Linear and Nonlinear Analysis
Volume 3, Number 2, 2017, 239–249
Yokohama Publishers
ISSN 2188-8167

TRANSFERENCE PRINCIPLE ON SIMULTANEOUS APPROXIMATION PROBLEMS OF p-ADIC NUMBERS AND MULTIDIMENSIONAL p-ADIC APPROXIMATION LATTICES

HIROHITO INOUE, SHOICHI KAMADA, AND KOICHIRO NAITO

Abstract. By using the simultaneous approximation problems (SAP) of p-adic numbers we construct the two types of multi-dimensional p-adic approximation lattices, which are combined by the famous transference principle. Using the duality relations between these two lattices, we construct the algorithm, which gives the solutions of the 2nd type SAP from the solutions of the 1st type SAP. Using the open source software Sage and the LLL algorithm, we also numerically estimate the l_∞ norms of the 2nd type SAP solutions.

1. Introduction

The lattice-based cryptography, the security of which depends on the NP hardness of various lattice problems, is considered as one of the most powerful post-quantum cryptography. In this paper we study the simultaneous approximation problems (SAP) of p-adic numbers, which are NP complete problems (see [6]), by using the multidimensional p-adic approximation lattices. In [4] we propose a lattice based cryptosystem, the private keys of which are the SAP solutions of p-adic lattices. The purpose of this paper is to find some efficient private keys in these lattice based cryptography by numerical estimating the SAP solutions in the p-adic lattices.

We study the two types, named the 1st type and the 2nd type, of simultaneous approximations of p-adic numbers. It is known that the transference principle gives the inequality relations between the exponents given by the SAP of p-adic numbers (cf. [5]). Here we estimate the l_∞ norms of the solutions of the 1st type and the 2nd type problems theoretically and numerically. For these approximation problems we construct basis matrices, given by mth order approximations of the p-adic numbers, and we show that the unimodular transformation of these matrices are combined by the duality relation, given by the transpose and the inverse operations of these matrices. Using these duality relations and the LLL algorithm, we construct the algorithm, which gives the solutions of the 2nd type SAP from the solutions of the 1st type SAP, and we numerically estimate the l_∞ norms of these SAP solutions. We can show that these norms of the numerical SAP solutions take their values under the theoretically given upper bound $p^{mn/(n+1)}$ in the dimensions under $n = 50$ for almost all the approximation orders m, but their numerical values become greater

2010 *Mathematics Subject Classification.* 11J13, 11E95, 11A55 .
Key words and phrases. Simultaneous approximation, P-adic theory, LLL algorithm.

than this upper bound for $n \geq 60$ and $m \geq 20$. In our cryptosystems proposed in [4] we use these SAP solutions as the private keys. We can conclude that the private keys of the SAP solutions, the l_∞ norms of which are under this upper bound value, must be secure against the LLL attacks in the dimension $n \geq 70$ and $m \geq 30$.

Our plan of this paper is as follows. In section 2 we give a brief review on lattices and the LLL algorithm. In section 3, introducing p-adic approximation lattices, we give some results on the minimum norms of the vectors in these lattices. In section 4 we construct the algorithm which gives the solutions of the 2nd type SAP from the solutions of the 1st type SAP by the duality of the related p-adic lattices. In section 5 we show some numerical results by using the algorithms given in section 4.

2. Lattice and LLL algorithm

In this section we give a brief review on lattices and the LLL algorithm. (For details, see [7], [9].)

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

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

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

Let B be the $m \times n$ matrix whose columns are $b_1, ..., b_n$, 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 $b_1, ..., b_n$ of a lattice, the Gram-Schmidt orthogonalized basis $b_1^*, ..., b_n^*$, which satisfies

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

is essentially used to construct the reduced basis.

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

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

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

where we define projection operations π_i from $\mathbb{R}^n$ onto $\text{span}(b_i^*, b_{i+1}^*, ..., b_n^*)$ 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 $B = (b_1, ..., b_n) \in \mathbb{R}^{n\times n}$ is a δ-LLL reduced basis with $\delta \in (1/4, 1)$, then*

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

Using the estimate (2.1), we obtain

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

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

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

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

Let $n \geq 1$ be an integer and let $\Xi = \{\xi_1, \xi_2, ..., \xi_n\}$ 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

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

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

Remark 3.2. For the case where $\xi_1 = \xi, \xi_2 = \xi^2, ..., \xi_n = \xi^n$ 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 $w_n(\Xi) \geq n$ for every p-adic number ξ, which is not algebraic of degree at most n. In [10] 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

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

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

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

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

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

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

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

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

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

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

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

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

$$\begin{aligned} \|b_0\|_2 &\leq \sqrt{n+1}\ |\det(B)|^{\frac{1}{n+1}} \left(\frac{2}{\sqrt{4\delta-1}}\right)^n \\ &= \sqrt{n+1}\ |\det(B_m)|^{\frac{1}{n+1}} \left(\frac{2}{\sqrt{4\delta-1}}\right)^n \end{aligned} \tag{3.2}$$

$$= \sqrt{n+1}\; p^{\frac{m}{n+1}} \left(\frac{2}{\sqrt{4\delta-1}}\right)^n.$$

Furthermore, it is known that

$$\left(\prod_{i=0}^{n} \|b_i\|_2\right)^{\frac{1}{n+1}} \leq K_n |\det(B)|^{\frac{1}{n+1}} = K_n p^{\frac{m}{n+1}}, \quad K_n \sim 2^{O(n)} \tag{3.3}$$

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

In [3] we have obtained the following estimate on 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 $\Xi = \{\xi_1, ..., \xi_n\}$, which are irrational and linearly independent over $\mathbb{Q}$, and each positive integer m, there exists a solution in integers $(a_{0,m}, a_{1,m}, ..., a_{n,m}) \in \mathbb{Z}^{n+1}$, which satisfies*

$$0 < |a_{0,m} + a_{1,m}\xi_1 + \cdots + a_{n,m}\xi_n|_p \leq p^{-m}, \tag{3.4}$$

$$\max_{0\leq i\leq n} |a_{i,m}| \leq p^{\frac{m}{n+1}}. \tag{3.5}$$

Consequently, we have

$$\lambda_1^{(\infty)}(\Gamma_m) \leq p^{\frac{m}{n+1}} = \det(\Gamma_m)^{\frac{1}{n+1}} \tag{3.6}$$

and

$$w_n(\Xi) \geq n. \tag{3.7}$$

Let $\{c_{0,m}^*, c_{1,m}^*, ..., c_{n,m}^*\}$ be an orthogonal basis obtained by the Gram-Schmidt process from a basis $\{c_{0,m}, c_{1,m}, ..., c_{n,m}\}$ of the approximation lattice Γ_m. We denote the fundamental parallelepiped of the orthogonal basis by $P(C_m^*)$ where $C_m^* = (c_{0,m}^*, c_{1,m}^*, ..., c_{n,m}^*)$. Since $\min_{0\leq i\leq n} \|c_{i,m}^*\|_2 \leq \lambda_1^{(2)}(\Gamma_m)$ (cf. [7]), we can estimate the upper and lower bound of $\lambda_1^{(\infty)}(\Gamma_m)$ by Theorem 3.3.

$$\frac{1}{\sqrt{n+1}} \min_{0\leq i\leq n} \|c_{i,m}^*\|_2 \leq \frac{1}{\sqrt{n+1}} \lambda_1^{(2)}(\Gamma_m) \leq \lambda_1^{(\infty)}(\Gamma_m) \leq (\prod_{i=0}^{n} \|c_{i,m}^*\|_2)^{\frac{1}{n+1}}. \tag{3.8}$$

Here the estimate

$$\frac{1}{\sqrt{n+1}} \lambda_1^{(2)}(\Gamma_m) \leq \lambda_1^{(\infty)}(\Gamma_m)$$

can be proved as follows. Let c_0 be the shortest vector in the l_∞ norm,

$$\|c_0\|_\infty = \lambda_1^{(\infty)}(\Gamma_m).$$

Since we have

$$\frac{1}{\sqrt{n+1}} \|c_0\|_2 \leq \|c_0\|_\infty,$$

we can estimate

$$\frac{1}{\sqrt{n+1}} \lambda_1^{(2)}(\Gamma_m) \leq \frac{1}{\sqrt{n+1}} \|c_0\|_2 \leq \|c_0\|_\infty.$$

Next, using the same parameters as those of the upper bounds, we give the lower bounds of the shortest vectors in the p-adic approximation lattices under some additional hypotheses.

Theorem 3.4. *Let $\Xi = \{\xi_1, ..., \xi_n\}$ be a n-tuple of p-adic integers, which are irrational and linearly independent over $\mathbb{Q}$, and for positive integers m and s we assume that the fundamental parallelepiped $P(C^*_{m-s})$ is almost contained in $P(C^*_m)$, satisfying the following estimate*

$$\det(\Gamma_{m-s})^{\frac{1}{n+1}} \leq \min_{0\leq i\leq n} \|c^*_{i,m}\|_2. \tag{3.9}$$

Then we have

$$\frac{1}{\sqrt{n+1}} p^{\frac{m-s}{n+1}} \leq \lambda_1^{(\infty)}(\Gamma_m) \leq p^{\frac{m}{n+1}}. \tag{3.10}$$

Proof. By using (3.8) and (3.9) and Theorem 3.3 we can estimate

$$\begin{aligned} \frac{1}{\sqrt{n+1}} p^{\frac{m-s}{n+1}} &= \frac{1}{\sqrt{n+1}} \det(\Gamma_{m-s})^{\frac{1}{n+1}} \leq \frac{1}{\sqrt{n+1}} \min_{0\leq i\leq n} \|c^*_{i,m}\|_2 \\ &\leq \frac{1}{\sqrt{n+1}} \lambda_1^{(2)}(\Gamma_m) \leq \lambda_1^{(\infty)}(\Gamma_m) \leq p^{\frac{m}{n+1}} \end{aligned}$$

□

4. Dual lattice

Next we consider the following 2nd type of the simultaneous approximation problems. Let $n \geq 1$ be an integer and let $\Xi = \{\xi_1, \xi_2, \ldots, \xi_n\}$ be a n-tuple of p-adic integers.

Definition 4.1. 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

$$\begin{aligned} &0 < \max_{1\leq i\leq n} |a_{0,j}\xi_i - a_{i,j}|_p \leq Y_j^{-\nu-1}, \\ &\max_{0\leq i\leq n} |a_{i,j}| \leq Y_j, \end{aligned}$$

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

$$\Lambda_m = \{(a_0, a_1, \ldots, a_n) \in \mathbb{Z}^{n+1} : \max_{1\leq i\leq n} |a_0\xi_i - a_i|_p \leq p^{-m}\}. \tag{4.1}$$

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

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

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

$$\xi_{i,m} = \sum_{k=0}^{m-1} x_{i,k} p^k. \tag{4.2}$$

Consider the basis $\{b'_{0,m}, b'_{1,m}, \ldots, b'_{n,m}\} \subset \mathbb{Z}^{n+1}$ of the lattice Λ_m given by

$$\begin{aligned} &b'_{0,m} = (1, \xi_{1,m}, \xi_{2,m}, \ldots, \xi_{n,m})^t,\ b'_{1,m} = (0, -p^m, 0, \ldots, 0)^t, \\ &b'_{2,m} = (0, 0, -p^m, 0, \ldots, 0)^t, \cdots, b'_{n,m} = (0, 0, \ldots, 0, -p^m)^t. \end{aligned}$$

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

$$\begin{aligned} \|b'_0\|_2 &\le \sqrt{n+1}\ \left|\det(B')\right|^{\frac{1}{n+1}} \left(\frac{2}{\sqrt{4\delta - 1}}\right)^n \\ &= \sqrt{n+1}\ \left|\det(B'_m)\right|^{\frac{1}{n+1}} \left(\frac{2}{\sqrt{4\delta - 1}}\right)^n \\ &= \sqrt{n+1}\ p^{\frac{mn}{n+1}} \left(\frac{2}{\sqrt{4\delta - 1}}\right)^n. \end{aligned} \tag{4.3}$$

In [3] we have obtained the following theorem on the estimates of the minimum norm value $\lambda_1^{(\infty)}(\Lambda_m) (= \lambda_1^{(\infty)}(L(B'_m)))$.

Theorem 4.2. *For a n-tuple of p-adic integers $\Xi = \{\xi_1, \dots, \xi_n\}$, which are irrational and linearly independent over $\mathbb{Q}$, and each positive integer m, there exists a solution in integers $(a_{0,m}, a_{1,m}, \dots, a_{n,m}) \in \mathbb{Z}^{n+1}$, which satisfies*

$$0 < \max_{1 \le i \le n} |a_{0,m}\xi_i - a_{i,m}|_p \le p^{-m}, \tag{4.4}$$

$$\max_{0 \le i \le n} |a_{i,m}| \le p^{\frac{nm}{n+1}}. \tag{4.5}$$

Consequently, we have

$$\lambda_1^{(\infty)}(\Lambda_m) \le p^{\frac{nm}{n+1}} = \det(\Lambda_m)^{\frac{1}{n+1}} \tag{4.6}$$

and

$$\nu_n(\Xi) \ge \frac{1}{n}. \tag{4.7}$$

For a lattice $L(A)$ with its basis square matrix A, define its dual lattice $L(A)^*$ by

$$L(A)^* = L((A^t)^{-1})$$

where A^t is the transpose of the matrix of A.

For the 1st type lattice $\Gamma_m = L(B_m)$ and the 2nd type lattice $\Lambda_m = L(B'_m)$ we have the following theorem.

Theorem 4.3. *For a positive integer m and the 1st type lattice $\Gamma_m = L(B_m)$ and the 2nd type lattice $\Lambda_m = L(B'_m)$, let $B = B_m U$ and $B' = B'_m V$ for some unimodular matrices U, V. Then the following duality relation*

$$L(B') = \Lambda_m = p^m \Gamma_m^* = L(p^m (B^t)^{-1}) \tag{4.8}$$

holds.

Proof. From the definitions of B_m and B'_m we have

$$B'_m = p^m (B_m^t)^{-1}.$$

Since $L(AW) = L(A)$ for any unimodular matrix W, we can easily obtain the following sequence of estimates.

$$\begin{aligned} L(B') &= L(B'_m) = L(p^m (B_m^t)^{-1}) \\ &= L(p^m (B^t)^{-1}) = p^m \Gamma_m^*. \end{aligned}$$

□

Since the solutions of the 1st SAP are given by the reduced matrix B and the solutions of the 2nd SAP are given by B', it follows from (4.8) that we can construct an algorithm, which gives the 2nd SAP solutions from the 1st SAP solutions by applying the LLL algorithm.

5. Numerical experiments

We apply the algorithm given in section 4 to obtain the solutions of the 2nd type simultaneous approximation problem for the small parameters. Let $p = 13, n = 5, m = 10, \xi_i = u_i^{\frac{1}{103}}, u_i = 5, 29, 53, 61, 75$. Here we apply the algorithm obtained by Theorem 4.3. Using the m-th order approximation of ξ_i, we define the lattice-basis matrix B_m. Here we note that the basis vectors are row vectors in Sage.

$$B_m = \begin{pmatrix} 137858491849 & 0 & 0 & 0 & 0 & 0 \\ 76365194160 & -1 & 0 & 0 & 0 & 0 \\ 51552443868 & 0 & -1 & 0 & 0 & 0 \\ 66523226082 & 0 & 0 & -1 & 0 & 0 \\ 72516179394 & 0 & 0 & 0 & -1 & 0 \\ 89446562878 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}.$$

Applying the LLL algorithm to B_m, we obtain the LLL reduced matrix B.

$$B = \begin{pmatrix} 11 & -32 & -5 & -29 & 19 & 4 \\ -37 & -8 & 9 & -1 & 25 & -41 \\ -8 & -13 & -2 & 50 & 24 & 45 \\ 1 & 30 & 59 & -23 & -8 & 21 \\ -65 & -24 & -43 & -16 & 16 & 18 \\ 8 & -94 & 49 & 3 & -88 & -33 \end{pmatrix}$$

Since $p^{m/(n+1)} = 71.8740...$, almost all elements of B, 92%, is less than $p^{m/(n+1)}$.

Next we calculate the matrix $p^m(B^t)^{-1}$

$$= \begin{pmatrix} 1241486672 & -1565359053 & 338147086 & -1393149657 & 1783053986 & 380504601 \\ -810996656 & -274240281 & 1079088758 & 519376011 & 1399964275 & -1499174723 \\ -74674568 & -734001285 & 714653880 & 1364167122 & 892328270 & 878314484 \\ -691724231 & 368990416 & 1527445157 & -791918767 & 21495681 & 919955864 \\ -1473720392 & -94860410 & -580868135 & -691166009 & -686783704 & 819031658 \\ -187779451 & -666858520 & 330002901 & 165127974 & -667340744 & -38924698 \end{pmatrix}.$$

Here we can admit that the l_∞ norm of the shortest vector $b' = (b'_0, b'_1, ..., b'_n)$ in the reduced basis B' satisfies the SAP estimate conditions

$$|b'_0\xi_i - b'_i|_p \leq 13^{-10}, \quad \forall i$$

and

$$\|b'\|_\infty = 1364167122 < 1918055940.1 \cdots = 13^{50/11} = p^{mn/(n+1)}.$$

Next we give the graphs which compare these numerical minimum and maximum vectors in the reduced dual basis $B' = p^m(B^t)^{-1}$ and the values $X_m = p^{mn/(n+1)}$ for the approximation orders m from 5 to 40 and the dimensions $n = 20, 40, 50, 60, 70, 80$. We plot the ratio of the l_∞ norms of the minimum and maximum vectors to the values X_m, for which we constantly set the value 1. To specify the behaviors of the minimum vectors we plot the values of maximum vectors only for the case $n = 20, 40$.

We investigate the following case.

- $p = 13$: prime number
- $\xi_i = u_i^{\frac{1}{103}}$: p-adic number, 103rd root of u_i:
  $11, 12, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 27, 28, 29, 30, 31, 32,$
  $33, 34, 35, 36, 37, 38, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 53, 54,$
  $55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75,$
  $76, 77, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 92, 93, 94, 95, 96, 97$
- $m = 5, 6, ..., 40$: approximation orders
- $n = 20, 40, 50, 60, 70, 80$: dimensions

We use the following line styles.

$-\cdot-\cdot-\cdot$ ratio of maximum norms of the reduced basis vectors in l_∞

——— $X_m = p^{nm/(n+1)} \equiv 1$

– – – ratio of minimum norms of the reduced basis vectors in l_∞.

From these graphs we can find that the SAP condition (4.5) is satisfied in the dimensions under $n = 50$ for almost all the approximation order m, but not satisfied for $n \geq 60$ and $m \geq 20$. In our cryptosystems proposed in [4] we use these SAP solutions as the private keys. The private keys of the SAP solutions, which satisfy (4.5), must be secure against the LLL attacks in the dimension $n \geq 70$ and $m \geq 30$.

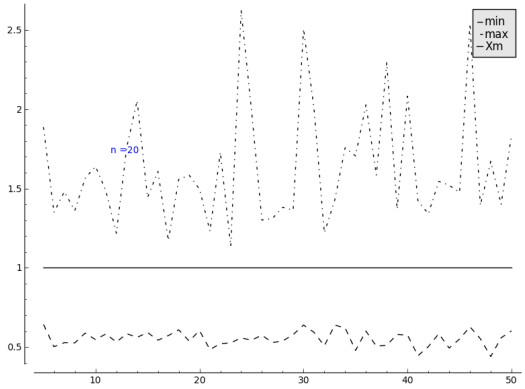

FIGURE 1. n=20

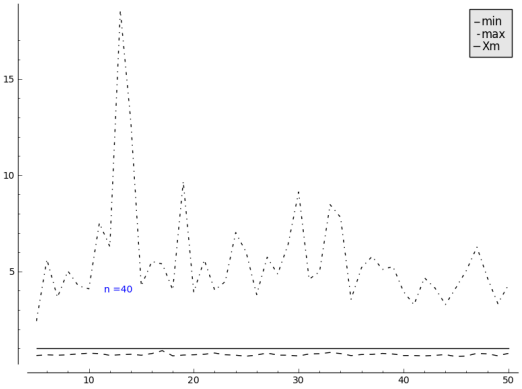

FIGURE 2. n=40

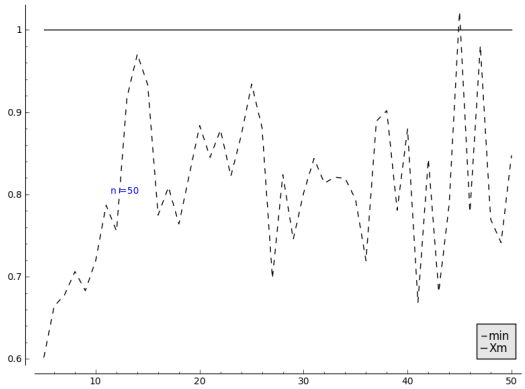

FIGURE 3. n=50

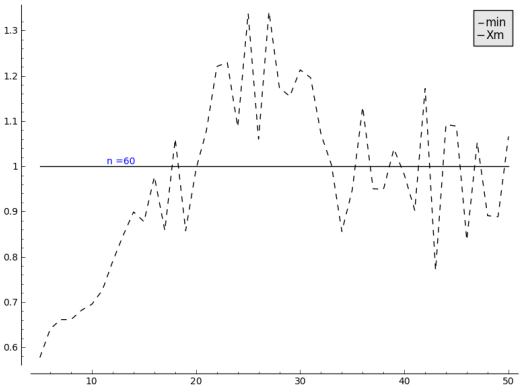

FIGURE 4. n=60

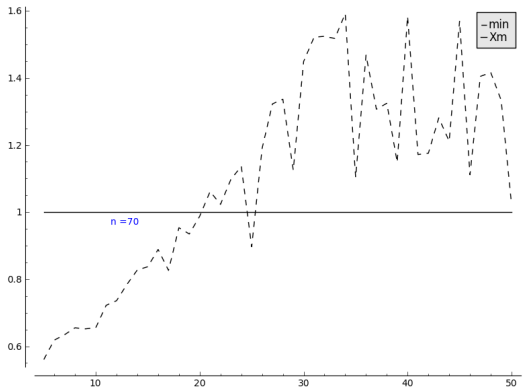

FIGURE 5. n=70

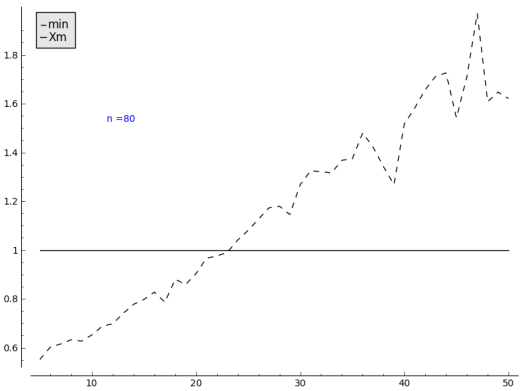

FIGURE 6. n=80

References

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

[2] H. Inoue, *p-adic continued fractions and theory of p-adic approximation lattices*, to appear in Linear Nonlinear Anal.

[3] H. Inoue and K. Naito, *The shortest vector problems in p-adic lattices and simultaneous approximation problems of p-adic numbers*, to appear in Linear Nonlinear Anal.

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

[5] V. Jarnik, *Über einen p-adischen Übertragungssatz*, Monatsh. Math. Phys. **48** (1939), 277–287 .

[6] J. C. Lagarias, *The computational complexity of simultaneous diophantine approximation problems*, SIAM Journal on Computing, *14* (1985), 196–209.

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

[8] D. Micciancio and O. Regev, *Lattice-Based Cryptography*, in: Post Quantum Cryptography, D.J. Bernstein; J. Buchmann; E. Dahmen (Eds.), Springer 2009, pp. 147–191.

[9] P.Q. Nguyen and B. Vallee (Eds.), *The LLL Algorithm, Survey and Applications*, Springer 2010.

[10] 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

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@gamil.com

Shoichi Kamada
Department of Mathematics, Graduate School of Science and Technology, Kumamoto University, Chuo-ku, Kurokami 2-39-1, Kumamoto, Japan
E-mail address: 168d9309@st.kumamoto-u.ac.jp

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