Linear and Nonlinear Analysis
Volume 3, Number 2, 2017, 213–224
Yokohama Publishers
ISSN 2188-8167

THE SHORTEST VECTOR PROBLEMS IN p-ADIC LATTICES AND SIMULTANEOUS APPROXIMATION PROBLEMS OF p-ADIC NUMBERS

HIROHITO INOUE AND KOICHIRO NAITO

Abstract. In this paper we construct the multi-dimensional p-adic approximation lattices by using simultaneous approximation problems (SAP) of p-adic numbers and we estimate the l_∞ norm of the p-adic SAP solutions theoretically by applying Dirichlet's principle and numerically by using the LLL algorithm.

1. Introduction

The p-adic numbers introduced by Kurt Hensel have been mainly used as significant objects in the number theory during almost 100 years. From 1980's applications of p-adic numbers were started and proposed in mathematical physics, especially in quantum mechanics. Now p-adic analysis has been studied in various fields to investigate extremely complex models, which have chaotic properties, such as the theory of turbulence, biology, dynamical systems, cryptography and economy ... from the natural sciences to the social sciences. On the other hand, the lattice-based cryptography is considered as one of the most powerful post-quantum cryptography. In this paper we construct the multi-dimensional p-adic approximation lattices by using simultaneous approximation problems (SAP) of p-adic numbers and we estimate the l_∞ norm of the p-adic SAP solutions theoretically by applying Dirichlet's principle and numerically by using the LLL algorithm.

We consider two types of SAP, named the 1st type and the 2nd type, and these two types of SAP are related by the transference principle (see [4]). In both cases we can show that the numerical estimates on the l_∞ norms of the p-adic SAP solutions by LLL algorithms satisfy the theoretical upper bounds in the lattice dimension $n \leq 60$, but in the case $n \geq 80$ and the p-adic approximation order $m \geq 30$ these numerical solutions become greater than these theoretical upper bounds.

In [3], using these SVP or SAP solutions as private keys, we construct a cryptosystem, the security of which is based on the hardness of SVP or SAP. Since we can numerically show that the l_∞ norms of the SVP solutions given by LLL in the lattices of dimensions over 80 and $m \geq 30$ exceed the theoretical boundary value of the SAP solutions, the private keys given in the lattices of dimensions over this value

2010 *Mathematics Subject Classification.* 11J13, 11E55, 11A05.

Key words and phrases. Simultaneous homogeneous approximation, p-adic theory, LLL algorithm.

are considered to be secure for the attacks by LLL. The purpose of this paper is to find some efficient private keys in these lattice based cryptography by numerically estimating the SAP solutions in the p-adic lattices.

Our plan of this paper is as follows. In Section 2 we give a brief review of lattices and LLL algorithm. In Section 3 we investigate the relations between the SAP of p-adic numbers and the SVP of p-adic approximation lattices and we estimate the l_∞ norm of p-adic SAP solutions. In Section 4 we give the numerical estimates of the SAP solutions by using the LLL reduction algorithm. In Section 5 and 6 we investigate the 2nd type SAP and we estimate the l_∞ norms of these SAP solutions theoretically and numerically.

2. Lattice and LLL algorithm

In this section we give a brief review on lattices and the LLL algorithm. (For details, see [5], [6].)

Given linearly independent vectors $b_1, \ldots, b_n \in \mathbb{R}^m$, the lattice generated by these vectors is defined by

$$L(b_1, \ldots, b_n) = \{\sum_{i=1}^{n} x_i b_i : x_i \in \mathbb{Z}\}.$$

We refer to $b_1, \ldots, b_n$ as a basis of the lattice.

Let B be the $m \times n$ matrix whose columns are $b_1, \ldots, b_n$, then the lattice generated by B is

$$L(B) = \{Bx : \ x \in \mathbb{Z}^n\}.$$

We say that the rank of lattice is n and its dimension is m. If $n = m$, the lattice is called a full-rank lattice. Hereafter we consider full-rank lattices.

For matrix B, $P(B) = \{Bx : x \in [0,1)^n\}$ is called the fundamental parallelepiped of B. Let $\Lambda = L(B)$ be a lattice of rank n. We define the determinant of Λ, denoted by $\det(\Lambda)$, as the n-dimensional volume of $P(B)$. In the full rank case, $\det(\Lambda) = |\det(B)|$.

The ith successive minimum of lattice Λ, $\lambda_i(\Lambda)$, is defined by

$$\lambda_i(\Lambda) = \inf\{r : \ \dim(\mathrm{span}(\Lambda \cap \overline{B}(0,r))) \geq i\}$$

where $\overline{B}(0,r)$ is a closed ball with its center 0 and its radius $r > 0$. The length of the shortest nonzero vector in the lattice is denoted by $\lambda_1(\Lambda)$ and the second minimum vector should be linearly independent to the shortest vector. The following estimate for the shortest vector is given by Minkowski's theorem in the l_2 norm (Euclidean norm).

$$\lambda_1(\Lambda) \leq \sqrt{n}\{\det(\Lambda)\}^{1/n}. \tag{2.1}$$

For the successive minimum in the l_∞ norm we use the notation $\lambda_i^{(\infty)}(\Lambda)$ and we also use $\lambda_i^{(2)}(\Lambda)$ for those in the l_2 norm to distinguish it from other norms. $\| \ \|_p$ denotes the l_p norm for $1 \leq p \leq \infty$.

Next we introduce the algorithm given by Lenstra, Lenstra and Lovász, which approximately solves the Shortest Vector Problem (SVP) within a factor of $2^{O(n)}$ for the lattices dimension n. The basic idea of LLL algorithm is to generalize Gauss's

algorithm to higher dimensions. For a basis $b_1, \dots, b_n$ of a lattice, the Gram-Schmidt orthogonalized basis $b_1^*, \dots, b_n^*$, which satisfies

$$\operatorname{span}(b_1, \dots, b_k) = \operatorname{span}(b_1^*, \dots, b_k^*), k = 1, \dots, n$$
$$b_k = \sum_{i=1}^{k} \mu_{k,i} b_i^*,\ \mu_{k,i} = \frac{(b_k, b_i^*)}{(b_i^*, b_i^*)} \text{ for } i \le k-1,\ \mu_{k,k} = 1,$$

is essentially used to construct the reduced basis.

Definition 2.1. For a constant $\delta : 1/4 < \delta < 1$, a basis $\{b_1, \dots, b_n\}$ of a lattice is called a δ-reduced basis if it satisfies the following two conditions.

- $|\mu_{k,i}| = \left|\frac{(b_k, b_i^*)}{(b_i^*, b_i^*)}\right| \le \frac{1}{2}$ for all $i < k$,
- for any pair of consecutive vectors b_i, b_{i+1},

$$\delta \|\pi_i(b_i)\|_2^2 \le \|\pi_i(b_{i+1})\|_2^2$$

where we define projection operations π_i from $\mathbb{R}^n$ onto $\operatorname{span}(b_i^*, b_{i+1}^*, \dots, b_n^*)$ by

$$\pi_i(x) = \sum_{j=i}^{n} \frac{(x, b_j^*)}{(b_j^*, b_j^*)} b_j^*.$$

The following estimate is well-known for the first vector in a δ-LLL reduced basis.

Lemma 2.2. *If $B = (b_1, \dots, b_n) \in \mathbb{R}^{n \times n}$ is a δ-LLL reduced basis with $\delta \in (1/4, 1)$, then*

$$\|b_1\|_2 \le \left(\frac{2}{\sqrt{4\delta - 1}}\right)^{n-1} \lambda_1(B). \tag{2.2}$$

Using the estimate (2.1), we obtain

$$\|b_1\|_2 \le \sqrt{n}\ |\det(B)|^{\frac{1}{n}} \left(\frac{2}{\sqrt{4\delta - 1}}\right)^{n-1}. \tag{2.3}$$

3. p-ADIC LATTICE

In this section we introduce p-adic approximation lattices and investigate simultaneous rational approximations of p-adic numbers. Let p be a fixed rational prime number and $|\cdot|_p$ be the corresponding p-adic valuation, normalized so that $|p|_p = p^{-1}$. The completion of $\mathbb{Q}$ w.r.t. $|\cdot|_p$ is called the field of p-adic numbers, denoted by $\mathbb{Q}_p$. The strong triangle inequality

$$|a + b|_p \le \max\{|a|_p, |b|_p\}, \quad a, b \in \mathbb{Q}_p$$

is most important and essential to construct p-adic approximation lattices. The set of p-adic integers is defined by $\mathbb{Z}_p = \{z \in \mathbb{Q}_p : |z|_p \le 1\}$.

Let $n \ge 1$ be an integer and let $\Xi = \{\xi_1, \xi_2, \dots, \xi_n\}$ be a n-tuple of p-adic integers.

Definition 3.1. We denote by $w_n(\Xi)$ the supremum of the real numbers w such that, for some infinitely many real numbers X_j, which goes to infinity, the inequalities

$$0 < |a_{0,j} + a_{1,j}\xi_1 + \cdots + a_{n,j}\xi_n|_p \le X_j^{-w-1},$$

$$\max_{0\le i\le n} |a_{i,j}| \le X_j,$$

have a solution in integers $a_{0,j}, a_{1,j}, \ldots, a_{n,j}$.

Remark 3.2. For the case where $\xi_1 = \xi, \xi_2 = \xi^2, \ldots, \xi_n = \xi^n$ for a p-adic number ξ the following results have been obtained (see [1]). $w_n(\Xi) = \min\{n, d-1\}$ holds if ξ is algebraic of degree d and $w_n(\Xi) \ge n$ for every p-adic number ξ, which is not algebraic of degree at most n. In [8] Sprindžuk proved that $w_n(\Xi) = n$ for almost all ξ in the sense of Haar Measure.

For a positive integer m we define the p-adic approximation lattice Γ_m by

$$\Gamma_m = \{(a_0, a_1, \ldots, a_n) \in \mathbb{Z}^{n+1} : |a_0 + a_1\xi_1 + \cdots + a_n\xi_n|_p \le p^{-m}\}. \tag{3.1}$$

When a p-adic integer ξ_i has the p-adic expansion

$$\xi_i = \sum_{k=0}^{\infty} x_{i,k}p^k,\ 0 \le x_{i,k} \le p-1,$$

let $\xi_{i,m}$ be the m-th order approximation of ξ_i defined by

$$\xi_{i,m} = \sum_{k=0}^{m-1} x_{i,k}p^k. \tag{3.2}$$

Consider the basis $\{b_{0,m}, b_{1,m}, \ldots, b_{n,m}\} \subset \mathbb{Z}^{n+1}$ of the lattice Γ_m given by

$$b_{0,m} = (p^m, 0, \ldots, 0)^t, \quad b_{1,m} = (\xi_{1,m}, -1, 0, \ldots, 0)^t,$$
$$b_{2,m} = (\xi_{2,m}, 0, -1, 0, \ldots, 0)^t, \cdots, b_{n,m} = (\xi_{n,m}, 0, \ldots, 0, -1)^t.$$

In fact, we have $b_{k,m} \in \Gamma_m,\ \forall k$, since we can estimate

$$|\xi_{k,m} - \xi_k|_p \le p^{-m}.$$

For $B_m = (b_{0,m}b_{1,m}\ldots b_{n,m})$ we have

$$B_m = \begin{pmatrix} p^m & \xi_{1,m} & \xi_{2,m} & \ldots & \xi_{n,m} \\ 0 & -1 & 0 & \ldots & 0 \\ 0 & 0 & -1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & -1 \end{pmatrix}, \quad |\det(B_m)| = p^m.$$

Applying the LLL algorithm for $\delta \in (1/4, 1)$, we denote $\{b_0, b_1, \ldots, b_n\}$ a reduced basis and $B = (b_0\ b_1\ \ldots\ b_n)$. It follows from (2.3) that the shortest vector b_0 in B satisfies

$$\begin{aligned} \|b_0\|_2 &\le \sqrt{n+1}\ |\det(B)|^{\frac{1}{n+1}} \left(\frac{2}{\sqrt{4\delta-1}}\right)^n \\ &= \sqrt{n+1}\ |\det(B_m)|^{\frac{1}{n+1}} \left(\frac{2}{\sqrt{4\delta-1}}\right)^n \\ &= \sqrt{n+1}\ p^{\frac{m}{n+1}} \left(\frac{2}{\sqrt{4\delta-1}}\right)^n. \end{aligned} \tag{3.3}$$

Furthermore, it is known that

$$\left(\prod_{i=0}^{n}\|b_i\|_2\right)^{\frac{1}{n+1}} \le K_n|\det(B)|^{\frac{1}{n+1}} = K_n p^{\frac{m}{n+1}}, \quad K_n \sim 2^{O(n)} \tag{3.4}$$

for the reduced basis $\{b_0, b_1, \ldots, b_n\}$.

Now we estimate the minimum norm value $\lambda_1^{(\infty)}(\Gamma_m)(=\lambda_1^{(\infty)}(L(B_m)))$ by using the famous Dirichlet principle.

Theorem 3.3. *For a n-tuple of p-adic integers $\Xi = \{\xi_1, \ldots, \xi_n\}$, which are irrational and linearly independent over $\mathbb{Q}$, and each positive integer m, there exists a solution in integers $(a_{0,m}, a_{1,m}, \ldots, a_{n,m}) \in \mathbb{Z}^{n+1}$, which satisfies*

$$0 < |a_{0,m} + a_{1,m}\xi_1 + \cdots + a_{n,m}\xi_n|_p \le p^{-m}, \tag{3.5}$$

$$\max_{0\le i\le n}|a_{i,m}| \le p^{\frac{m}{n+1}}. \tag{3.6}$$

Consequently, we have

$$\lambda_1^{(\infty)}(\Gamma_m) \le p^{\frac{m}{n+1}} = \det(\Gamma_m)^{\frac{1}{n+1}} \tag{3.7}$$

and

$$w_n(\Xi) \ge n. \tag{3.8}$$

Proof. For each positive integer m we use the pigeonhole principle for the holes, which are defined by

$$H_k = \{z \in \mathbb{Z}_p : z \equiv \sum_{j=0}^{m-1} h_{k,j}p^j \mod p^m\}$$

for $0 \le h_{k,j} \le p-1,\ j = 0, 1, \ldots, m-1,\ k = 1, 2, \ldots, p^m$. Here we can take each set H_k, defined by the numbers $\{h_{k,j}\}_{0\le j\le m-1}$, which satisfies

$$\mathbb{Z}_p = \bigcup_{k=1}^{p^m} H_k, \quad H_k \cap H_{k'} = \emptyset \ \text{ for } k \ne k'.$$

Next we consider the following nonzero p-adic integers given by

$$b_0 + b_1\xi_1 + \cdots + b_n\xi_n,$$
$$b_i \in \{0, 1, \ldots, l\},\ i = 0, 1, \ldots, n$$

where the integer l is given by $l = [p^{m/(n+1)}]$. Since the total number of these p-adic integers satisfies

$$(l+1)^{n+1} > (p^{\frac{m}{n+1}})^{n+1} = p^m,$$

and it is greater than the total number of the pigeonholes, there exists a pigeonhole H_k, which contains at least a pair of p-adic integers,

$$b_0 + b_1\xi_1 + \cdots + b_n\xi_n,\ b_0' + b_1'\xi_1 + \cdots + b_n'\xi_n \in H_k.$$

Putting $a_i = b_i - b_i',\ i = 0, 1, \ldots, n$, we can obtain the solution in integers $a_0, \ldots, a_n$, which satisfies

$$0 < |a_0 + a_1\xi_1 + \cdots + a_n\xi_n|_p \le p^{-m},$$

$$\max_{0\le i\le n}|a_i| \le l \le p^{\frac{m}{n+1}}.$$

It follows from the definitions that we can obtain the estimates (5.7) and (5.8). □

4. Numerical calculations on SAP

In this section, we compare the minimum norms of the vectors given by the LLL reduction algorithm and the upper bound of the norms of the shortest vectors $X_m := p^{m/(n+1)}$ given in Theorem 5.2, using the open source software Sage. We investigate the following case.

$p = 13$: prime number,

$\xi_i = u_i^{\frac{1}{103}}$: p-adic number, 103rd root of u_i:

$11, 12, 14, 15, 16, 17, 18, 19, 20, 21$,

$m = 5$: approximation order

$n = 10$: dimension

For the approximation order $m = 5$ and the dimension $n = 10$, we apply the LLL reduction ($\delta = 0.99999$). Then we obtain the reduced basis B from B_m. Here we note that the basis is given by row vectors in Sage.

$$B_m = \begin{pmatrix} 371293 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 125400 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 286272 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 282218 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 340728 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 128378 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 4671 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 341596 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 366035 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 6311 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 348639 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}.$$

$$B = \begin{pmatrix} 0 & -1 & -1 & -1 & -1 & 2 & 0 & 0 & 0 & 2 & -1 \\ 0 & 1 & 2 & -1 & 1 & 0 & -2 & -1 & 1 & -1 & 1 \\ 1 & 1 & -2 & 2 & 0 & -1 & 0 & 0 & 1 & -1 & -1 \\ 0 & -1 & 2 & 2 & 0 & 1 & 1 & 1 & -1 & -1 & 0 \\ 2 & -1 & 1 & 0 & -2 & 1 & 2 & 0 & -1 & 1 & 0 \\ -1 & 0 & 1 & 0 & -1 & 0 & 0 & -1 & 2 & 2 & -1 \\ 0 & -1 & -2 & 0 & 2 & 0 & 1 & -1 & 1 & -2 & 0 \\ -1 & 1 & -1 & -1 & 0 & 0 & -1 & -3 & 0 & -2 & 0 \\ 0 & 0 & 0 & -1 & 1 & -1 & -2 & -1 & -2 & -1 & -2 \\ 1 & -2 & -1 & 2 & -1 & 0 & 0 & 0 & 0 & -2 & 2 \\ 1 & -1 & 0 & 1 & 1 & -1 & -1 & 0 & -2 & 3 & 1 \end{pmatrix}.$$

We obtain

$$\min_{0\le i\le n}\|b_i\|_2 = 3.60555..., \quad \max_{0\le i\le n}\|b_i\|_2 = 4.35889...,$$
$$\min_{0\le i\le n}\|b_i\|_\infty = 2, \quad \max_{0\le i\le n}\|b_i\|_\infty = 3,$$

which are sufficiently effective solutions of SVP, smaller than the value $X_m = p^{m/(n+1)} = 3.208764...$, comparing the theoretical estimate (5.7) in Theorem 5.2

$$\lambda_1^{(\infty)}(\Gamma_m) \le p^{\frac{m}{n+1}} = \det(\Gamma_m)^{\frac{1}{n+1}}.$$

5. Second Type SAP

We consider the following simultaneous approximation problems. Let $n \ge 1$ be an integer and let $\Xi = \{\xi_1, \xi_2, \dots, \xi_n\}$ be a n-tuple of p-adic integers.

Definition 5.1. We denote by $\nu_n(\Xi)$ the supremum of the real numbers ν such that, for some infinitely many real numbers Y_j, which goes to infinity, the inequalities

$$0 < \max_{1\le i\le n} |a_{0,j}\xi_i - a_{i,j}|_p \le Y_j^{-\nu-1},$$
$$\max_{0\le i\le n} |a_{i,j}| \le Y_j,$$

have a solution in integers $a_{0,j}, a_{1,j}, ..., a_{n,j}$.

For a positive integer m we define the p-adic approximation lattice Λ_m by

$$\Lambda_m = \{(a_0, a_1, \dots, a_n) \in \mathbb{Z}^{n+1} : \max_{1\le i\le n} |a_0\xi_i - a_i|_p \le p^{-m}\}. \tag{5.1}$$

When a p-adic integer ξ_i has the p-adic expansion

$$\xi_i = \sum_{k=0}^{\infty} x_{i,k}p^k,\ 0 \le x_{i,k} \le p-1,$$

let $\xi_{i,m}$ be the m-th order approximation of ξ_i defined by

$$\xi_{i,m} = \sum_{k=0}^{m-1} x_{i,k}p^k. \tag{5.2}$$

Consider the basis $\{b_{0,m}, b_{1,m}, \dots, b_{n,m}\} \subset \mathbb{Z}^{n+1}$ of the lattice Λ_m given by

$$b_{0,m} = (1, \xi_{1,m}, \xi_{2,m}, \dots, \xi_{n,m})^t,\ b_{1,m} = (0, -p^m, 0, \dots, 0)^t,$$
$$b_{2,m} = (0, 0, -p^m, 0, \dots, 0)^t, \cdots, b_{n,m} = (0, 0, \dots, 0, -p^m)^t.$$

In fact, we have $b_{k,m} \in \Lambda_m,\ \forall k$, since we can estimate

$$|\xi_{k,m} - \xi_k|_p \le p^{-m}.$$

For $B_m = (b_{0,m}b_{1,m}\dots b_{n,m})$ we have

$$B_m = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ \xi_{1,m} & -p^m & 0 & \dots & 0 \\ \xi_{2,m} & 0 & -p^m & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \xi_{n,m} & 0 & 0 & \dots & -p^m \end{pmatrix}, \quad |\det(B_m)| = p^{nm}.$$

Applying the LLL algorithm for $\delta \in (1/4, 1)$, we denote $\{b_0, b_1, \dots, b_n\}$ a reduced basis and $B = (b_0\ b_1\ \dots\ b_n)$. It follows from (2.3) that the shortest vector b_0 in B satisfies

$$\|b_0\|_2 \le \sqrt{n+1}\ |\det(B)|^{\frac{1}{n+1}} \left(\frac{2}{\sqrt{4\delta-1}}\right)^n \tag{5.3}$$

$$= \sqrt{n+1}\ |\det(B_m)|^{\frac{1}{n+1}} \left(\frac{2}{\sqrt{4\delta-1}}\right)^n$$
$$= \sqrt{n+1}\ p^{\frac{mn}{n+1}} \left(\frac{2}{\sqrt{4\delta-1}}\right)^n.$$

Furthermore, it is known that

$$\left(\prod_{i=0}^{n} \|b_i\|_2\right)^{\frac{1}{n+1}} \leq K_n |\det(B)|^{\frac{1}{n+1}} = K_n p^{\frac{nm}{n+1}}, \quad K_n \sim 2^{O(n)} \tag{5.4}$$

for the reduced basis $\{b_0, b_1, \ldots, b_n\}$.

Now we estimate the minimum norm value $\lambda_1^{(\infty)}(\Lambda_m)(= \lambda_1^{(\infty)}(L(B_m)))$ by using the famous Dirichlet principle.

Theorem 5.2. *For a n-tuple of p-adic integers $\Xi = \{\xi_1, \ldots, \xi_n\}$, which are irrational and linearly independent over $\mathbb{Q}$, and each positive integer m, there exists a solution in integers $(a_{0,m}, a_{1,m}, \ldots, a_{n,m}) \in \mathbb{Z}^{n+1}$, which satisfies*

$$0 < \max_{1\leq i\leq n} |a_{0,m}\xi_i - a_{i,m}|_p \leq p^{-m}, \tag{5.5}$$

$$\max_{0\leq i\leq n} |a_{i,m}| \leq p^{\frac{nm}{n+1}}. \tag{5.6}$$

Consequently, we have

$$\lambda_1^{(\infty)}(\Lambda_m) \leq p^{\frac{nm}{n+1}} = \det(\Lambda_m)^{\frac{1}{n+1}} \tag{5.7}$$

and

$$\nu_n(\Xi) \geq \frac{1}{n}. \tag{5.8}$$

Proof. For each positive integer m we use the pigeonhole principle for the holes $B_{k(\cdot)}$, which are defined as follows. Consider the set K of all functions $k(\cdot)$ from $\{1, 2, ..., n\}$ to $\{1, 2, ..., p^m\}$

$$K = \{k(\cdot) : k(i) \in \{1, 2, ..., p^m\}, \quad i \in \{1, ..., n\}\}, \quad \#(K) = p^{nm}.$$

For each fixed $i \in \{1, ..., n\}$, define

$$H_{k(i)} = \{z \in \mathbb{Z}_p : z \equiv \sum_{j=0}^{m-1} h_{k(i),j} p^j \mod p^m\}$$

for $0 \leq h_{k(i),j} \leq p-1,\ j = 0, 1, \ldots, m-1$. Here, for each fixed i, we can take each set $H_{k(i)}$, defined by the sequences $\{h_{k(i),j}\}_{0\leq j\leq m-1}$, which satisfies

$$\mathbb{Z}_p = \bigcup_{k\in K} H_{k(i)}, \quad H_{k(i)} \cap H_{k'(i)} = \emptyset \ \text{ for } \{h_{k(i),j}\} \neq \{h_{k'(i),j}\}.$$

Now we can define the pigeonholes $B_{k(\cdot)}$ by

$$B_{k(\cdot)} := \prod_{i=1}^{n} H_{k(i)} \subset \mathbb{Z}_p^n,$$

which satisfy

$$\bigcup_{k\in K} B_{k(\cdot)} = \mathbb{Z}_p^n, \quad B_{k(\cdot)} \cap B_{k'(\cdot)} = \emptyset \ \text{ for } \ k \neq k'.$$

Next we consider the following nonzero vectors of p-adic integers given by

$$(b_0\xi_1 - b_1, b_0\xi_2 - b_2, ..., b_0\xi_n - b_n) \in \mathbb{Z}_p^n$$
$$b_i \in \{0, 1, \ldots, l\}, \ i = 0, 1, \ldots, n,$$

where the integer l is given by $l = [p^{mn/(n+1)}]$. Since the total number of these p-adic integers satisfies

$$(l+1)^{n+1} > (p^{\frac{nm}{n+1}})^{n+1} = p^{nm}, \tag{5.9}$$

and it is greater than the total number of the pigeonholes, there exists a pigeonhole $B_{k(\cdot)}$, which contains at least a pair of vectors of p-adic integers,

$$(b_0\xi_1 - b_1, b_0\xi_2 - b_2, ..., b_0\xi_n - b_n), \quad (b_0'\xi_1 - b_1', b_0'\xi_2 - b_2', ..., b_0'\xi_n - b_n') \in B_{k(\cdot)}.$$

Putting $a_i = b_i - b_i', \ i = 0, 1, \ldots, n$, we can obtain the solution in integers $a_0, \ldots, a_n$, which satisfies

$$0 < \max_{1\le i\le n} |a_0\xi_i - a_i|_p \le p^{-m},$$
$$\max_{0\le i\le n} |a_i| \le l \le p^{\frac{nm}{n+1}}$$

where we note that, if $a_0 = 0$, there exists $a_j \neq 0 : |a_j| < p^m$, which contradicts that $|a_j|_p \le p^{-m}$. It follows from the definitions that we can obtain the estimates (5.7) and (5.8).

□

6. Numerical computations of 2nd type

In this section, we compare the minimum norms of the vectors given by the LLL reduction algorithm and the upper bound of the norms of the shortest vectors $X_m := p^{mn/(n+1)}$ given in Theorem 5.2, using the open source software Sage. We investigate the following case.

$p = 13$: prime number,

$\xi_i = u_i^{\frac{1}{103}}$: p-adic number, 103rd root of u_i:

$11, 12, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 27, 28, 29, 30, 31, 32,$
$33, 34, 35, 36, 37, 38, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 53, 54,$
$55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75,$
$76, 77, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 92, 93, 94, 95, 96, 97$

$m = 5, 6, \ldots, 50$: approximation orders

$n = 20, 60, 70, 80$: dimensions

First we show our numerical process by using the small parameters, $n = 10$, $\xi_i = u_i^{\frac{1}{103}}$, $m = 5$. For the approximation order $m = 5$ and the dimension $n = 10$,

we apply the LLL reduction ($\delta = 0.99999$). Then we obtain the reduced basis B from B_m. Here we note that the basis is given by row vectors in Sage.

$$B_m = \begin{pmatrix} 1 & 111456 & 18940 & 350689 & 212426 & 303156 & 144193 & 25368 & 63624 & 59421 & 22667 \\ 0 & 371293 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 371293 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 371293 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 371293 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 371293 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 371293 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 371293 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 371293 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 371293 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 371293 \end{pmatrix},$$

$$B = \begin{pmatrix} -69434 & 24095 & 39846 & 26207 & 27541 & 9052 & 18983 & 12280 & -24702 & -29898 & 50549 \\ -45752 & 3150 & 54982 & -38719 & 51216 & 27996 & 15888 & 25182 & 11872 & -22246 & -39235 \\ 23932 & -3920 & -76673 & -17824 & 35276 & 64172 & 29734 & 42921 & -23025 & 11182 & 7571 \\ 100625 & -16358 & -9469 & 22612 & 28240 & 10913 & 32771 & 15625 & -40199 & -64347 & 13976 \\ 18545 & -36611 & -878 & -40683 & 21440 & -90586 & 6999 & 21329 & -62074 & -35179 & 55839 \\ 70240 & -43465 & 2781 & 75154 & 21742 & 23890 & -14134 & 13213 & 67212 & 26427 & 25696 \\ 70927 & 40449 & 19306 & 29340 & 40255 & -3311 & -88774 & -9742 & -35674 & 6424 & 3619 \\ 7586 & 71055 & -11551 & 12409 & 52016 & -47426 & 18920 & 111874 & -29236 & 18004 & 43203 \\ -54693 & 25466 & 22050 & 20317 & -85955 & -50900 & -84429 & 69917 & -29436 & 14876 & 21096 \\ 39752 & -40457 & -79324 & 22150 & 41653 & 411 & -61198 & -3052 & -66668 & -62474 & -69527 \\ -45915 & 29179 & -61894 & -21904 & -43973 & -4463 & -96112 & -25579 & 37364 & -54251 & -21026 \end{pmatrix}.$$

We obtain

$$\min_{0\le i\le n} \|b_i\|_\infty = 54982, \quad \max_{0\le i\le n} \|b_i\|_\infty = 111874 \ < \ p^{\frac{mn}{n+1}} = 115712.126290745...,$$

which shows that the SVP solutions given by LLL satisfy the theoretical estimate (5.7) of the SAP solutions in Theorem 5.2

$$\lambda_1^{(\infty)}(\Gamma_m) \le p^{\frac{mn}{n+1}} = \det(\Gamma_m)^{\frac{1}{n+1}}.$$

Next we give the graphs which compare these numerical minimum and maximum values in the l_∞ norm for the shortest vectors given by the LLL reduction basis and the values $X_m := p^{nm/(n+1)}$ for the approximation orders m from 10 to 50 and the dimensions $n = 20, 60, 70, 80$. Here we take the ratio of these numerical minimum and maximum values to the value X_m.

Since the LLL reduction algorithm approximately finds the shortest vectors in the l_2 norm, we use their l_∞ norm values as the substitutes of the shortest vectors in the l_∞ norm. We use the following line styles in the graphs.

- - - - - - - - - : ratio of minimum norm values of the reduced basis vectors in l_∞,
———————— : $X_m = p^{nm/(n+1)} \equiv 1$,
· · · · · · · · · · · · : ratio of maximum norm values of the reduced basis vectors in l_∞.

These graphs show that the LLL algorithm is effective enough to obtain the solutions of SAP, which satisfy the estimate (5.7), if the dimension n is under 60 (see Figure 1 and 2), but this estimate is not satisfied for some m if $n > 60$ and if $n \ge 80$ and $m \ge 30$ (see Figure 4).

In [7] we found the remark on the run-time of exact SVP, quoted from [2], that up to dimension 60 the shortest vector problem could be solved within an hour, whereas dimension 100 seemed out of reach.

These graphs show that the LLL algorithm is effective enough to obtain the solutions of SAP, which satisfy the estimate (5.6),

$$\lambda_1^{(\infty)}(\Gamma_m) \le p^{\frac{nm}{n+1}},$$

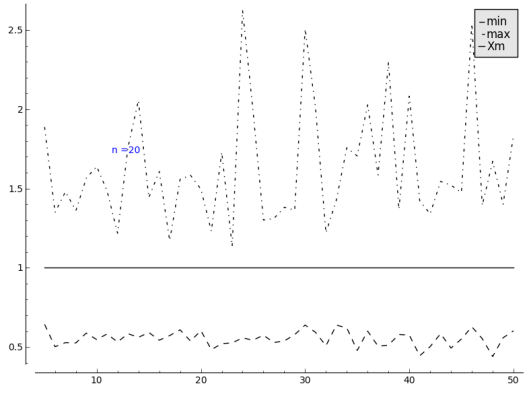

FIGURE 1. n=20

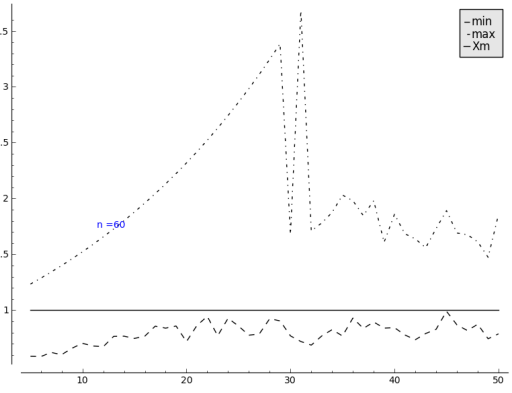

FIGURE 2. n=60

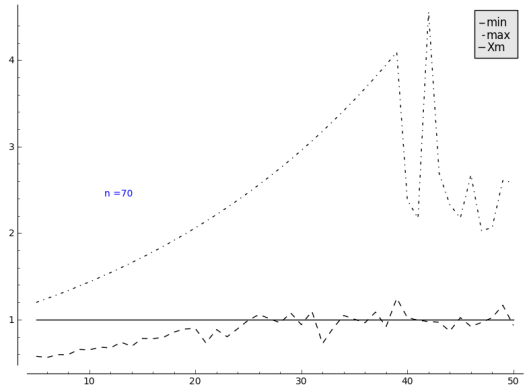

FIGURE 3. n=70

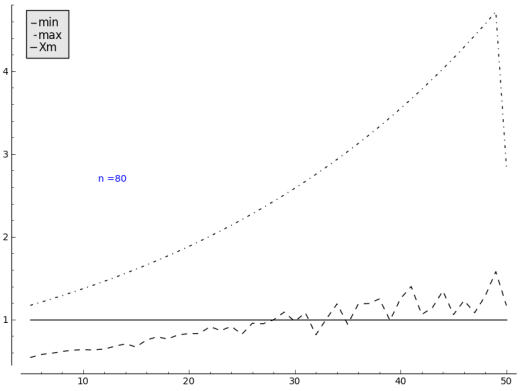

FIGURE 4. n=80

if the dimension n is under 60 (see Figure 1 and 2), but this estimate is not satisfied for some m if $n > 60$ and if $n \geq 80$ and $m \geq 30$ (see Figure 4 and [2], [7]). In our cryptosystems proposed in [3] we use these SAP solutions as the private keys. The private keys of the SAP solutions, which satisfy (3.6), must be secure against the LLL attacks in the dimension $n \geq 80$ and $m \geq 30$.

REFERENCES

[1] Y.Bugeaud, *Approximation by Algebraic Numbers*, Cambridge Tracts in Mathematics, Cambridge University Press, 2004.

[2] N. Gama and P. Q. Nguyen, *Predicting lattice reduction*, Nigel P. Smart:editor, EUROCRYPT, vol. 4965, Lecture Notes in Computer Science, Springer 2008, pp. 31–51.

[3] H. Inoue, S. Kamada and K. Naito, *Simultaneous approximations of p-adic numbers and their applications to cryptography*, to appear in Linear Nonlinar Anal.

[4] H. Inoue, S. Kamada and K. Naito, *Transference principle on simultaneous approximation problems of p-adic numbers and multidimensional p-adic approximation lattices* , to appear in Linear Nonlinar Anal.

[5] D. Micciancio and S. Goldwasser, *Complexity of Lattice Problems, a Cryptographic Perspective*, Springer International Series in Engineering and Computer Science, vol. 671. Springer, 2002

[6] P. Q. Nguyen and B. Vallee (Eds.), *The LLL Algorithm, Survey and Applications*, Springer, 2010.
[7] J. van de Pol and Nigel P. Smart, *Estimating key sizes for high dimensional lattice-based systems*, IMA Int. Conf., vol. 8308 Lecture Notes in Computer Science, Springer, 2013, pp. 290–303.
[8] V. G. Sprindžuk, *Mahler's problem in metric number theory*. Izdat. "Nauka i Tehnika", Minsk, 1967 (in Russian). English translation by B. Volkmann, Translations of Mathematical Monographs, Vol. 25, American Mathematical Society, Providence, R.I., 1969
[9] B.M.M. de Weger, *Approximation Lattices of p-adic Numbers*, Journal of Number Theory. **24** (1986), 70–88.

Manuscript received 2 March 2015
revised 10 April 2015

Hirohito Inoue
Department of Applied Mathematics, Graduate School of Science and Technology, Kumamoto University, Kurokami 2-39-1, Kumamoto, Japan
E-mail address: hiro886@gmail.com

Koichiro Naito
Department of Applied Mathematics, Graduate School of Science and Technology, Kumamoto University, Kurokami 2-39-1, Kumamoto, Japan
E-mail address: knaito@gpo.kumamoto-u.ac.jp