J Syst Sci Complex (2022) 35: 1191–1200

On Some Computational Problems in Local Fields*

DENG Yingpu · LUO Lixia · PAN Yanbin · XIAO Guanju

DOI: 10.1007/s11424-021-0074-8
Received: 8 April 2020

Abstract Lattices in Euclidean spaces are important research objects in geometric number theory, and they have important applications in many areas, such as cryptology. The shortest vector problem (SVP) and the closest vector problem (CVP) are two famous computational problems about lattices. In this paper, we consider p-adic lattices in local fields, and define the p-adic analogues of SVP and CVP in local fields. The authors find that, in contrast with lattices in Euclidean spaces, the situation is different and interesting. The SVP in Euclidean spaces corresponds to the Longest Vector Problem (LVP) in local fields. The authors develop relevant algorithms, indicating that these problems are computable.

Keywords CVP, lattice, LVP, local field, SVP.

1 Introduction

Let $\mathbb{R}$ be the field of real numbers, and let n be a positive integer. Denote $\mathbb{R}^n = \{(x_1, x_2, \cdots, x_n) \mid x_i \in \mathbb{R}, 1 \leq i \leq n\}$. Let $\| \cdot \|$ be a norm on $\mathbb{R}^n$, namely, for $a \in \mathbb{R}, \boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^n$, $\| \boldsymbol{x} \|$ is a nonnegative real number satisfying: 1) $\| \boldsymbol{x} \| = 0$ if and only if $\boldsymbol{x} = \boldsymbol{0}$; 2) $\| a\boldsymbol{x} \| = | a | \| \boldsymbol{x} \|$; 3) $\| \boldsymbol{x} + \boldsymbol{y} \| \leq \| \boldsymbol{x} \| + \| \boldsymbol{y} \|$. An important family of norm functions is given by the $l_p (1 \leq p \leq \infty)$ norms. For any real $p \geq 1$, the l_p norm of a vector $\boldsymbol{x} = (x_1, x_2, \cdots, x_n) \in \mathbb{R}^n$ is

$$\| \boldsymbol{x} \|_p = \left(\sum_{i=1}^{n} | x_i |^p \right)^{\frac{1}{p}}.$$

And the l_∞ norm is

$$\| \boldsymbol{x} \|_\infty = \max_{1 \leq i \leq n} | x_i | .$$

DENG Yingpu · LUO Lixia · PAN Yanbin · XIAO Guanju
Key Laboratory of Mathematics Mechanization, NCMIS, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190*, China; School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing* 100049*, China.*
Email: dengyp@amss.ac.cn; luolixia@amss.ac.cn; panyanbin@amss.ac.cn; gjXiao@amss.ac.cn.
*This research was supported by the National Key Research and Development Project under Grant No. 2018YFA0704705.
◇ *This paper was recommended for publication by Editor MANUEL Kauers.*

Let m be a positive integer with $1 \leq m \leq n$. Let $\alpha_1, \alpha_2, \cdots, \alpha_m \in \mathbb{R}^n$ be m $\mathbb{R}$-linearly independent vectors. A lattice in $\mathbb{R}^n$ is the set

$$\mathcal{L}(\alpha_1, \alpha_2, \cdots, \alpha_m) = \left\{ \sum_{i=1}^{m} a_i \alpha_i \mid a_i \in \mathbb{Z}, 1 \leq i \leq m \right\}$$

of all integral linear combinations of $\alpha_1, \alpha_2, \cdots, \alpha_m$. The integers m and n are called the rank and dimension of the lattice, respectively. When $n = m$, we say that the lattice is full rank. A lattice in $\mathbb{R}^n$ is a discrete additive subgroup of it, and the reverse is also true. See [1] for a proof of this fact.

Given a lattice $\mathcal{L}(\alpha_1, \alpha_2, \cdots, \alpha_m)$ in $\mathbb{R}^n$, and a norm $\| \cdot \|$ on $\mathbb{R}^n$, there are two famous computational problems, i.e., the shortest vector problem (SVP) and the closest vector problem (CVP). SVP is to find a nonzero lattice vector $\boldsymbol{v} \in \mathcal{L}(\alpha_1, \alpha_2, \cdots, \alpha_m)$ such that

$$\| \boldsymbol{v} \| = \min\{ \| \boldsymbol{x} \| \mid 0 \neq \boldsymbol{x} \in \mathcal{L}(\alpha_1, \alpha_2, \cdots, \alpha_m) \}.$$

Given a target vector $\boldsymbol{t} \in \mathbb{R}^n$ and a lattice $\mathcal{L}(\alpha_1, \alpha_2, \cdots, \alpha_m)$ in $\mathbb{R}^n$. CVP is to find a lattice vector $\boldsymbol{v} \in \mathcal{L}(\alpha_1, \alpha_2, \cdots, \alpha_m)$ such that

$$\| \boldsymbol{t} - \boldsymbol{v} \| = \min\{ \| \boldsymbol{t} - \boldsymbol{x} \| \mid \boldsymbol{x} \in \mathcal{L}(\alpha_1, \alpha_2, \cdots, \alpha_m) \}.$$

Note that, since the zero vector is in fact the shortest vector in a lattice, SVP is to find a second shortest vector in a lattice.

Lattices are important research objects in geometric number theory, see [2]. Algorithmic studies of SVP and CVP can be found in [3]. Lattices in Euclidean spaces have important applications in many areas, such as cryptology. The reader can easily find numerous literatures in recent cryptographic conference proceedings, such as Crypto, Eurocrypt, Asiacrypt, etc.

We know that $\mathbb{R}$ is the completion of the field $\mathbb{Q}$ of rational numbers with respect to the usual absolute value. Let p be a prime number, and let $\mathbb{Q}_p$ be the completion of $\mathbb{Q}$ with respect to the p-adic absolute value. Let n be a positive integer, and let K be an extension field of $\mathbb{Q}_p$ of degree n. We know that the p-adic absolute value on $\mathbb{Q}_p$ can be extended uniquely to K. In this paper, we define so-called p-adic lattices in K, and consider the p-adic analogues of SVP and CVP in the local field K. We find that, in contrast with lattices in Euclidean spaces, the situation is different and interesting. The SVP in Euclidean spaces corresponds to the Longest Vector Problem (LVP) in local fields. Usually, p-adic lattices are defined as free $\mathbb{Z}_p$-modules in a finite dimensional vector space over $\mathbb{Q}_p$. We embed p-adic lattices into an extension field K of $\mathbb{Q}_p$ so that we can use the natural norm in K to derive good properties of relevant problems. However, $\mathbb{R}^n$ can be viewed as a field only when $n = 1, 2, 4$. The case $n = 2$ is the field of complex numbers and when $n = 4$, the field is non-commutative (i.e., Hamilton quaternions). This is the famous Frobenius Theorem. We develop relevant algorithms, indicating that these problems are computable.

The major motivation of this paper is the post quantum cryptography. Due to Peter Shor's quantum polynomial time algorithms for integer factorization and discrete logarithm, classical

public-key cryptosystems such as RSA and ElGamal would be broken under future quantum computer. NIST has initiated the solicitation of standard of post quantum cryptography[4]. New hard computational problems have been proposed, such as isogeny between elliptic curves[5, 6]. Lattices in Euclidean spaces have obtained extensive study in recent years[3]. However, p-adic lattices do not gain any attention. We propose new computational problems, and these problems may be hard. Further algorithmic improvement and complexity study are our future research direction. The potential construction of cryptographic schemes based on these problems is also a natural research direction.

The paper is organized as follows. We give some necessary basic facts about local fields in Section 2. We consider the p-adic analogues of the shortest vector problem and the closest vector problem in local fields in Sections 3, 4, respectively. We describe a simple relationship between the discriminant of a lattice and λ_2 in Section 5.

2 Basic Facts About Local Fields

In this section, we recall some basic facts about local fields, for detailed study of local fields, see [7–9].

Let p be a prime number. For $x \in \mathbb{Q}$ with $x \neq 0$, write $x = p^t \frac{a}{b}$ with $t, a, b \in \mathbb{Z}$ and $p \nmid ab$. Define $\mid x \mid_p = p^{-t}$ and $\mid 0 \mid_p = 0$. Then $\mid \cdot \mid_p$ is a non-Archimedean absolute value on $\mathbb{Q}$. Namely, we have: 1) $\mid x \mid_p \geq 0$ and $\mid x \mid_p = 0$ if and only if $x=0$; 2) $\mid xy \mid_p = \mid x \mid_p \mid y \mid_p$; 3) $\mid x + y \mid_p \leq \max(\mid x \mid_p, \mid y \mid_p)$. If $\mid x \mid_p \neq \mid y \mid_p$, then $\mid x + y \mid_p = \max(\mid x \mid_p, \mid y \mid_p)$.

Let $\mathbb{Q}_p$ be the completion of $\mathbb{Q}$ with respect to $\mid \cdot \mid_p$. Denote $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid\mid x \mid_p \leq 1\}$. $\mathbb{Z}_p$ is a discrete valuation ring, it has a unique nonzero principal maximal ideal $p\mathbb{Z}_p$ and p is called a uniformizer of $\mathbb{Q}_p$. The unit group of $\mathbb{Z}_p$ is $\mathbb{Z}_p^\times = \{x \in \mathbb{Q}_p \mid\mid x \mid_p = 1\}$. The residue class field $\mathbb{Z}_p/p\mathbb{Z}_p$ is a finite field with p elements. We have $\mathbb{Z}_p = \{\sum_{i=0}^{\infty} a_i p^i \mid a_i \in \{0, 1, \cdots, p-1\}, i \geq 0\}$ and $\mathbb{Q}_p = \{\sum_{i=j}^{\infty} a_i p^i \mid a_i \in \{0, 1, \cdots, p-1\}, i \geq j, j \in \mathbb{Z}\}$. $\mathbb{Z}_p$ is compact and $\mathbb{Q}_p$ is locally compact.

Let n be a positive integer, and let K be an extension field of $\mathbb{Q}_p$ of degree n. We fix some algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ and view K as a subfield of $\overline{\mathbb{Q}}_p$. Such K exists, for example, let $K = \mathbb{Q}_p(\alpha)$ with $\alpha^n = p$. Because $X^n - p$ is an Eisenstein polynomial over $\mathbb{Q}_p$, it is irreducible over $\mathbb{Q}_p$, so K has degree n over $\mathbb{Q}_p$. Further, there are only finitely many extension fields of $\mathbb{Q}_p$ of degree n contained in $\overline{\mathbb{Q}}_p$, see [10]. The p-adic absolute value (or norm) $\mid \cdot \mid_p$ on $\mathbb{Q}_p$ can be extended uniquely to K, i.e., for $x \in K$, we have $\mid x \mid_p = \mid N_{K/\mathbb{Q}_p}(x) \mid_p^{\frac{1}{n}}$, where $N_{K/\mathbb{Q}_p}$ is the norm map from K to $\mathbb{Q}_p$. And K is complete with respect to $\mid \cdot \mid_p$. See [8] for a proof.

Denote $\mathcal{O}_K = \{x \in K \mid\mid x \mid_p \leq 1\}$. $\mathcal{O}_K$ is also a discrete valuation ring, it has a unique nonzero principal maximal ideal $\pi\mathcal{O}_K$ and π is called a uniformizer of K. $\mathcal{O}_K$ is a free $\mathbb{Z}_p$-module of rank n. $\mathcal{O}_K$ is compact and K is locally compact. The unit group of $\mathcal{O}_K$ is $\mathcal{O}_K^\times = \{x \in K \mid\mid x \mid_p = 1\}$. The residue class field $\mathcal{O}_K/\pi\mathcal{O}_K$ is a finite extension of $\mathbb{Z}_p/p\mathbb{Z}_p$. Call the positive integer $f = [\mathcal{O}_K/\pi\mathcal{O}_K : \mathbb{Z}_p/p\mathbb{Z}_p]$ the residue field degree of $K/\mathbb{Q}_p$. As ideals in $\mathcal{O}_K$, we have $p\mathcal{O}_K = \pi^e\mathcal{O}_K$. Call the positive integer e the ramification index of $K/\mathbb{Q}_p$. We have $n = [K : \mathbb{Q}_p] = ef$. When $e = 1$, the extension $K/\mathbb{Q}_p$ is unramified, and when $e = n$, $K/\mathbb{Q}_p$ is

totally ramified. Each element x of the multiplicative group $K^\times$ of nonzero elements of K can be written uniquely as $x = u\pi^t$ with $u \in \mathcal{O}_K^\times$ and $t \in \mathbb{Z}$. We have $p = u\pi^e$ with $u \in \mathcal{O}_K^\times$, so $\mid \pi \mid_p = p^{-\frac{1}{e}}$. The valuation group of K is

$$\{\mid x \mid_p \mid x \in K^\times\} = p^{\frac{\mathbb{Z}}{e}}.$$

3 Longest Vector Problem in Local Fields

As in the previous section, let p be a prime number, and let K be an extension field of $\mathbb{Q}_p$ of degree n, where n is a positive integer. Let m be a positive integer with $1 \le m \le n$. Let $\alpha_1, \alpha_2, \cdots, \alpha_m \in K$ be m many $\mathbb{Q}_p$-linearly independent vectors. A lattice in K is the set

$$\mathcal{L}(\alpha_1, \alpha_2, \cdots, \alpha_m) = \left\{ \sum_{i=1}^{m} a_i \alpha_i \mid a_i \in \mathbb{Z}_p, 1 \le i \le m \right\}$$

of all $\mathbb{Z}_p$-linear combinations of $\alpha_1, \alpha_2, \cdots, \alpha_m$. The sequence of vectors $\alpha_1, \alpha_2, \cdots, \alpha_m$ is called a basis of the lattice $\mathcal{L}(\alpha_1, \alpha_2, \cdots, \alpha_m)$. The integers m and n are called the rank and dimension of the lattice, respectively. When $n = m$, we say that the lattice is full rank.

Remark Usually, p-adic lattices are defined as follows, see [9, 11]. Let V be a finite dimensional vector space over $\mathbb{Q}_p$. A p-adic lattice in V is a free $\mathbb{Z}_p$-module in V. We embed p-adic lattices into an extension field K of $\mathbb{Q}_p$ so that we can use the natural norm in K. Since all norms on a finite dimensional vector space over a locally compact field are equivalent, see [7], our convention does not matter.

Lemma 3.1 *The lattice $\mathcal{L} = \mathcal{L}(\alpha_1, \alpha_2, \cdots, \alpha_m)$ is compact in K.*

Proof Since $\mid \cdot \mid_p$ makes $\mathcal{L}$ a metric space, compactness is equivalent to sequential compactness. We have therefore to show that every sequence $\{A_j\}_{j=1}^{\infty}$ of elements of $\mathcal{L}$ has a convergent subsequence. The proof applies the well-known "diagonal process" to the representation

$$A_j = \sum_{i=1}^{m} a_j^{(i)} \alpha_i.$$

Since $a_j^{(i)} \in \mathbb{Z}_p$ and $\mathbb{Z}_p$ is compact, there is a convergent subsequence $a_{n_{j1}}^{(1)}$ of $a_j^{(1)}$. Also, there is a convergent subsequence $a_{n_{j2}}^{(2)}$ of $a_{n_{j1}}^{(2)}$, there is a convergent subsequence $a_{n_{j3}}^{(3)}$ of $a_{n_{j2}}^{(3)}$, and so on. Finally, we obtain convergent subsequences $a_{n_{jm}}^{(i)}$ of $a_j^{(i)}$ for each $1 \le i \le m$. Then

$$\sum_{i=1}^{m} a_{n_{jm}}^{(i)} \alpha_i$$

is a convergent subsequence of A_j. ∎

For any element $\alpha = \sum_{i=1}^{m} a_i \alpha_i \in \mathcal{L}$, since each $a_i \in \mathbb{Z}_p$, we have

$$\mid \alpha \mid_p = \left| \sum_{i=1}^{m} a_i \alpha_i \right|_p \le \max_{1 \le i \le m} (\mid a_i \alpha_i \mid_p) \le \max_{1 \le i \le m} (\mid \alpha_i \mid_p).$$

This indicates that the length $\mid \alpha \mid_p$ of any element of the p-adic lattice $\mathcal{L}$ is bounded above. Since the valuation group of K is discrete, as a subset of K, the set of lengths of elements of the lattice $\mathcal{L}$ is also discrete. So we have the following definition.

Definition 3.2 Let $\mathcal{L} = \mathcal{L}(\alpha_1, \alpha_2, \cdots, \alpha_m)$ be a lattice in K. We define recursively a sequence of positive real numbers: $\lambda_1, \lambda_2, \cdots$ as follows:

$$\lambda_1 = \max_{1 \le i \le m} (\mid \alpha_i \mid_p),$$
$$\lambda_{j+1} = \max\{\mid x \mid_p \mid x \in \mathcal{L}, \mid x \mid_p < \lambda_j\} \text{ for } j \ge 1.$$

We have $\lambda_1 > \lambda_2 > \cdots$ and $\lim_{j \to \infty} \lambda_j = 0$. In fact, we have the following.

Lemma 3.3 *Let $\mathcal{L} = \mathcal{L}(\alpha_1, \alpha_2, \cdots, \alpha_m)$ be a lattice in K, and let $0 \neq \alpha \in \mathcal{L}$ be any nonzero element of the lattice. Then we have*

$$p^{-\frac{1}{e}} \lambda_j \ge \lambda_{j+1} \ge p^{-j} \mid \alpha \mid_p \quad \text{for } j \ge 1,$$

where e is the ramification index for $K/\mathbb{Q}_p$.

Proof Induction on j. Note that the valuation group of K is

$$\{\mid x \mid_p \mid x \in K^\times\} = p^{\frac{\mathbb{Z}}{e}}.$$

The proof is finished. ∎

Definition 3.4 Given a lattice $\mathcal{L} = \mathcal{L}(\alpha_1, \alpha_2, \cdots, \alpha_m)$ in K, the longest vector problem (LVP) is to find a lattice vector $v \in \mathcal{L}$ such that $\mid v \mid_p = \lambda_2$.

Of course, the longest vector v is not unique, for, if $u \in \mathbb{Z}_p^\times$, then uv is also a longest vector in the lattice $\mathcal{L}$.

Example 3.1 Put $\mathcal{L} = \mathcal{O}_K$. Since any nonzero element α of $\mathcal{O}_K$ can be written uniquely as $\alpha = u\pi^t$ with $u \in \mathcal{O}_K^\times$ and $t \in \mathbb{Z}, t \ge 0$, where π is a uniformizer of K. So $\mid \pi \mid_p = \lambda_2$ and the uniformizer π is a longest vector in $\mathcal{O}_K$. Since uniformizers are important for a local field K, so the LVP is significant.

Proposition 3.5 *Given a lattice $\mathcal{L} = \mathcal{L}(\alpha_1, \alpha_2, \cdots, \alpha_m)$ in K with $\mid \alpha_1 \mid_p \ge \mid \alpha_2 \mid_p \ge \cdots \ge \mid \alpha_m \mid_p$. If $K/\mathbb{Q}_p$ is unramified, then, for $j \ge 0$, $p^j \alpha_1 \in \mathcal{L}$ satisfying*

$$\mid p^j \alpha_1 \mid_p = \lambda_{j+1} = p^{-j} \lambda_1.$$

Proof Since the valuation group of K is $p^{\mathbb{Z}}$, the result follows. ∎

The above proposition shows that the LVP is easy to solve for an unramified extension $K/\mathbb{Q}_p$.

Theorem 3.6 *Given a lattice $\mathcal{L} = \mathcal{L}(\alpha_1, \alpha_2, \cdots, \alpha_m)$ in K. Fix an integer $j \ge 2$. There exists an algorithm to find a lattice vector $v_j \in \mathcal{L}$ satisfying*

$$\mid v_j \mid_p = \lambda_j.$$

The algorithm takes $O(p^{m(j-1)})$ many p-adic absolute value computations of elements of K.

Proof Without loss of generality, we can assume $\mid \alpha_1 \mid_p \geq \mid \alpha_2 \mid_p \geq \cdots \geq \mid \alpha_m \mid_p$. Let $\alpha \in \mathcal{L}$ be an arbitrary vector. Write

$$\alpha = \sum_{i=1}^{m} b_i \alpha_i + p^{j-1}\beta,$$

with $b_i \in \mathbb{Z}, 0 \leq b_i \leq p^{j-1} - 1, 1 \leq i \leq m$ and $\beta \in \mathcal{L}$. Set

$$S_j = \left\{ \sum_{i=1}^{m} b_i \alpha_i \mid b_i \in \mathbb{Z}, 0 \leq b_i \leq p^{j-1} - 1, 1 \leq i \leq m \right\} \bigcup \{p^{j-1}\alpha_1\}.$$

There are $p^{m(j-1)} + 1$ elements in S_j. By Lemma 3.3, we have $\mid p^{j-1}\beta \mid_p \leq \mid p^{j-1}\alpha_1 \mid_p \leq \lambda_j$. For $\mid \alpha \mid_p > \lambda_j$, we have $\mid \sum_{i=1}^{m} b_i\alpha_i \mid_p = \mid \alpha - p^{j-1}\beta \mid_p = \mid \alpha \mid_p > \lambda_j$. Hence, there are lattice vectors of length $\lambda_1, \lambda_2, \cdots, \lambda_{j-1}$ in S_j. If $\mid p^{j-1}\alpha_1 \mid_p < \lambda_j$, then $\mid p^{j-1}\beta \mid_p < \lambda_j$. Hence, for $\mid \alpha \mid_p = \lambda_j$, we have $\mid \sum_{i=1}^{m} b_i\alpha_i \mid_p = \mid \alpha - p^{j-1}\beta \mid_p = \lambda_j$. So there is a lattice vector of length λ_j in S_j. If $\mid p^{j-1}\alpha_1 \mid_p \geq \lambda_j$, then $\mid p^{j-1}\alpha_1 \mid_p = \lambda_j$. In this case, we have $v_j = p^{j-1}\alpha_1$. The assertion about the time of the algorithm is obvious. We ignore the time of comparing. ∎

We know, from the proof of the above theorem, that we can simultaneously find out the values $\lambda_2, \lambda_3, \cdots, \lambda_j$ and the corresponding vectors $v_2, v_3, \cdots, v_j$. From the proof of Theorem 3.6, the mentioned algorithm is a brute force searching algorithm. We provide a numerical example.

Example 3.2 Let $K = \mathbb{Q}_2(\sqrt[3]{2})$. Here $p = 2$ and $n = 3$. Let $\mathcal{L} = \mathbb{Z}_p + \mathbb{Z}_p\sqrt[3]{2}$ be a lattice in K of rank 2. Here $m = 2$ and $\alpha_1 = 1, \alpha_2 = \sqrt[3]{2}$. Since $\mid \alpha_2 \mid_2 = 2^{-\frac{1}{3}}$, we have $\lambda_1 = 1$. We want to find λ_3. Set

$$S_3 = \{i + j\alpha_2 \mid 0 \leq i, j \leq 3\} \bigcup \{4\}.$$

Using $N_{K/\mathbb{Q}_2}(i + j\alpha_2) = i^3 + 2j^3$, we can easily find out the 2-adic absolute value of each element of S_3. A calculation shows that $\lambda_2 = 2^{-\frac{1}{3}}, \lambda_3 = 2^{-1}$ and $v_2 = \alpha_2, v_3 = 2$.

4 Closest Vector Problem in Local Fields

As in the previous section, let p be a prime number, and let K be an extension field of $\mathbb{Q}_p$ of degree n, where n is a positive integer. Let m be a positive integer with $1 \leq m \leq n$. Let $\mathcal{L} = \mathcal{L}(\alpha_1, \alpha_2, \cdots, \alpha_m)$ be a lattice in K. In this section, we consider the p-adic analogue of the closest vector problem in K. Suppose $\mid \alpha_1 \mid_p \geq \mid \alpha_2 \mid_p \geq \cdots \geq \mid \alpha_m \mid_p$.

Given a target vector $t \in K$. Since the function

$$\mathcal{L} \longrightarrow \mathbb{R}, v \longmapsto \mid t - v \mid_p$$

is continuous on the compact set $\mathcal{L}$, it can take the minimum and maximum on $\mathcal{L}$. Set

$$\mu_{\min} = \min_{v \in \mathcal{L}} \mid t - v \mid_p \text{ and } \mu_{\max} = \max_{v \in \mathcal{L}} \mid t - v \mid_p .$$

If $t \in \mathcal{L}$, it is obvious that we have $\mu_{\min} = 0$ and $\mu_{\max} = \lambda_1$. Here λ_1 is the same as in Definition 3.2. So we below assume $t \notin \mathcal{L}$. Hence, $\mu_{\min} > 0$. Since the valuation group of K is discrete, the above distance function will take only finitely many values. So we have the following definition.

Definition 4.1 Let $\mathcal{L} = \mathcal{L}(\alpha_1, \alpha_2, \cdots, \alpha_m)$ be a lattice in K and let $t \in K - \mathcal{L}$ be a target vector. Define s positive real numbers $\mu_1 > \mu_2 > \cdots > \mu_s$ as follows, where s is a positive integer.

$$\{\mu_1, \mu_2, \cdots, \mu_s\} = \{| \ t - v \ |_p | \ v \in \mathcal{L}\}.$$

So $\mu_{\max} = \mu_1$ and $\mu_{\min} = \mu_s$.

If $| \ t \ |_p > \lambda_1$, since $| \ t - v \ |_p = | \ t \ |_p$, we have $\mu_{\min} = \mu_{\max} = | \ t \ |_p$. So we below assume $| \ t \ |_p \leq \lambda_1$.

Definition 4.2 Let $\mathcal{L} = \mathcal{L}(\alpha_1, \alpha_2, \cdots, \alpha_m)$ be a lattice in K and let $t \in K - \mathcal{L}$ be a target vector with $| \ t \ |_p \leq \lambda_1$. The closest vector problem (CVP) is to find a lattice vector $v \in \mathcal{L}$ such that

$$| \ t - v \ |_p = \mu_{\min}.$$

And the farthest vector problem (FVP) is to find a lattice vector $v \in \mathcal{L}$ such that

$$| \ t - v \ |_p = \mu_{\max}.$$

Proposition 4.3 *Let $\mathcal{L} = \mathcal{L}(\alpha_1, \alpha_2, \cdots, \alpha_m)$ be a lattice in K and let $t \in K - \mathcal{L}$ be a target vector with $| \ t \ |_p \leq \lambda_1$. Suppose $| \ t \ |_p \neq \lambda_j$ for any $j \geq 1$. Let $j_0 \geq 1$ be such that $\lambda_{j_0+1} < | \ t \ |_p < \lambda_{j_0}$. Then we have $s = j_0 + 1$ and $\mu_i = \lambda_i$ for $1 \leq i \leq j_0$ and $\mu_{j_0+1} = | \ t \ |_p$.*

Proof For any $v \in \mathcal{L}$, we have $| \ t - v \ |_p = \max(| \ t \ |_p, | \ v \ |_p)$. If $| \ v \ |_p \leq \lambda_{j_0+1}$, then $| \ t - v \ |_p = | \ t \ |_p$. If $| \ v \ |_p \geq \lambda_{j_0}$, then $| \ t - v \ |_p = | \ v \ |_p$. The result follows. ∎

Theorem 4.4 *Let $\mathcal{L} = \mathcal{L}(\alpha_1, \alpha_2, \cdots, \alpha_m)$ be a lattice in K and let $t \in K - \mathcal{L}$ be a target vector with $| \ t \ |_p \leq \lambda_1$. Suppose $| \ t \ |_p \neq \lambda_j$ for any $j \geq 1$. There exists an algorithm to find the values $\mu_i, 1 \leq i \leq s$ and the lattice vectors $v_i \in \mathcal{L}$ such that*

$$| \ t - v_i \ |_p = \mu_i \text{ for } 1 \leq i \leq s.$$

The algorithm takes $O\left(\left(\frac{\lambda_1}{|t|_p}\right)^{mn}\right)$ many p-adic absolute value computations of elements of K.

Proof By Lemma 3.3, $\lambda_{j+1} \leq p^{-\frac{1}{e}} \lambda_j$ for $j \geq 1$. Hence, $\lambda_j \leq p^{-\frac{j-1}{e}} \lambda_1$. Let $j_0 \geq 1$ be such that $\lambda_{j_0+1} < | \ t \ |_p < \lambda_{j_0}$. We have $| \ t \ |_p < p^{-\frac{j_0-1}{e}} \lambda_1$. Hence, $j_0 < e \log_p \left(\frac{\lambda_1}{|t|_p}\right) + 1 \leq n \log_p \left(\frac{\lambda_1}{|t|_p}\right) + 1$. Now the result follows from Proposition 4.3 and Theorem 3.6. ∎

Example 4.1 Let $\mathcal{L}$ be as in Example 3.2. Suppose $t = \alpha_2^2$. Since $| \ t \ |_2 = 2^{-\frac{2}{3}}$, we see $\lambda_3 < | \ t \ |_2 < \lambda_2$. So $s = 3$ and $\mu_1 = 1, \mu_2 = 2^{-\frac{1}{3}}, \mu_3 = 2^{-\frac{2}{3}}$.

Theorem 4.5 *Let $\mathcal{L} = \mathcal{L}(\alpha_1, \alpha_2, \cdots, \alpha_m)$ be a lattice in K and let $t \in K - \mathcal{L}$ be a target vector with $| \ t \ |_p \leq \lambda_1$. Suppose $| \ t \ |_p = \lambda_{j_0}$ for some $j_0 \geq 1$. Then $s \geq j_0$ and there exists an algorithm to find the values $\mu_i, 1 \leq i \leq j_0$ and the lattice vectors $v_i \in \mathcal{L}$ such that*

$$| \ t - v_i \ |_p = \mu_i \text{ for } 1 \leq i \leq j_0.$$

The algorithm takes $O\left(p^{-m}\left(\frac{\lambda_1}{|t|_p}\right)^{mn}\right)$ many p-adic absolute value computations of elements of K.

Proof Now by assumption $\mid t \mid_p = \lambda_{j_0}$ for some $j_0 \geq 1$. For $v \in \mathcal{L}$ with $\mid v \mid_p < \lambda_{j_0}$, then $\mid t - v \mid_p = \lambda_{j_0}$. For $v \in \mathcal{L}$ with $\mid v \mid_p > \lambda_{j_0}$, then $\mid t - v \mid_p = \mid v \mid_p$. For $v \in \mathcal{L}$ with $\mid v \mid_p = \lambda_{j_0}$, then $\mid t - v \mid_p \leq \lambda_{j_0}$. Hence, $s \geq j_0$, and $\mu_i = \lambda_i$ for $1 \leq i \leq j_0$. From the proof of Theorem 4.4, we have $j_0 \leq n \log_p \left(\frac{\lambda_1}{|t|_p}\right) + 1$. Since we can put $v_{j_0} = 0$, we only need to know the vectors $v_i \in \mathcal{L}$ such that $\mid v_i \mid_p = \lambda_i$ for $1 \leq i \leq j_0 - 1$, the theorem follows from Theorem 3.6. ∎

By the above Theorems 4.4 and 4.5, in any case, we always have $\mu_1 = \lambda_1$. When $\mid t \mid_p < \lambda_1$, we can put $v_1 = \alpha_1$; when $\mid t \mid_p = \lambda_1$, we can put $v_1 = 0$. So the FVP is easy to solve.

Theorem 4.6 *Let $\mathcal{L} = \mathcal{L}(\alpha_1, \alpha_2, \cdots, \alpha_m)$ be a lattice in K and let $t \in K - \mathcal{L}$ be a target vector with $\mid t \mid_p \leq \lambda_1$. Suppose $\mid t \mid_p = \lambda_{j_0}$ for some $j_0 \geq 1$. Then $s \geq j_0$ and there exists an algorithm to find the values $\mu_i, j_0 < i \leq s$ and the lattice vectors $v_i \in \mathcal{L}$ such that*

$$\mid t - v_i \mid_p = \mu_i \text{ for } j_0 < i \leq s.$$

The algorithm terminates within finitely many steps.

Proof For $v \in \mathcal{L}$, write

$$v = \sum_{i=1}^{m} b_i \alpha_i + p^{j_0} \beta$$

with $b_i \in \mathbb{Z}, 0 \leq b_i \leq p^{j_0} - 1$ for $1 \leq i \leq m$ and $\beta \in \mathcal{L}$. By Lemma 3.3, we have $\mid p^{j_0} \beta \mid_p \leq \lambda_{j_0+1}$. Set $\alpha = \sum_{i=1}^{m} b_i \alpha_i$. If $\mid \alpha \mid_p > \lambda_{j_0}$, then we have $\mid t - v \mid_p = \mid t - \alpha - p^{j_0} \beta \mid_p = \mid \alpha \mid_p$. If $\mid \alpha \mid_p < \lambda_{j_0}$, then we have $\mid t - v \mid_p = \mid t - \alpha - p^{j_0} \beta \mid_p = \mid t \mid_p = \lambda_{j_0}$. If $\mid \alpha \mid_p = \lambda_{j_0}$, then we have $\mid t - v \mid_p = \mid t - \alpha - p^{j_0} \beta \mid_p \leq \lambda_{j_0}$.

Denote B_1 the set of such α with $\mid \alpha \mid_p = \lambda_{j_0}$. B_1 is a non-empty finite set. Set

$$\eta_1 = \min\{\mid t - \alpha \mid_p \mid \alpha \in B_1\}.$$

Then we have $\eta_1 \leq \lambda_{j_0}$. If $\eta_1 > p^{-j_0} \lambda_1$, since $\mid p^{j_0} \beta \mid_p \leq p^{-j_0} \lambda_1$, we have $\mu_{\min} = \eta_1$. And

$$\{\mu_1, \mu_2, \cdots, \mu_s\} = \{\lambda_1, \lambda_2, \cdots, \lambda_{j_0}\} \bigcup \{\mid t - \alpha \mid_p \mid \alpha \in B_1\}.$$

We are done. If $\eta_1 \leq p^{-j_0} \lambda_1$, assume $\eta_1 > p^{-j_1} \lambda_1$ with some integer $j_1 > j_0$. For $v \in \mathcal{L}$, write

$$v = \sum_{i=1}^{m} b_i \alpha_i + p^{j_1} \beta$$

with $b_i \in \mathbb{Z}, 0 \leq b_i \leq p^{j_1} - 1$ for $1 \leq i \leq m$ and $\beta \in \mathcal{L}$. Repeat the above process. Set $\alpha = \sum_{i=1}^{m} b_i \alpha_i$. We need only to consider the case $\mid \alpha \mid_p = \lambda_{j_0}$. Denote B_2 the set of such α with $\mid \alpha \mid_p = \lambda_{j_0}$. B_2 is a non-empty finite set. Set

$$\eta_2 = \min\{\mid t - \alpha \mid_p \mid \alpha \in B_2\}.$$

Since B_1 is a subset of B_2, we have $\eta_2 \leq \eta_1$. If $\eta_2 > p^{-j_1} \lambda_1$, since $\mid p^{j_1} \beta \mid_p \leq p^{-j_1} \lambda_1$, we have $\mu_{\min} = \eta_2$. And

$$\{\mu_1, \mu_2, \cdots, \mu_s\} = \{\lambda_1, \lambda_2, \cdots, \lambda_{j_0}\} \bigcup \{\mid t - \alpha \mid_p \mid \alpha \in B_2\}.$$

We are done. If $\eta_2 \leq p^{-j_1}\lambda_1$, assume $\eta_2 > p^{-j_2}\lambda_1$ with some integer $j_2 > j_1$. And so on. Since $\mu_{\min} > 0$, there is some integer $k \geq 1$ such that $\mu_{\min} > p^{-j_{k-1}}\lambda_1$. Hence $\eta_k \geq \mu_{\min} > p^{-j_{k-1}}\lambda_1$. So $\eta_k = \mu_{\min}$. And

$$\{\mu_1, \mu_2, \cdots, \mu_s\} = \{\lambda_1, \lambda_2, \cdots, \lambda_{j_0}\} \bigcup \{\mid t - \alpha \mid_p \mid \alpha \in B_k\},$$

where

$$B_k = \left\{ \alpha = \sum_{i=1}^{m} b_i \alpha_i \mid b_i \in \mathbb{Z}, 0 \leq b_i \leq p^{j_{k-1}} - 1 \text{ for } 1 \leq i \leq m, \mid \alpha \mid_p = \lambda_{j_0} \right\}.$$

We are done. ∎

Example 4.2 We provide two toy examples to explain that both cases $s = j_0$ and $s > j_0$ will happen. In these two examples, let $\mathcal{L} = \mathbb{Z}_p$, i.e., $m = 1$ and $\alpha_1 = 1$. We have $\lambda_1 = 1$. 1) Let $K = \mathbb{Q}_2(\zeta)$, where ζ is a primitive 3-th root of unity. $K/\mathbb{Q}_2$ is unramified, see [8]. Here $n = 2$ and $p = 2$. Suppose $t = \zeta$. Since $\mid t \mid_2 = 1$, we have $j_0 = 1$. Hence, $B_1 = \{1\}$. Since $\mid t - 1 \mid_2 = 1$, we have $\eta_1 = 1$. So $s = 1, \mu_1 = 1$. 2) Let $K = \mathbb{Q}_3(\zeta)$, where ζ is a primitive 3-th root of unity. Here $n = 2$ and $p = 3$. Suppose $t = \zeta$. Since $\mid t \mid_3 = 1$, we have $j_0 = 1$. Hence, $B_1 = \{1, 2\}$. Since $\mid t - 1 \mid_3 = 3^{-\frac{1}{2}}$ and $\mid t - 2 \mid_3 = 1$, we have $\eta_1 = 3^{-\frac{1}{2}}$. Since $\eta_1 > p^{-j_0}\lambda_1$, we have $s = 2, \mu_1 = 1, \mu_2 = 3^{-\frac{1}{2}}$.

5 Discriminants and λ_2

Let K be an extension of $\mathbb{Q}_p$ of degree n. Let $\mathcal{L} = \mathcal{L}(\alpha_1, \alpha_2, \cdots, \alpha_n)$ be a lattice in K of full rank. Let $\sigma_i : K \hookrightarrow \overline{\mathbb{Q}}_p (1 \leq i \leq n)$ be the n distinct $\mathbb{Q}_p$-embeddings of K. Recall the discriminant of $\alpha_1, \alpha_2, \cdots, \alpha_n$ is defined as

$$D(\alpha_1, \alpha_2, \cdots, \alpha_n) = (\det(\sigma_i(\alpha_j))_{i,j})^2 \in \mathbb{Q}_p^{\times}.$$

For another basis $\beta_1, \beta_2, \cdots, \beta_n$ of $\mathcal{L}$, we have $D(\beta_1, \beta_2, \cdots, \beta_n) = uD(\alpha_1, \alpha_2, \cdots, \alpha_n)$ with $u \in (\mathbb{Z}_p^{\times})^2$. So $\mid D(\alpha_1, \alpha_2, \cdots, \alpha_n) \mid_p$ is an invariant of the lattice $\mathcal{L}$. Define

$$D(\mathcal{L}) = \mid D(\alpha_1, \alpha_2, \cdots, \alpha_n) \mid_p .$$

Theorem 5.1 *Let $\mathcal{L} = \mathcal{L}(\alpha_1, \alpha_2, \cdots, \alpha_n)$ be a lattice in K of full rank. Let m be the number of vectors amongst $\alpha_1, \alpha_2, \cdots, \alpha_n$ whose length is λ_1. Then we have*

$$D(\mathcal{L}) \leq \lambda_1^{2m} \lambda_2^{2(n-m)}.$$

Proof It is obvious from the definition of the discriminant $D(\alpha_1, \alpha_2, \cdots, \alpha_n)$. ∎

6 Remarks

All the above results can be easily generalized to the general setting of local fields. A field k is a local field, we mean that k is complete with respect to a discrete valuation and has a finite

residue class field. Let k be a local field, and let K/k be a finite extension. Then K is also a local field. We can define lattices in K. And all the previous results still hold in this general setting.

Using operations in the p-adic number field $\mathbb{Q}_p$, based on the NP-hardness of the p-adic Simultaneous Approximation Problem, a cryptosystem has been constructed in [12]. But the system is not a public-key cryptosystem, because the encryption uses the information of the private key. Constructing a public-key cryptosystem or other cryptographic schemes based on LVP and CVP defined in this paper is a natural research direction.

The results in this paper are only of theoretic interest in nature, we do not implement the mentioned algorithms.

References

[1] Fröhlich A and Taylor M J, *Algebraic Number Theory*, Cambridge University Press, Cambridge, 1991.

[2] Siegel C L, *Lectures on the Geometry of Numbers*, Springer, New York, 1989.

[3] Micciancio D and Goldwasser S, *Complexity of Lattice Problems, A Cryptographic Perspective*, Kluwer, Boston, 2002.

[4] https://csrc.nist.gov/Projects/Post-Quantum-Cryptography.

[5] Eisenträger K, Hallgren S, Lauter K, et al., *Supersingular Isogeny Graphs and Endomorphism Rings: Reductions and Solutions*, Eds. by Nielsen J B and Rijmen V, EUROCRYPT 2018, LNCS 10822, 2018, 329–368.

[6] Kohel D, Endomorphism rings of elliptic curves over finite fields, Ph.D. thesis, University of California, Berkeley, 1996.

[7] Koblitz N, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Second edition, Springer, New York, 1984.

[8] Cassels J W S, *Local Fields*, Cambridge University Press, Cambridge, 1986.

[9] Serre J P, *Local Fields*, Springer, New York, 1979.

[10] Narkiewicz W, *Elementary and Analytic Theory of Algebraic Numbers*, Third Edition, Springer, New York, 2004.

[11] Weil A, *Basic Number Theory*, Third Edition, Springer, New York, 1974.

[12] Inoue H and Naito K, The shortest vector problems in p-adic approximation lattices and their applications to cryptography, Proceedings of Kyoto University Institute of Mathematics and Physical Sciences, 2015, **1963**: 16–23.