A PERIODIC JACOBI-PERRON LIKE ALGORITHM BY COEFFICIENT REDUCTION

KIYOHISA TANIMOTO

Abstract. The author presents a multi-dimensional periodical algorithm like the Jacobi-Perron Algorithm(multi-dimensional continued fraction expansion) for any real algebraic number field of degree $n(n \geq 2)$. The author inserts a lattice basis reduction process to that Jacobi-Perron algorithm and succeed to get periodicity. This paper shows the algorithm and the proof of its periodicity.

1. Introduction

As well known, Lagrange showed that continued fraction expansion of any real quadratic number become eventually periodic in 1770 (Lagrange's continued fraction theorem).

C.G.J.Jacobi and O.Perron extended that ordinal continued fraction algorithm to higher degree number field (called as Jacobi-Perron Algorithm: JPA).

(About JPA,refer Zuzana Masakova's workshop document [1]).

Jacob-Perron algorithm (equivalent expression)

Let $\mathbb{Q}, \theta$ and $K = \mathbb{Q}(\theta)$ be respectively the rational numbers, a real algebraic integer of degree n ($n \geq 2$) and the number field generated by θ over $\mathbb{Q}$.
Suppose $\{\alpha_1(m) = 1, \alpha_2(m), \ldots, \alpha_n(m)\} \in K^n$ be linearly independent over $\mathbb{Q}$, then JPA is defined by the following recurrence relation.

$$\alpha_i(m+1) = \begin{cases} (\alpha_{i+1}(m) - \lfloor \alpha_{i+1}(m) \rfloor)/(\alpha_2(m) - \lfloor \alpha_2(m) \rfloor) & \text{i=1,...,n-1} \\ 1/(\alpha_2(m) - \lfloor \alpha_2(m) \rfloor) & \text{i=n} \end{cases} \tag{1}$$

The phrase of "periodic" in this paper means that there exist such positive integers s (*startpoint*), l(*period*) $\in \mathbb{Z}^+$, $\alpha_i(s+l) = \alpha_i(s)$ for $i = 1, \ldots, n$.

Claim 1. When a sequence is periodic, $\prod_{i=s}^{s+l-1}(\alpha_2(m) - \lfloor \alpha_2(m) \rfloor)$ is a non-trivial unit of K.

Unfortunately JPA does not always produce periodic sequence. Succeeding many mathematicians studied algorithms to obtain periodical sequence for stimulus diophantine approximation , calculation of unit and/or another purpose.

- Leon Bernstein [2] [3] found many classes that JPA sequences are periodic.
- E.V.Podsypanin [4] improved JPA as the modified JPA (MJPA) by swapping of order in a tuple and found many classes that MJPA become periodic.

Date: April 16, 2018.
2010 *Mathematics Subject Classification.* Primary 11A55; Secondary 11J70.
Key words and phrases. Jacobi-Perron algorithm, periodic series.

MJPA is similar to JPA except assurance of the following inequality by term swapping,

(2) $(\alpha_2(m) - \lfloor \alpha_2(m) \rfloor) \leq (\alpha_i(m) - \lfloor \alpha_i(m) \rfloor)$ for any $i \geq 2$)

- Paul Voutier [5] showed that there are infinitely many classes which have any given period and that for every real cubic number field there is a pair of numbers with periodic Jacob–Perron expansion.
- E. Dubois and R. Paysant-Le Roux [6] showed periodical algorithm about any cubic fields when a non-trivial unit is given.
- Shin-ichi Yasutomi and Jun-ichi Tamura [7] presented an algorithm named as the algebraic JPA (AJPA), and by their numerical experiments AJPA sequence become periodic in 3,4 degree number field.

  AJPA is similar to MJPA but the inequality is different such as

$$(\alpha_2(m) - \lfloor \alpha_2(m) \rfloor)/norm((\alpha_2(m) - \lfloor \alpha_2(m) \rfloor))$$
$$\leq (\alpha_i(m) - \lfloor \alpha(m) \rfloor)/norm((\alpha_i(m) - \lfloor \alpha(m) \rfloor)) \quad \text{for any } i \geq 2 \tag{3}$$

  instead of $(\alpha_2(m) - \lfloor \alpha_2(m) \rfloor) \leq (\alpha_i(m) - \lfloor \alpha(m) \rfloor)$ for any $i \geq 2$.

However these JPA like algorithms have some limitation ,like as 'not all real algebraic number fields' or 'units are given and so on.

The author has found a JPA like algorithm that produces periodic sequence by adoption of coefficient size reduction in arbitrary real algebraic number field (noted as rJPA in this paper). This paper describes the algorithm and proof of periodicity. Furthermore as a corollary, a unit of $K = \mathbb{Q}(\theta)$ is derived by using this algorithm.

2. Notations and remarks

Following notations are used in this paper.

- $\mathbb{Q}$: the rational numbers
- $\mathbb{Z}$: the rational integers
- θ: a real algebraic integer of degree n (where $n \geq 2$)
- K: $= \mathbb{Q}(\theta)$
- $M(n, \mathbb{Z})$: the n-th integer square matrices.
- $GL(n, \mathbb{Z})$: the n-th unimodular matrix group.
- English letters with subscript such as a_{ij}, b_{ij} express rational numbers. Greek letters with subscript such as α_i, β_i express elements of K.
- We assume the expression $\alpha_i = \sum_{j=1}^n a_{ij}\theta^{j-1}, \beta_i = \sum_{j=1}^n b_{ij}\theta^{j-1}$.
- $det(M)$: the determinant of a matrix M
- σ_i $(i = 1, \ldots, n)$: isomorphisms which transfer θ to an another conjugate of θ, where σ_1 be the identity map.
- $\beta_i \bullet \beta_j$: $\stackrel{\text{def}}{=} \sum_{k=2}^n b_{ik}b_{jk}$
- $\{\alpha_i\}$: a column vector of K, where $i = 1, \ldots, n$ and $\alpha_1 = 1$.
- $\{\alpha_i\}_\sigma$: the n-square matrix which (i,j) element is $\sigma_j(\alpha_i)$
- $\{a_{ij}\}$: the n square matrix of which (i, j) element equals to a_{ij} where $i, j = 1, \ldots, n$.

  Note. $\{\alpha_i\} = \{a_{ij}\}\{\theta^{(i-1)}\}$.
- $\{b_{ij}\}'$: the $n-1$ square matrix of which (i, j) element equals to b_{ij} where $i, j = 2, \ldots, n$.

- $norm(\xi)$: $= \prod_{i=1}^{n} \sigma_i(\xi)$ *for* $\xi \in K$

  Note. If ξ is an algebraic integer of K, $norm(\xi)$ is an rational integer.

  Note. For $\xi \in K$, $det(\{\xi\alpha_i\}_\sigma) = norm(\xi) det(\{\alpha_i\}_\sigma)$.

- D: $\stackrel{\text{def}}{=} \{\theta^{(i-1)}\}_\sigma$

  Note. $det(D)^2$ is the discriminant of θ and is not zero.

  Note. For $\alpha_i = \sum_{j=1}^{n} a_{ij}\theta^{j-1}$, $a_{ij} = det(\{1, \theta, , \theta^{(j-1)}, \alpha_i, \theta^{(j+1)}, , \theta^{(n-1)}\}_\sigma)/det(D)$

  Note. $\{\alpha_i\}_\sigma = \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \ldots\ldots & \ldots\ldots & \ldots\ldots \\ \sigma_1(\alpha_n) & \cdots & \sigma_n(\alpha_n) \end{pmatrix} = \{a_{ij}\}\{\theta^{(i-1)}\}_\sigma$.

  $$a_{1j} = \begin{cases} 1 & \text{j=1} \\ 0 & \text{j=2,...,n} \end{cases}$$

- $rdet(m)$: $\stackrel{\text{def}}{=} det(\{\alpha_i(m)\}_\sigma)/det(D)(= det(\{a_{ij}(m)\}))$

  Note. $rdet(m) = det(\{a_{ij}(m)\})$ $(i = 2, \ldots, n, j = 2, \ldots, n)$ because $\alpha_1 = 1$

- $Round(x)$[1]: If the fraction part of x is 0.5 then the nearest even integer to x else the nearest integer to x.

  Note. Thus $Round(0.5) = Round(-0.5) = 0$.

3. Definition of $rJPA$(coefficient size reducing JPA)

The proposed algorithm (called as rJPA in this paper) is consisted of the coefficient size reduction step and the successor calculation step. The coefficient reduction algorithm is an algorithm to obtain $\{\beta_i\} \in K^n$ for given $\{\alpha_i\} \in K^n$ (where $\alpha_1 = 1$ *and* $\beta_1 = 1$) which satisfies the following conditions(*) . An example of such algorithm is shown at the section 5.

Reduction condition(*)

(4) $\exists T \in GL(n, \mathbb{Z}),\ T\{a_{ij}\} = \{b_{ij}\}$

(5) $$\prod_{i=2}^{n}(\sum_{j=2}^{n} b_{ij}^2) \leq C_1 * det(\{b_{ij}\}')^2$$

where C_1 is a constant depend only the degree n.

(6) $$\sum_{j=2}^{n} b_{2j}^2 \leq \sum_{j=2}^{n} b_{ij}^2$$

Claim 2. The above condition (4) is equivalent to that $\mathbb{Z}[\alpha_1 = 1, \alpha_2, \ldots, \alpha_n] = \mathbb{Z}[\beta_1 = 1, \beta_2, \ldots, \beta_n]$ as $\mathbb{Z} - module$.

Note. $det(\{\alpha_i\}_\sigma) = det(\{\beta\}_\sigma)$.

[1] This can be replaced with another type of rounding function which satisfys $Round(0.5) * Round(-0.5) = 0$

If there is a unimodular matrix $T' \in GL(n-1,\mathbb{Z})$ such that $T'\{a_{ij}\}' = \{b_{ij}\}'$, then the above condition 4 is satisfied.

$\because$ It is clear from setting T_1 to $\begin{pmatrix} 1 & 0 \\ 0 & T' \end{pmatrix}$ and setting $\{\beta_i\}$ to $T_1\{\alpha_i\}$.

Now We define rJPA n-tuple sequences $\{\alpha_i(m)\}$ by induction with respect m as the followings.

Definition of rJPA: The rJPA is continuously repeating algorithm of the coefficient reduction step (CR-step) and the succeeding n-tuple computing step (SC-step) with the initial n-tuples $\{\alpha_i(1)\} = \{\theta^{(i-1)}\}$.

3.1. CR-step: Transform a n-tuple$\{\alpha_i(m)\}$ to a reduced coefficient n-tuple $\{\beta_i(m)\}$ by a coefficient reduce algorithm.

Note. We can apply a coefficient reduction algorithm and obtain reduced coefficients..

3.2. SC-step: Transform a n-tuple $\{\beta_i(m)\}$ to the succeeding n-tuple $\{\alpha_i(m+1)\}$ like as the following.

$$u_i(m) = Round(\beta_i(m)) \qquad (i = 2, \dots, n) \tag{7}$$

$$\alpha_i(m+1) = \begin{cases} (\beta_{i+1}(m) - u_{(i+1)}(m))/(\beta_2(m) - u_2(m)) & \text{i=1,\dots,n-1} \\ 1/(\beta_2(m) - u_2(m)) & \text{i=n} \end{cases} \tag{8}$$

Claim 3. $\{\alpha_i(m+1)\} = T_2(m)\{\beta_i(m)\}/(\beta_2(m) - u_2(m))$,

$$\text{where } T_2(m) = \begin{pmatrix} -u_2(m) & 1 & 0 & \cdots & 0 \\ -u_3(m) & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ -u_n(m) & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix}$$

Therefore

$$\begin{aligned} |det(\{\alpha_i(m+1)\}_\sigma)| &= |det(\{\beta_i(m)\}_\sigma)/norm(\beta_2(m) - u_2(m))| \\ &= |det(\{\alpha_i(m)\}_\sigma)/norm(\beta_2(m) - u_2(m))| \end{aligned}$$

4. Theorem and proof

We will prove our theorem by following scenario and contradiction. At first We will show $1/rdet(m)$ is a rational integer and that rJPA sequence elements divided by $rdet(m)$ are elements of $\mathbb{Z}[\theta]$. Then if rJPA sequence will not be periodic ,$rdet(m+1)$ must divert to ∞, finally causes a contradiction. Thus by contradiction, we can conclude rJPA sequence must become periodic.

Proposition 1. *There is a matrix $A(m)$ of $GL(n,\mathbb{Z})$ such that $\{(\alpha_i(m)\} = A(m)\{\theta^{(i-1)}\}/(\prod_{k=1}^{m-1}(\beta_2(k) - u_2(k)))$. Furthermore $\prod_{k=1}^{m-1}(\beta_2(k) - u_2(k))$ is an element of $\mathbb{Z}[\theta]$.*

Proof. We use induction with respect to m. Notations are same to the ones in the definitions.

As $\{\beta_i(m)\} = T_1\{\alpha_i(m)\}$, $\{\alpha_i(m+1)\} = T_2\{\beta_i(m)\}/(\beta_2(m) - u_2(m))$ therefore

$$\begin{aligned}\{\alpha_i(m+1)\} &= T_2T_1\{\alpha_i(m)\}/(\beta_2(m) - u_2(m)) \\ &= T_2T_1A(m)\{\theta^{(i-1)}\}/\prod_{k=1}^{m-1}(\beta_2(k) - u_2(k)/(\beta_2(m) - u_2(m)) \\ &= A(m+1)\{\theta^{(i-1)}\}/\prod_{k=1}^{m}(\beta_2(k) - u_2(k)).\end{aligned}$$

By induction ,the first statement is satisfied.

As $\alpha_1(m) = 1, \prod_{k=1}^{m-1}(\beta_2(k) - u_2(k))$ is the (1,1) element of $A(m)\{\theta^{(i-1)}\}$,this means an element of $\mathbb{Z}[\theta]$. i.e. the second statement is also satisfied. □

Cororraly 4.1. *$\{\alpha_i(m)\}$ can be expressed as $\alpha_i(m) = \xi_i(m)/\xi_1(m)$ by using $\xi_1(m),,,\xi_n(m) \in \mathbb{Z}[\theta]$.*

∵ Under an expression $\{\xi_i(m)\} = A(m)\{\theta^{(i-1)}\}, \xi_1(m) = \prod_{k=1}^{m-1}(\beta_2(k) - u_2(k))$. Hence $\alpha_i(m) = \xi_i(m)/\xi_1(m)$.

Cororraly 4.2. *$rdet(m) = 1/norm(\prod_{k=1}^{m-1}(\beta_2(k) - u_2(k))) = 1/\prod_{k=1}^{m-1} norm(\beta_2(k) - u_2(k))$.*

Proposition 2. *Suppose that $\alpha_i(m) = \sum_{j=1}^{n} a_{ij}(m)\theta^{(j-1)}$ for rJPA sequence $\{\alpha_i(m)\}$, then $a_{ij}(m)/rdet(m)$ are rational integers and $1/rdet(m)$ is also a rational integer.*

Proof. By Proposition 1, We have the following formula (9).

$$\exists A(m) \in GL(n, \mathbb{Z}), \{(\alpha_i(m)\} = A(m)\{\theta^{(i-1)}\}/(\prod_{k=1}^{m-1}(\beta_2(k) - u_2(k))). \quad (9)$$

Then as θ is an algebraic integer and $\prod_{k=1}^{m-1}(\beta_2(k) - u_2(k)))\{\theta^{(i-1)}\}$ is an element of $\mathbb{Z}[\theta]$, we obtain

$$\exists M \in M(n, \mathbb{Z}), (\prod_{k=1}^{m-1}(\beta_2(k) - u_2(k)))\{\theta^{(i-1)}\} = M\{\theta^{(i-1)}\} \quad (10)$$

From the formula (9), (10) and $\{\alpha_i(m)\} = \{a_{ij}(m)\}\{\theta^{(i-1)}\}$, we get

$$\{a_{ij}(m)\}M\{\theta^{(i-1)}\} = A(m)\{\theta^{(i-1)}\} \quad (11)$$

This formula implies the following formula (12) because $1, \theta, \ldots, \theta^{n-1}$ is linearly independent over $\mathbb{Q}$.

$$\{a_{ij}(m)\}M = A(m) \quad (12)$$

Therefore the following relation (13) is satisfied.

$$\{a_{ij}(m)\}/rdet(m) = A(m)M^{-1} * det(M) \quad (13)$$

On the other hand, $M^{-1} * det(M)$ is the adjugate matrix (or transpose of cofactor matrix) of M by the Cramer's rule and is an integer matrix when M is an integer matrix. This means that $\{a_{ij}(m)\}/rdet(m)$ is an integer matrix.

Therefore $a_{ij}(m)/rdet(m)$ are integers and $1/rdet(m)$ is also an integer because $a_{11} = 1$.

□

Cororraly 4.3. *Absolute value* $|rdet(m)| \leq 1$

Cororraly 4.4. $b_{ij}(m)/rdet(m)$ *are integers.*

Now, we will investigate what happen if tupul sequence of rJPA $\{\alpha_i(m)\}$ wouldn't be periodic.

Lemma 1. *If rJPA sequence* $\{\alpha_i(m)\}$ *wouldn't be periodic, then*
$\overline{\lim}_{m\to\infty} |norm(\beta_2(m) - u_2(m))| \leq (1/2)^n < 1$.

Proof. We will prove this lemma in the following order by using contradiction.
(1) $lim_{m\to\infty} rdet(m) = 0$
(2) $\lim_{m\to\infty} b_{2j}(m) = 0$.
(3) $\overline{\lim}_{m\to\infty} |b_{21}(m) - u_2(m)| \leq 1/2 < 1$
(4) $\overline{\lim}_{m\to\infty} |norm(\beta_2(m) - u_2(m))| \leq (1/2)^n < 1$.

Proof of (1): If $lim_{m\to\infty}\ rdet(m)$ is not 0 ,then there is an $\epsilon > 0$ such that $|rdet(m)| > \epsilon$ for infinitely many $m \in \mathbb{Z}^+$. By the reduction condition (*) ,

$$\prod_{i=2}^{n}\sum_{j=2}^{n}(b_{ij}(m)^2)/rdet(m)^2 \leq C_1 det(b_{ij}(m))^2/rdet(m)^2 \tag{14}$$

$$\leq C_1 rdet(m)^{(2-2(n-1))} \tag{15}$$

$$< C_1\epsilon^{2(2-n)} \tag{16}$$

for infinitely many m. While the value of the left hand side of this inequality is an integer and the value of the right hand side is upper bounded for infinitely many m. The absolute values of $|b_{i1}(m) - u_i(m)|$ are also upper bounded because $b_{ij}(m)^2$ $(j \geq 2)$ are upper bounded and $|\beta_i(m) - u_i(m)| \leq 1/2$. Therefore same combinations of $\{b_{ij}(m)\,(j \geq 2),\, b_{i1}(m) - u_i(m)\}$ must appear. However same combination appearance is contradict to aperiodicity. Hence $lim_{m\to\infty} rdet(m) = 0$.

Proof of (2): We recall $\prod_{i=2}^{n}\sum_{j=2}^{n}(b_{ij}(m)^2) \leq C_1 rdet(m)^2$ again.
As $\sum_{j=2}^{n} b_{2j}(m)^2 \leq \sum_{j=2}^{n} b_{ij}(m)^2, \sum_{j=2}^{n} b_{2j}(m)^2 \leq (C_1 * rdet(m))^{(1/(n-1))}$.
Therefore $\lim_{m\to\infty}(\sum_{j=1}^{n} b_{2j}(m)^2) = 0$. Hence $\lim_{m\to\infty} b_{2j}(m) = 0\ (j = 2, \ldots, n)$

Proof of (3): It is clear from (2) and $|\beta_2(m) - u_2(m)| \leq 1/2$.

Proof of (4): By (2) and (3), $\overline{\lim}_{m\to\infty} |\sigma_j(\beta_2(m) - u_2(m))| \leq 1/2$. Therefore $\overline{\lim}_{m\to\infty} \prod_{j=1}^{n} |\sigma_j(\beta_2(m) - u_2(m))| \leq (1/2)^n < 1$.
This means that $\overline{\lim}_{m\to\infty} |norm(\beta_2(m) - u_2(m))| \leq (1/2)^n < 1$

□

Now We are ready to prove the theorem.

Theorem 1. *rJPA produces periodic sequences.*

Proof. We use contradiction. According $rdet(m + 1) = \prod_{k=1}^{m}(1/norm(\beta_2(k) - u_2(k)))$ and the above Lemma 1, $|\prod_{k=1}^{m}(1/norm(\beta_2(k) - u_2(k)))|$ diverges to ∞. On the other hand Proposition-2 corollary-4.3 requires $|rdet(m)| \leq 1$. Contradiction. Hence rJPA sequence must become periodic. □

Cororraly 4.5. *Suppose that* $\{\alpha_i(s+l)\} = \{\alpha_i(s)\}$. *Then the product* $\prod_{k=s}^{s+l-1}(\beta_2(k) - u_2(k))$ *is an non-trivial unit of* K *in* $\mathbb{Z}[\theta]$

Proof. By the proposition 1,
$A(s+l)\{\theta^{i-1}\}/\prod_{k=1}^{s+l-1}(\beta_2(k) - u_2(k)) = A(s)\{\theta^{i-1}\}/\prod_{k=1}^{s-1}(\beta_2(k) - u_2(k))$. Thus $\prod_{k=s}^{s+l-1}(\beta_2(k) - u_2(k))$ is an eigenvalue of a unimodular matrix and $\{\theta^{i-1}\}$ is the eigen vector of that matrix. Hence this product is a unit of $K = \mathbb{Q}(\theta)$ and this unit locates in $\mathbb{Z}[\theta]$. By $1/|\beta(m)2 - u2(m)| > 1$, it is non trivial. □

Here the remained item to be proven is to show the existence of algorithms for the reduction condition(*).

5. Instances of coefficient reduction algorithm

The following algorithms are instances of coefficient reduction algorithm.
(1) case of $n = 2$
It is trivial for this case and We can set $\{\beta_i\} = \{\alpha_i\}$.

(2) case of $n = 3$: basicaly same to the Gauss' Algorithm.
$\{\beta_i\} := \{\alpha_i\}$:
REPEAT
  $\{\gamma_i\} := \{\beta_i\}$:
  $\beta_2 := \beta_2 - Round(\frac{\beta_2 \bullet \beta_3}{\beta_3 \bullet \beta_3}) * \beta_3;$
  $\beta_3 := \beta_3 - Round(\frac{\beta_2 \bullet \beta_3}{\beta_2 \bullet \beta_2}) * \beta_2;$
UNTIL $\{\gamma_i\} == \{\beta_i\}$;
IF $\beta_3 \bullet \beta_3 < \beta_2 \bullet \beta_2$ THEN SWAP β_2 and β_3 ENDIF ;

This process terminates because the following three reasons.
(i) The value of $\beta_2 \bullet \beta_2 + \beta_3 \bullet \beta_3$ decrease weakly monotonically.
(ii) Coefficients of β_2 *and* β_3 are rational numbers.
(iii) Round(0.5)=Round(-0.5)=0 .

By the identical equation $(ad - bc)^2 + (ac + bd)^2 = (a^2 + b^2)(c^2 + d^2)$, we have $(det(\{1, \beta_2, \beta_3\}'))^2 + (\beta_2 \bullet \beta_3)^2 = (\beta_2 \bullet \beta_2) * (\beta_3 \bullet \beta_3)$. The process termination means $|\beta_2 \bullet \beta_3| \leq (\beta_2 \bullet \beta_2)/2$ and $|\beta_2 \bullet \beta_3| \leq (\beta_3 \bullet \beta_3)/2$. Thus $(\beta_2 \bullet \beta_3)^2 \leq \frac{1}{4} * (\beta_2 \bullet \beta_2) * (\beta_3 \bullet \beta_3)$.
Hence $(\beta_2 \bullet \beta_2) * (\beta_3 \bullet \beta_3) \leq \frac{4}{3} * det(\{1, \beta_2, \beta_3\}')^2$
This $\{\beta_i\}(= \{\sum_{j=1}^{3} b_{ij}\theta^{j-1})\})$ is the desired one.
Obviously this algorithm keeps $\mathbb{Z}[1, \alpha_2, \alpha_3] = \mathbb{Z}[1, \beta_2, \beta_3]$ and satisfy the reduction condition(*) with $C_1 = \frac{4}{3}$.

3)case of $n \geq 4$

We can use L.L.L. algorithm [8] which were developped by Lenstra,Lenstra and Lovasz. The L.L.L. algorithm is a lattice basis reduction algorithm which calculates a short, nearly orthogonal lattice basis. Details are described in their paper "Factoring Polynomials with rational coefficients" [8].

the inequality (1.8) of their paper says,

$b_1, b_2, \ldots, b_n$ be a reduced basis for a lattice $L \in \mathbb{R}^n$
(1.8) $d(L) \leq \prod_{i=1}^{n} |b_i| \leq 2^{n(n-1)/4} d(L)$,
where || means the euclidean metric and d(L) is the determinant of the basis of the lattice L. By the L.L.L. algorithm , $|b_1| \leq |b_i|$ for any i.

The right inequality part of this (1.8) means in our case
$\prod_{i=2}^{n}(\sum_{j=2}^{n} b_{ij}^2)^{1/2} \leq 2^{(n-1)(n-2)/4} * det(\{b_{ij}\})$ where $i = 2, \ldots, n$, $j = 2, \ldots, n$.
Therefore, $\prod_{i=2}^{n}(\sum_{j=2}^{n} b_{ij}^2) \leq 2^{(n-1)(n-2)/2} * det(\{b_{ij}\})^2$ where $i = 2, \ldots, n$, $j = 2, \ldots, n$
This inequality satisfies the our reduction condition(*) with $C_1 = 2^{(n-1)(n-2)/2}$.

L.L.L. Algorithm is described at from (1.15) P.518 through to P.522 (1.25)

Hence our Theorem and its Corollary are completely proved.

References

[1] Zuzana Masáková, Multidimensional continued fractions Jacobi-Perron algorithm for simultaneous rational approximation of d real numbers, Workshop on Algebraic Structures Telč, August 11-15, 2008

[2] LEON BERNSTEIN, NEW INFINITE CLASSES OF PERIODIC JACOBI-PERRON ALGORITHMS, PACIFIC JOURNAL OF MATHEMATICS, **16**, (1965), No.3

[3] L. Bernstein, The Jacobi-Perron algorithm.Its theory and application, Springer-Verlag, Berlin, 1971.

[4] E.V.Podsypanin, A generalization of continued fraction algorithm that is related to the ViggoBrun algorithm, Studies in Number Theory, (1977)

[5] PAUL VOUTIER, FAMILIES OF PERIODIC JACOBI-PERRON ALGORITHMS FOR ALL PERIOD LENGTHS, (2015)

[6] E. Dubois and R. Paysant-Le Roux, Algorithme de Jacobi-Perron dans les extensions cubiques, C. R. Acad. Sci. not yet confirmed by me

[7] Shin-ichi Yasutomi,Jun-ichi Tamura, A new multidimensional continued fraction Algorithm, MATHEMATICS OF COMPUTATION,, **78**, (2009),

[8] A.K.Lenstra, H.W.Lenstra,Jr., L.Lovasz, Factoring Polynomials with rational coefficients, Math.Ann. **261**, (1982) 513–534

[9] V.Bertheé Multidimensional Euclidean algorithms, numeration and substitutions, Laboratoire d'fInformatique Algorithmique : Fondements et Applications, Université Paris Diderot, Paris 7 - Case 7014 F-75205 Paris Cedex 13 , France

Individual
E-mail address: tanichan@aqu.bekkoame.ne.jp