A GENERALIZATION OF LLL LATTICE BASIS REDUCTION OVER IMAGINARY QUADRATIC FIELDS

KOICHI ARIMOTO AND YASUYUKI HIRANO

Received July 27, 2017

ABSTRACT. In this paper we generalize LLL lattice basis reduction defined by Lenstra, Lenstra, and Lovász. We consider $\mathcal{O}_F$-lattice, where $\mathcal{O}_F$ is the ring of integers in algebraic number field F. We can prove that basic properties of reduced basis can hold over imaginary quadratic fields. We can reveal existence of a least positive element over other algebraic number fields.

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.

In last section, we consider a general algebraic number field F. Let $\mathcal{O}_F$ be the ring of integers in F, we state that $\mathcal{O}_F$ has a least positive element or not. And we show a necessary and sufficient condition for algebraic number field F to lead structure of lattice.

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

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

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 $d(\Lambda) = |\det(\boldsymbol{b}_i, \boldsymbol{b}_j)|^{\frac{1}{2}} > 0$, 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

2010 *Mathematics Subject Classification.* 11Y40, 11R04.
Key words and phrases. basis reduction, LLL-algorithm, imaginary quadratic fields.

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 [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

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

$$\mu_{ij} := \frac{(\boldsymbol{b}_i, \boldsymbol{b}_j^*)}{(\boldsymbol{b}_j^*, \boldsymbol{b}_j^*)}, \tag{2}$$

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

$$|\mu_{ij}| \leq \frac{1}{2} \quad \text{for } 1 \leq j < i \leq n \tag{3}$$

and

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

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 (4) 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 (4) 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 an 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 *Hermitian inner product* of $\boldsymbol{a}$ and $\boldsymbol{b}$ is defined by

$$(5) \qquad (\boldsymbol{a}, \boldsymbol{b}) = a_1\bar{b}_1 + \cdots + a_n\bar{b}_n.$$

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

$$(6) \qquad \|\boldsymbol{x}\| = \sqrt{(\boldsymbol{x}, \boldsymbol{x})} = \sqrt{|x_1|^2 + \cdots + |x_n|^2},$$

where, $x_i (\in \mathbb{C})$ is the i-th coordinate 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 $\boldsymbol{b}_i^* (1 \le i \le n)$ and the complex numbers $\mu_{ij} (1 \le j < i \le n)$ 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 Hermitian inner product on $\mathbb{C}^n$. And LLL-reduced basis is similarly defined by (3), (4).

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 $r \in \mathcal{O}_F, |r|^2 \ge 1$.*

Proof. (i) In case $m \not\equiv 1 \pmod 4$. Let $r =: a + b\sqrt{m}$, where $a, b \in \mathbb{Z}$. Then we can rewrite r as $r = a + b\sqrt{-m}i$, therefore $|r|^2 = a^2 - mb^2$.
We assume $a \ne 0$. Then $|r|^2 \ge 1$. If $b \ne 0$, then $|r|^2 \ge -m \ge 1$. Hence if either $a \ne 0$ or $b \ne 0$, then $|r|^2 \ge 1$.
(ii) In case $m \equiv 1 \pmod 4$. Let $r =: \frac{a + b\sqrt{m}}{2}$, where $a, b \in \mathbb{Z}$, with $a \equiv b \pmod 2$. Then $|r|^2 = \frac{a^2 - mb^2}{4}$. We show that if either $a \ne 0$ or $b \ne 0$ then $|r|^2 \ge 1$. Since $m < 0$, $m \equiv 1 \pmod 4$, the minimum value of $-m (> 0)$ is 3. Hence $|r|^2 \ge \frac{a^2 + 3b^2}{4}$.
(a) In case $a \equiv b \equiv 0 \pmod 2$. The minimum value of $a^2 + 3b^2$ is 4 $(a = \pm 2, b = 0)$.
(b) In case $a \equiv b \equiv 1 \pmod 2$. The minimum value of $a^2 + 3b^2$ is 4 $(a = \pm 1,\ b = \pm 1)$.
In any case, we have $|r|^2 \ge \frac{a^2 + 3b^2}{4} \ge 1$. ■

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*

$$(7) \qquad \|\boldsymbol{x}\|^2 \ge \|\boldsymbol{b}_i^*\|^2 \quad \text{for some } i \le n.$$

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

Proof. For every $\boldsymbol{x} \in \Lambda$, we can write $\boldsymbol{x} =: \sum_{j=1}^n r_j \boldsymbol{b}_j = \sum_{j=1}^n s_j \boldsymbol{b}_j^*$, where $r_j \in \mathcal{O}_F$ and $s_j \in \mathbb{Q}(\sqrt{m})$. Let i be the largest index with $r_i \ne 0$. We claim that $\boldsymbol{x} = \sum_{j=1}^i s_j \boldsymbol{b}_j^*$ and

$r_i = s_i$. By $\boldsymbol{b}_i = \boldsymbol{b}_i^* + \sum_{j=1}^{i-1} \mu_{ij} \boldsymbol{b}_j^*$, we have

$$\boldsymbol{x} = \sum_{j=1}^{i} r_j \boldsymbol{b}_j = \sum_{j=1}^{i} \left(r_j + \sum_{k=j+1}^{i} r_k \mu_{kj} \right) \boldsymbol{b}_j^*. \tag{8}$$

We suppose $j = i$, we have $r_i = s_i$.
Next,

$$\|\boldsymbol{x}\|^2 = \|s_1 \boldsymbol{b}_1^*\|^2 + \|s_2 \boldsymbol{b}_2^*\|^2 + \cdots + \|s_i \boldsymbol{b}_i^*\|^2 \geq |s_i|^2 \|\boldsymbol{b}_i^*\|^2 \tag{9}$$

Now since $s_i = r_i, |r_i|^2 \geq 1$(by Lemma 3.1). Therefore we have

$$\|\boldsymbol{x}\|^2 \geq |r_i|^2 \|\boldsymbol{b}_i^*\|^2 \geq \|\boldsymbol{b}_i^*\|^2, \tag{10}$$

for some $i \leq n$. ■

These arguments imply the following main theorem. The idea of following proof is due to [2].

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* $\boldsymbol{x} \in \Lambda, \boldsymbol{x} \neq \boldsymbol{0}$,
(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 (6).

Proof. (i) From (4) and (3) we see that

$$\|\boldsymbol{b}_i^*\|^2 \geq \left(\frac{3}{4} - |\mu_{i,i-1}|^2 \right) \|\boldsymbol{b}_{i-1}^*\|^2 \geq \frac{1}{2} \|\boldsymbol{b}_{i-1}^*\|^2$$

for $1 < i \leq n$, so by induction

$$\|\boldsymbol{b}_j^*\|^2 \leq 2^{i-j} \|\boldsymbol{b}_i^*\|^2 \quad \text{for } 1 \leq j \leq i \leq n.$$

From (1) and (3) we now obtain

$$\begin{aligned} \|\boldsymbol{b}_i\|^2 &= \|\boldsymbol{b}_i^*\|^2 + \sum_{j=1}^{i-1} |\mu_{ij}|^2 \|\boldsymbol{b}_j^*\|^2 \\ &\leq \|\boldsymbol{b}_i^*\|^2 + \sum_{j=1}^{i-1} \frac{1}{4} \cdot 2^{i-j} \|\boldsymbol{b}_i^*\|^2 \\ &= \left(1 + \frac{1}{4}(2^i - 2) \right) \|\boldsymbol{b}_i^*\|^2 \\ &\leq 2^{i-1} \|\boldsymbol{b}_i^*\|^2. \end{aligned}$$

It follows that

$$\|\boldsymbol{b}_j^*\|^2 \leq 2^{j-1} \|\boldsymbol{b}_j^*\|^2 \leq 2^{i-1} \|\boldsymbol{b}_i^*\|^2$$

for $1 \leq j \leq i \leq n$. This proves (i).
(ii) From $d(\Lambda) = |\det(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n)|$ and (1), it follows that

$$d(\Lambda) = |\det(\boldsymbol{b}_1^*, \cdots, \boldsymbol{b}_n^*)|$$

and therefore, since the $\boldsymbol{b}_i^*$ are pairwise orthogonal

$$d(\Lambda) = \prod_{i=1}^{n} \|\boldsymbol{b}_i^*\|.$$

From $\|\boldsymbol{b}_i^*\| \leq \|\boldsymbol{b}_i\|$ and $\|\boldsymbol{b}_i\| \leq 2^{(i-1)/2}\|\boldsymbol{b}_i^*\|$ we now obtain (ii).
(iii) Putting $j = 1$ in (i) and taking the product over $i = 1, \cdots, n$ we find (iii).
(iv) By Proposition 3.2, for every non-zero $\boldsymbol{x} \in \Lambda$, $\|\boldsymbol{x}\|^2 \geq \|\boldsymbol{b}_i^*\|^2$ for some $i \leq n$. Putting $j = 1$ in (i), we have $\|\boldsymbol{b}_1\|^2 \leq 2^{i-1}\|\boldsymbol{b}_i^*\|^2 \leq 2^{n-1}\|\boldsymbol{b}_i^*\|^2$. This proves (iv).
(v) Write $\boldsymbol{x}_j = \sum_{i=1}^{n} r_{ij}\boldsymbol{b}_i$ with $r_{ij} \in \mathcal{O}_F(1 \leq i \leq n)$ for $1 \leq j \leq t$. For fixed j, let $i(j)$ denote the largest i for which $r_{ij} \neq 0$. Then we have, by the proof of Proposition 3.2,

$$\|\boldsymbol{x}_j\|^2 \geq \|\boldsymbol{b}_{i(j)}^*\|^2 \tag{11}$$

for $1 \leq j \leq t$. Renumber the $\boldsymbol{x}_j$ such that $i(1) \leq \cdots \leq i(t)$. We claim that $j \leq i(j)$ for $1 \leq j \leq t$. If not, then $\boldsymbol{x}_1, \cdots, \boldsymbol{x}_j$ would all belong to $\mathcal{O}_F\boldsymbol{b}_1 + \cdots + \mathcal{O}_F\boldsymbol{b}_{j-1}$, a contradiction with the linear independence of $\boldsymbol{x}_1, \cdots, \boldsymbol{x}_t$. From $j \leq i(j)$ and (i) we obtain, using (11):

$$\|\boldsymbol{b}_j\|^2 \leq 2^{i(j)-1} \cdot \|\boldsymbol{b}_{i(j)}^*\|^2 \leq 2^{n-1} \cdot \|\boldsymbol{b}_{i(j)}^*\|^2 \leq 2^{n-1} \cdot \|\boldsymbol{x}_j\|^2$$

for $j = 1, \cdots, t$. This proves (iv). ■

4 Absolute values of elements in some the rings of integers $\mathcal{O}_F$ In case F is the rational or an imaginary quadratic field the absolute value of the non-zero elements of $\mathcal{O}_F$ is greater than one. The situation is different for general number fields, as we shall show in the sequel.

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 free abelian group of rank n.

Using the Pigeonhole Principle, we can prove the following lemma. It is a special case of Dirichlet's simultaneous approximation theorem. The proof is given in [7].

Lemma 4.1 *Suppose 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 free abelian group 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 $|z| < \epsilon$.*

Proof. We may assume that $n = 3$ and $L = \mathbb{Z}\boldsymbol{a} + \mathbb{Z}\boldsymbol{b} + \mathbb{Z}\boldsymbol{e}$. Since $\mathbb{C}$ is a 2-dimensional vector space over $\mathbb{R}$, there exist real numbers α and β such that $\boldsymbol{e} = \alpha\boldsymbol{a} + \beta\boldsymbol{b}$ and at least one of α, β is in $\mathbb{R} \setminus \mathbb{Q}$. By the lemma above, there are integers p, q, r such that $|p\alpha + q| < \epsilon/(\|\boldsymbol{a}\| + \|\boldsymbol{b}\|)$ and $|p\beta + r| < \epsilon/(\|\boldsymbol{a}\| + \|\boldsymbol{b}\|)$. Then we have $\|p\boldsymbol{e} + q\boldsymbol{a} + r\boldsymbol{b}\| = \|(p\alpha + q)\boldsymbol{a} + (p\beta + r)\boldsymbol{b}\| \leq |(p\alpha + q)|\|\boldsymbol{a}\| + |(p\beta + r)|\|\boldsymbol{b}\| < \epsilon$. ■

By similar way, we can prove the following.

Proposition 4.3 *Let L be a free abelian group 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 $|z| < \varepsilon$.*

By these propositions, the ring of integers $\mathcal{O}_F$ has a least positive element, if and only if F is the rational number field or an imaginary quadratic field. Therefore we conclude the following theorem.

Theorem 4.4 *Let F be a number field and $\mathcal{O}_F$ is the ring of integers in F. Then $\mathcal{O}_F$ has a least positive element if and only if F is either the rational number field or an imaginary quadratic field.*

Acknowledgment The authors would like to express their hearty thanks to the referee for his valuable advices.

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.

[7] W.M.Schmidt, *Diophantine Approximation*, LNM **785**, Springer Verlag, 1980.

Communicated by *Pál Dömösi*

Koichi Arimoto:
Joint Graduate School (Ph.D. Program) in Science of School Education,
Hyogo University of Teacher Education,
Kato-Shi, Hyogo 673-1494, Japan

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