TRANSFERENCE PRINCIPLE ON SIMULTANEOUS APPROXIMATION PROBLEMS OF $p$-ADIC NUMBERS AND CONSTRUCTION OF LATTICE BASED CRYPTOSYSTEMS

HIROHITO INOUE, SHOICHI KAMADA AND KOICHIRO NAITO

GRADUATE SCHOOL OF SCIENCE AND TECHNOLOGY, KUMAMOTO UNIVERSITY

1. INTRODUCTION

In this paper we study the two types, named the 1st type and the 2nd type, of simultaneous approximations problems (SAP) of $p$-adic numbers, constructing multi-dimensional $p$-adic approximation lattices. It is known that the transference principle gives the inequality relations between the exponents given by the SAP of $p$-adic numbers (cf. [1]). First we estimate the $l_\infty$ norms of the solutions of the 1st type and the 2nd type SAP theoretically. For these approximation problems we construct basis matrices, given by $m$th 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 (cf. [8], [9], [10]), we construct the algorithm, which gives the solutions of the 2nd type SAP from the solutions of the 1st type SAP.

Next we propose a new lattice based cryptosystem where we choose a $n$-tuple of $p$-adic integers as public keys and we set the 2nd type SAP solutions of these numbers as common private keys, the security of which depends on NP-hardness of SAP (see [7]).

Our plan of this paper is as follows. In section 2 we introduce the $p$-adic approximation lattices and we estimate the $l_\infty$ norm of $p$-adic solutions of the 1st type SAP. In section 3 we treat the 2nd type SAP and we give the duality relation between these two types of SAP solutions. In section 4 we propose a new lattice based cryptosystem as an application.

2. $p$-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 ring 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 $\Xi = \{\xi_1, \xi_2, \ldots, \xi_n\}$ be a $n$-tuple of $p$-adic integers.

**Definition 2.1.** 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 $a_{0,j}, a_{1,j}, \ldots, a_{n,j}$.

For a positive integer $m$ we define the $p$-adic approximation lattice $\Gamma_m$ by

$$(2.1) \quad \Gamma_m = \{(a_0, a_1, \ldots, a_n) \in \mathbb{Z}^{n+1} : |a_0 + a_1\xi_1 + \cdots + a_n\xi_n|_p \leq p^{-m}\}.$$

When a $p$-adic integer $\xi_i$ has the $p$-adic expansion

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

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

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

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

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

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

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

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

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

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

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 is known that the shortest vector $b_0$ in $B$
satisfies

\[(2.3) \quad \|b_0\|_2 \leq \sqrt{n+1} |\det(B)|^\frac{1}{n+1} \left( \frac{2}{\sqrt{4\delta} - 1} \right)^n\]

\[= \sqrt{n+1} |\det(B_m)|^\frac{1}{n+1} \left( \frac{2}{\sqrt{4\delta} - 1} \right)^n\]

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

(cf. [8]).

In [4] we have given the upper bound of the minimum norm value \(\lambda_1^{(\infty)}(\Gamma_m) (= \lambda_1^{(\infty)}(B_m))\) by using the famous Dirichlet principle.

**Theorem 2.2.** 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

\[(2.4) \quad 0 < |a_{0,m} + a_{1,m}\xi_1 + \cdots + a_{n,m}\xi_n|_p \leq p^{-m},\]

\[(2.5) \quad \max_{0 \leq i \leq n} |a_{i,m}| \leq p^\frac{m}{n+1}.

Consequently, we have

\[(2.6) \quad \lambda_1^{(\infty)}(\Gamma_m) \leq p^\frac{m}{n+1} = \det(\Gamma_m)^\frac{1}{n+1}.

3. 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 3.1.** We denote by \(\nu_n(\Xi)\) the supremum of the real numbers \(\nu\) such that, for some infinitely many real numbers \(Y_j\), which goes to infinity, the inequalities

\[0 < \max_{1 \leq i \leq n} |a_{0,j}\xi_i - a_{i,j}|_p \leq Y_j^{-\nu-1},\]

\[\max_{0 \leq i \leq n} |a_{i,j}| \leq Y_j,

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

For a positive integer \(m\) we define the p-adic approximation lattice \(\Lambda_m\) by

\[(3.1) \quad \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}\}.

For a p-adic integer \(\xi_i\) with its p-adic expansion

\[\xi_i = \sum_{k=0}^{\infty} x_{i,k}p^k, \quad 0 \leq x_{i,k} \leq p - 1\]
and the $m$-th order approximation $\xi_{i,m}$ given by (2.2) we can construct the basis 
\{ $b'_{0,m}, b'_{1,m}, \ldots, b'_{n,m}$ \} $\subset \mathbb{Z}^{n+1}$ of the lattice $\Lambda_{m}$ where 
\[
\begin{align*}
 b'_{0,m} &= (1, \xi_{1,m}, \xi_{2,m}, \ldots, \xi_{n,m})^t, \\
 b'_{1,m} &= (0, -p^m, 0, \ldots, 0)^t, \\
 b'_{2,m} &= (0, 0, -p^m, 0, \ldots, 0)^t, \\
 &\vdots \\
 b'_{n,m} &= (0, 0, \ldots, 0, -p^m)^t.
\end{align*}
\]

In fact, we have $b'_{k,m} \in \Lambda_{m}$, $\forall k$, since we can estimate 
\[|\xi_{k,m} - \xi_{k}|_p \leq p^{-m}.\]

For $B'_m = (b'_{0,m} b'_{1,m} \ldots b'_{n,m})$ we have 
\[
B'_m = \begin{pmatrix}
1 & 0 & 0 & \cdots & 0 \\
\xi_{1,m} & -p^m & 0 & \cdots & 0 \\
\xi_{2,m} & 0 & -p^m & \cdots & 0 \\
& \vdots & & \ddots & \vdots \\
\xi_{n,m} & 0 & 0 & \cdots & -p^m
\end{pmatrix}, \quad |\det(B'_m)| = p^{nm}.
\]

Applying the LLL algorithm for $\delta \in (1/4, 1)$, we denote \{ $b'_0, b'_1, \ldots, b'_n$ \} a reduced basis and $B' = (b'_0 \ b'_1 \ldots \ b'_n)$. The shortest vector $b'_0$ in $B'$ satisfies the following estimates, which are similar to (2.3), 
\[
\begin{align*}
(3.2) \quad \|b'_0\|_2 &\leq \sqrt{n+1} |\det(B')|^{\frac{1}{n+1}} \left(\frac{2}{\sqrt{4\delta - 1}}\right)^n \\
&= \sqrt{n+1} |\det(B'_m)|^{\frac{1}{n+1}} \left(\frac{2}{\sqrt{4\delta - 1}}\right)^n \\
&= \sqrt{n+1} p^{\frac{mn}{n+1}} \left(\frac{2}{\sqrt{4\delta - 1}}\right)^n.
\end{align*}
\]

In [5] we have given the estimates of the minimum norm value $\lambda_1^{(\infty)}(\Lambda_m) (= \lambda_1^{(\infty)}(L(B'_m)))$.

**Theorem 3.2.** 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 
\[
(3.3) \quad 0 < \max_{1 \leq i \leq n} |a_{0,m}\xi_i - a_{i,m}|_p \leq p^{-m},
\]
\[
(3.4) \quad \max_{0 \leq i \leq n} |a_{i,m}| \leq p^{\frac{nm}{n+1}}.
\]

Consequently, we have 
\[
(3.5) \quad \lambda_1^{(\infty)}(\Lambda_m) \leq p^{\frac{nm}{n+1}} = \det(\Lambda_m)^{\frac{1}{n+1}}
\]
and 
\[
(3.6) \quad \nu_n(\Xi) \geq \frac{1}{n}.
\]

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 3.3.** 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 $B = B_mU$ and $B' = B'_mV$ for some unimodular matrices $U, V$. Then the following duality relation

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

holds.

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

$$B'_m = p^m(B'_m)^{-1}.$$

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

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

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 (3.7) that we can construct an algorithm, which gives the 2nd SAP solutions from the 1st SAP solutions by applying the LLL algorithm. (For details, see [5].)

### 4. Cryptosystem

In this section we propose a new cryptosystem, the security of which depends on the hardness of solving the SAP in the higher dimensions. Now we assume that Alice wants to send a message to Bob in this cryptosystem.

For a $n$-tuple of public keys $\xi_i \in \mathbb{Z}_p, i = 1, \ldots, n$, let $B' = (b_0', b_1', \ldots, b_n')$ be a reduced basis given by applying the LLL algorithm as in section 3 from the lattice basis matrix

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

For a constant $K > 0$ and a vector of random integers $(s_0, \ldots, s_n) \in \mathbb{Z}^n : |s_i| \leq K, \forall i$, we define the secret keys $(a_0, a_1, \ldots, a_n)$ by

$$(a_0, a_1, \ldots, a_n) = \sum_{i=0}^{n} s_i b'_i.$$ 

Let the secret key $a_i$ be the sum of $\alpha_i$ and $\beta_i$, that is

$$a_i = \alpha_i + \beta_i, \ \alpha_i, \beta_i \in \mathbb{Z}, \ i = 0, 1, \ldots, n.$$
Alice has the secret key \(\{\alpha_i\}\) and Bob has the secret key \(\{\beta_i\}\).

**Encryption**

Alice wants to send to Bob a list of messages given by

\[
x^{(i)} = \sum_{k=0}^{m-1} x_k^{(i)} p^k, \quad 0 \leq x_k^{(i)} \leq p-1, \quad i=1, \ldots, n.
\]

Alice constructs the ciphertext \(c_A\) by

\[
c_A = (c_{1,A}, c_{2,A}, \ldots, c_{m,A}) \quad \text{where} \quad c_{i,A} = \alpha_0 \xi_i - \alpha_i + x^{(i)}
\]

and she sends the ciphertext \(c_A\) to Bob.

**Decryption**

Bob takes the sum of \(c_A\) and \(c_B\), given by

\[
c_B = (c_{1,B}, \ldots, c_{n,B}) \quad \text{where} \quad c_{i,B} = \beta_0 \xi_i - \beta_i,
\]

\[
c = (c_1, \ldots, c_n) = c_A + c_B \quad \text{where} \quad c_i = \alpha_0 \xi_i - \alpha_i + x^{(i)}.
\]

Then he can easily obtain the messages \(x^{(i)}\) by calculating

\[
c_i \equiv x^{(i)} \mod p^m.
\]

**REFERENCES**

Department of Mathematics,
Graduate School of Science and Technology,
Kumamoto University,
Kurokami 2-39-1, Kumamoto, Japan
140d8162@st.kumamoto-u.ac.jp

Department of Applied Mathematics,
Graduate School of Science and Technology,
Kumamoto University,
132d9307@st.kumamoto-u.ac.jp

Department of Applied Mathematics,
Graduate School of Science and Technology,
Kumamoto University,
knaito@gpo.kumamoto-u.ac.jp

熊本大学大学院・自然科学研究科 鎌田 祥一

熊本大学大学院・自然科学研究科 井上 裕仁

熊本大学大学院・自然科学研究科 内藤 幸一郎