.Napias generalized LLL reduction algorithm over euclidean rings or orders([3]).

In this paper we define LLL reduced basis over imaginary quadratic fields. We consider a lattice in the n-dimensional linear space $V = F^n$, so F is an imaginary quadratic field. F is included by the field of complex numbers. Lenstra, Lenstra, and Lovász showed some properties about reduced bases over real number fields. We proved these properties hold over imaginary quadratic fields.

2 Basis reduction on $\mathbb{Z}$-modules

We consider a lattice in n-dimensional linear space $\mathbb{R}^n$, where $\mathbb{R}$ is the field of real numbers.

A subset Λ of the n-dimensional real vector space $\mathbb{R}^n$ is called a *lattice* if there exists a basis $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n$ of $\mathbb{R}^n$ such that

$$\Lambda = \sum_{i=1}^{n} \mathbb{Z}\boldsymbol{b}_i = \left\{ \sum_{i=1}^{n} r_i\boldsymbol{b}_i \;\middle|\; r_i \in \mathbb{Z}\ (1 \leq i \leq n) \right\}.$$

*This paper is a preliminary version and a final version will be submitted to elsewhere.

In this situation we say that the set $\{\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n\}$ of vectors forms a basis for Λ, or that it spans Λ. We call n the *rank* of Λ.

For a $\mathbb{Z}$-basis $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n$ of Λ the *discriminant* $d(\Lambda)$ of Λ is defined by $d(\Lambda) = |\det(\boldsymbol{b}_i, \boldsymbol{b}_j)|^{\frac{1}{2}} \geq 0$, where $(\ ,\ )$ denotes the ordinary inner product on $\mathbb{R}^n$. This does not depend on the choice of the basis. And by Hadamard's inequality, we have $d(\Lambda) \leq \prod_{i=1}^n \|\boldsymbol{b}_i\|$.

In the sequel we consider the construction of special bases of lattices Λ. For the applications and for geometrical reasons we are interested in bases consisting of vectors of small norm. *Minkowski reduced* is an example of reduced basis. The computation of a Minkowski reduced basis of a lattice can be very time consuming. Hence, in many cases one is satisfied with constructing bases of lattices which are reduced in a much weaker sense. The most important reduction procedure now in use is LLL-reduction which was introduced in 1982 by Lenstra, Lenstra, and Lovász in a paper [2].

Let $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n \in \mathbb{R}^n$ be linearly independent. We recall the Gram-Schmidt orthogonalization process. The vectors $\boldsymbol{b}_i^* (1 \leq i \leq n)$ and the real numbers $\mu_{ij} (1 \leq j < i \leq n)$ are inductively defined by

$$\boldsymbol{b}_i^* := \boldsymbol{b}_i - \sum_{j=1}^{i-1} \mu_{ij} \boldsymbol{b}_j^*, \quad \mu_{ij} := \frac{(\boldsymbol{b}_i, \boldsymbol{b}_j^*)}{(\boldsymbol{b}_j^*, \boldsymbol{b}_j^*)},$$

where $(\ ,\ )$ denotes the ordinary inner product on $\mathbb{R}^n$. We call a basis $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n$ for a lattice *LLL-reduced* if

$$|\mu_{ij}| \leq \frac{1}{2} \quad \text{for } 1 \leq j < i \leq n \tag{1}$$

and

$$\|\boldsymbol{b}_i^* + \mu_{i,i-1} \boldsymbol{b}_{i-1}^*\|^2 \geq \frac{3}{4} \|\boldsymbol{b}_{i-1}^*\|^2 \quad \text{for } 1 < i \leq n \tag{2}$$

where $\|\cdot\|$ denotes the ordinary Euclidean length. Notice that the vectors $\boldsymbol{b}_i^* + \mu_{i,i-1} \boldsymbol{b}_{i-1}^*$ and $\boldsymbol{b}_{i-1}^*$ appearing in (2) are projections of $\boldsymbol{b}_i$ and $\boldsymbol{b}_{i-1}$ on the orthogonal complement of $\sum_{j=1}^{i-2} \mathbb{R}\boldsymbol{b}_j$. The constant $\frac{3}{4}$ in (2) is arbitrarily chosen, and may be replaced by any fixed real number y with $\frac{1}{4} < y < 1$.

We state without proof several key properties of LLL-reduced bases. The proof is given in [2].

Proposition 2.1 [2, Proposition(1.6), (1.11), (1.12)] *If $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n$ is some reduced basis for a lattice Λ in $\mathbb{R}^n$, then*

(i) $\|\boldsymbol{b}_j\|^2 \leq 2^{i-1} \|\boldsymbol{b}_i^*\|^2$ *for* $1 \leq j \leq i \leq n$,

(ii) $d(\Lambda) \leq \prod_{i=1}^n \|\boldsymbol{b}_i\| \leq 2^{n(n-1)/4} d(\Lambda)$,

(iii) $\|\boldsymbol{b}_1\| \leq 2^{(n-1)/4} d(\Lambda)^{1/n}$,

(iv) $\|\boldsymbol{b}_1\|^2 \leq 2^{n-1} \|\boldsymbol{x}\|^2$ *for every* $\boldsymbol{x} \in \Lambda, \boldsymbol{x} \neq \boldsymbol{0}$,

(v) For any linearly independent set of vectors $\boldsymbol{x}_1, \boldsymbol{x}_2, \cdots, \boldsymbol{x}_t \in \Lambda$ *we have* $\|\boldsymbol{b}_j\|^2 \leq 2^{n-1} \max\{\|\boldsymbol{x}_1\|^2, \cdots, \|\boldsymbol{x}_t\|^2\}$ *for* $1 \leq j \leq t \leq n$,

where $\|\cdot\|$ denotes the ordinary Euclidean length.

3 Basis reduction on $\mathcal{O}_F$-modules

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

Let n be a positive integer. A subset Λ of the n-dimensional vector space V is called a *$\mathcal{O}_F$-lattice* if there exists an $\mathcal{O}_F$-basis $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n$ of V such that

$$\Lambda = \sum_{i=1}^{n} \mathcal{O}_F \boldsymbol{b}_i = \left\{ \sum_{i=1}^{n} r_i \boldsymbol{b}_i \;\middle|\; r_i \in \mathcal{O}_F \ (1 \leq i \leq n) \right\}.$$

Suppose that $\boldsymbol{a} = (a_1, \cdots, a_n)^t, \boldsymbol{b} = (b_1, \cdots, b_n)^t$ are vectors in $\mathbb{C}^n$. The *complex euclidean inner product* of $\boldsymbol{a}$ and $\boldsymbol{b}$ is defined by

$$(\boldsymbol{a}, \boldsymbol{b}) = a_1 \bar{b}_1 + \cdots + a_n \bar{b}_n. \tag{3}$$

Suppose that $\boldsymbol{x} = (x_1, \cdots, x_n)^t$ is vector in $\mathbb{C}^n$. The *norm of $\boldsymbol{x}$* is defined by

$$\|\boldsymbol{x}\| = \sqrt{(\boldsymbol{x}, \boldsymbol{x})} = \sqrt{|x_1|^2 + \cdots + |x_n|^2}, \tag{4}$$

where, $x_i (\in \mathbb{C})$ is the i-th component of $\boldsymbol{x}$, and $\|\boldsymbol{x}\| \in \mathbb{R}$.

Let $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n \in F^n$ be linearly independent. Similarly the vectors $\boldsymbol{b}_i^* (1 \leq i \leq n)$ and the complex numbers $\mu_{ij} (1 \leq j < i \leq n)$ are inductively defined by $\boldsymbol{b}_i^* := \boldsymbol{b}_i - \sum_{j=1}^{i-1} \mu_{ij} \boldsymbol{b}_j^*$, $\mu_{ij} := (\boldsymbol{b}_i, \boldsymbol{b}_j^*)/(\boldsymbol{b}_j^*, \boldsymbol{b}_j^*)$, where $(\ ,\ )$ denotes the complex euclidean inner product on $\mathbb{C}^n$. And LLL-reduced basis is similarly defined by (1), (2).

From now on, we consider the imaginary quadratic field $F = \mathbb{Q}(\sqrt{m})$, where m is a square free negative integer, $R = \mathcal{O}_F$, the ring of integers in F.

Given imaginary quadratic field $\mathbb{Q}(\sqrt{m}) := \{a + b\sqrt{m} \mid a, b \in \mathbb{Q}\}$, the ring $\mathcal{O}_F$ 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 $\mathcal{O}_F := \left\{\frac{a+b\sqrt{m}}{2} \mid a, b \in \mathbb{Z},\ a \equiv b \ (\mathrm{mod} 2)\right\}$.

For above two cases about m, we can prove its non-zero absolute values are greater than 1. So, we show below it as a lemma.

Lemma 3.1 *If $F = \mathbb{Q}(\sqrt{m})$, where $m < 0$, we get for any non-zero $r \in \mathcal{O}_F, |r|^2 \geq 1$.*

This lemma implies the following proposition.

Proposition 3.2 *Let F denote the imaginally quadratic field $\mathbb{Q}(\sqrt{m})$ and $R = \mathcal{O}_F$ be the ring of integers in F. Let $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n$ be a basis of Λ, and $\boldsymbol{b}_i^*$ $(i = 1, 2, \cdots, n)$ be as above. Then we have*

$$\|\boldsymbol{x}\|^2 \geq \|\boldsymbol{b}_i^*\|^2 \quad \text{for some } i \leq n. \tag{5}$$

for any non-zero $\boldsymbol{x} \in \Lambda$.

These arguments imply the following main theorem.

Theorem 3.3 *Let* $F = \mathbb{Q}(\sqrt{m})$*, where* m *is a square free negative integer, If* $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n$ *is some reduced basis for a lattice* Λ *in* V*, then*
(i) $\|\boldsymbol{b}_j\|^2 \leq 2^{i-1}\|\boldsymbol{b}_i^*\|^2$ *for* $1 \leq j \leq i \leq n$,
(ii) $d(\Lambda) \leq \prod_{i=1}^n \|\boldsymbol{b}_i\| \leq 2^{n(n-1)/4} d(\Lambda)$,
(iii) $\|\boldsymbol{b}_1\| \leq 2^{(n-1)/4} d(\Lambda)^{1/n}$,
(iv) $\|\boldsymbol{b}_1\|^2 \leq 2^{n-1}\|\boldsymbol{x}\|^2$ *for every* $\boldsymbol{x} \in \Lambda, \boldsymbol{x} \neq \mathbf{0}$,
(v) *For any linearly independent set of vectors* $\boldsymbol{x}_1, \cdots, \boldsymbol{x}_t \in \Lambda$ *we have* $\|\boldsymbol{b}_j\|^2 \leq 2^{n-1}\max\{\|\boldsymbol{x}_1\|^2, \cdots, \|\boldsymbol{x}_t\|^2\}$ *for* $1 \leq j \leq t \leq n$,
where $\|\cdot\|$ *denotes the norm defined by (4).*

4 Absolute values of elements in some the rings of integers $\mathcal{O}_F$

In case F is a rational number field or a imaginary quadratic field, for non-zero element of $\mathcal{O}_F$, its absolute value is greater than 1. About this, we shall discuss about general number fields.

Let F be a number field of degree n and $\mathcal{O}_F$ denote its ring of integers. It is well-known that $\mathcal{O}_F$ is a lattice (free abelian group) of rank n. We shall use the Pigeonhole Principle, we can prove the following lemma.

Lemma 4.1 *Suppoose that* α *and* β *are real numbers and at least one of* α, β *is in* $\mathbb{R} \setminus \mathbb{Q}$*. Then there are infinitely many triads* (x, y, z) *of integers such that* $|x - z\alpha| < 1/\sqrt{z}$ *and* $|y - z\beta| < 1/\sqrt{z}$.

Proposition 4.2 *Let* L *be a lattice of rank* $n \geq 3$ *in* $\mathbb{C}$*. Then, for any positive real number* ϵ*, there is a non-zero* $z \in L$ *such that* $|z| < \epsilon$.

By similar way, we can prove the following.

Proposition 4.3 *Let* L *be a lattice of rank* $n \geq 2$ *in* $\mathbb{R}$*. Then, for any positive real number* ϵ*, there is a non-zero* $z \in L$ *such that* $|z| < \epsilon$.

By these propositions, for a non-zero element of $\mathcal{O}_F$, its absolute value is greater than 1, if and only if F is a rational number field or a imaginary quadratic field. We shall think this problem from other approaches using concept of group theory. About this we shall show as the following.

Lemma 4.4 *Let G be some additive subgroup of real number that has at least two elements. In this case, G is either dense or cycic (has a least positive element).*

Using this lemma, we shall discuss about an absolute value of a non-zero element over general number fields. Let G be the ring of integers in F i.e. $G = \mathcal{O}_F$. Then we can prove next propositions.

Proposition 4.5 *Let $G = \mathcal{O}_F$ be the ring of integers in F and rank $n \geq 2$ in $\mathbb{R}$. Then G is dense in $\mathbb{R}$.*

Proposition 4.6 *Let $G = \mathcal{O}_F$ be the ring of integers in F and rank $n \geq 3$ in $\mathbb{C}$. Then 0 is an accumulation point in $\mathbb{C}$.*

References

[1] H.Cohen, *A Course in Computational Algebraic Number Theory*, GTM **138**, Springer Verlag, 1993.

[2] A.K.Lenstra, H.W.Lenstra,Jr., and L.Lovász, *Factoring Polynomials with Rational Coefficients*, Math. Ann., **261**, 515-534, 1982.

[3] H.Napias, *A generalization of the LLL-algorithm over euclidean rings or orders*, Journal de Theorie des Nombres de Bordeaux, tome 8, no 2,387-396, 1996.

[4] K.Peter, *The LLL-Algorithm and some Applications*, 2009, available at `http://user.math.uzh.ch/dehaye/thesis_students/Karin`

[5] M.E.Pohst *Computational Algebraic Number Theory*, DMV Seminar **21**, Birkhäuser Verlag, 1993.

[6] M.Pohst and H.Zassenhaus, *Algorithmic Algebraic Number Theory*, Cambridge University Press, 1989.

Joint Graduate School in Science of School Education,
Hyogo University of Teacher Education,
Kato-Shi, Hyogo 673-1494, Japan

Department of Mathematics,
Naruto University of Education,
Naruto-Shi, Tokushima 772-8502, Japan