数理解析研究所講究録
第2011巻 2016年 57-63

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_∞ norms of the solutions of the 1st type and the 2nd type SAP theoretically. 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 (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_∞ 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

2010 *Mathematics Subject Classification.* 11E95, 11A55, 14G50.
Key words and phrases. P-adic theory, LLL algorithm, Cryptography.

$|p|_p = p^{-1}$. 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 ring 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 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

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

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

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

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

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

$$\xi_{i,m} = \sum_{k=0}^{m-1} x_{i,k}p^k. \tag{2.2}$$

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

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

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

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

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

satisfies

$$\begin{aligned} \|b_0\|_2 &\leq \sqrt{n+1}\ |\det(B)|^{\frac{1}{n+1}} \left(\frac{2}{\sqrt{4\delta-1}}\right)^n \\ &= \sqrt{n+1}\ |\det(B_m)|^{\frac{1}{n+1}} \left(\frac{2}{\sqrt{4\delta-1}}\right)^n \\ &= \sqrt{n+1}\ p^{\frac{m}{n+1}} \left(\frac{2}{\sqrt{4\delta-1}}\right)^n \end{aligned} \tag{2.3}$$

(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*

$$0 < |a_{0,m} + a_{1,m}\xi_1 + \cdots + a_{n,m}\xi_n|_p \leq p^{-m}, \tag{2.4}$$

$$\max_{0\leq i\leq n} |a_{i,m}| \leq p^{\frac{m}{n+1}}. \tag{2.5}$$

Consequently, we have

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

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

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

$$\Lambda_m = \{(a_0, a_1, \ldots, a_n) \in \mathbb{Z}^{n+1} : \max_{1\leq i\leq n} |a_0\xi_i - a_i|_p \leq p^{-m}\}. \tag{3.1}$$

For a p-adic integer ξ_i with its p-adic expansion

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

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 Λ_m where

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

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

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

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),

$$\begin{aligned} \|b'_0\|_2 &\leq \sqrt{n+1}\ |\det(B')|^{\frac{1}{n+1}} \left(\frac{2}{\sqrt{4\delta - 1}}\right)^n \\ &= \sqrt{n+1}\ |\det(B'_m)|^{\frac{1}{n+1}} \left(\frac{2}{\sqrt{4\delta - 1}}\right)^n \\ &= \sqrt{n+1}\ p^{\frac{mn}{n+1}} \left(\frac{2}{\sqrt{4\delta - 1}}\right)^n. \end{aligned} \tag{3.2}$$

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*

$$0 < \max_{1 \leq i \leq n} |a_{0,m}\xi_i - a_{i,m}|_p \leq p^{-m}, \tag{3.3}$$

$$\max_{0 \leq i \leq n} |a_{i,m}| \leq p^{\frac{nm}{n+1}}. \tag{3.4}$$

Consequently, we have

$$\lambda_1^{(\infty)}(\Lambda_m) \leq p^{\frac{nm}{n+1}} = \det(\Lambda_m)^{\frac{1}{n+1}} \tag{3.5}$$

and

$$\nu_n(\Xi) \geq \frac{1}{n}. \tag{3.6}$$

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 $B = B_m U$ and $B' = B'_m V$ for some unimodular matrices U, V. Then the following duality relation*

$$L(B') = \Lambda_m = p^m \Gamma_m^* = L(p^m (B^t)^{-1}) \tag{3.7}$$

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 (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

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

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

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

Let the secret key a_i be the sum of α_i and β_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

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

Alice constructs the ciphertext $\mathbf{c}_A$ by

$$\mathbf{c}_A = (c_{1,A}, c_{2,A}, ..., c_{n,A}),\ c_{i,A} = \alpha_0 \xi_i - \alpha_i + x^{(i)}$$

and she sends the ciphertext $\mathbf{c}_A$ to Bob.

Decryption

Bob takes the sum of $\mathbf{c}_A$ and $\mathbf{c}_B$, given by

$$\mathbf{c}_B = (c_{1,B}, ..., c_{n,B}),\ c_{i,B} = \beta_0 \xi_i - \beta_i,$$

$$\mathbf{c} = (c_1, ..., c_n) = \mathbf{c}_A + \mathbf{c}_B,\ c_i = a_0 \xi_i - a_i + x^{(i)}.$$

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

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

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*, Proceedings of the 8th International Conference on Nonlinear Analysis and Convex Analysis 2013, 139–153.
3. H. Inoue and K. Naito, *Recurrent properties of quasi-periodic dynamical systems with multiple frequencies of p-adic Liouville numbers*, P-Adic Numbers, Ultrametric Analysis, and Applications **6** (2014), 195–206.
4. H.Inoue and K.Naito, *The shortest vector problems in p-adic lattices and simultaneous approximation problems of p-adic numbers*, to appear in Proc. of ICM Satellite Conference 2014: the 4th Asian Conf. on Nonlinear Analysis and Optimization 2014 (Taipei).
5. 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 Proc. of ICM Satellite Conference 2014: the 4th Asian Conf. on Nonlinear Analysis and Optimization 2014 (Taipei).
6. H.Inoue, S.Kamada and K.Naito, *Simultaneous approximations of p-adic numbers and their applications to cryptography*, to appear in Proc. of ICM Satellite Conference 2014: the 4th Asian Conf. on Nonlinear Analysis and Optimization 2014 (Taipei).
7. J. C. Lagarias, *The computational complexity of simultaneous diophantine approximation problems*, SIAM Journal on Computing, *14* (1985), 196–209.
8. D. Micciancio and S. Goldwasser, "Complexity of Lattice Problems, a Cryptographic Perspective", Springer International Series in Engineering and Computer Science, vol. 671. Springer, 2002
9. D. Micciancio and O. Regev, *Lattice-Based Cryptography*, in "Post Quantum Cryptography", D.J. Bernstein; J. Buchmann; E. Dahmen (Eds.), Springer 2009, 147–191.
10. P.Q. Nguyen and B. Vallee (Eds.), "The LLL Algorithm, Survey and Applications", Springer 2010.

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

熊本大学大学院・自然科学研究科　鎌田　祥一

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

熊本大学大学院・自然科学研究科　井上 裕仁

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　内藤 幸一郎