A Local-Global Approach to Solving Ideal Lattice Problems

Tian Yuan[1], Sun Rongxin, Zhu Xueyong, and Cai Wuyang

Network Department, Software School, Dalian University of Technology, P.R.China,
tianyuan_ca@sina.com

Abstract. We construct an innovative SVP(CVP) solver for ideal lattices in case of any relative extension of number fields L/K of degree n where L is real(contained in R). The solver, by exploiting the relationships between the so-called local and global number fields, reduces solving SVP(CVP) of the input ideal A in field L to solving a set of (at most n) SVP(CVP) of the ideals A_i in field L_i with relative degree $1 \leq n_i < n$ and $\sum_i n_i = n$. The solver's space-complexity is polynomial and its time-complexity's explicit dependence on the dimension (relative extension degree n) is also polynomial. More precisely, our solver's time-complexity is $poly(n, |S|, N_{PG}, N_{PT}, N_d, N_l)$ where $|S|$ is bit-size of the input data and N_{PG}, N_{PT}, N_d, N_l are the number of calls to some oracles for relatively simpler problems (some of which are decisional). This feature implies that if such oracles can be implemented by efficient algorithms (with time-complexity polynomial in n), which is indeed possible in some situations, our solver will perform in this case with time-complexity polynomial in n. Even if there is no efficient implementations for these oracles, this solver's time-complexity may still be significantly lower than those for general lattices, because these oracles may be implemented by algorithms with sub-exponential time-complexity

Keywords:Shortest Vector Problem(SVP); Closest Vector Problem(CVP); ideal lattices; field valuations; non-Archimedean valuations; local field; global field.

1 Introduction

Lattice problems take important roles in combinatorial optimization, public-key cryptography and many other fields in computer science[1–5]. In the shortest lattice vector problem (SVP), a non-zero lattice vector $\boldsymbol{x}$ in $\mathbf{BZ}^n$ is to be found to minimize $|\boldsymbol{x}|$ on input the lattice basis matrix $\mathbf{B}$ with respect to some specific norm $||$ in R^n. In the closest lattice vector problem (CVP), a lattice vector $\boldsymbol{x}$ is to be found to minimize $|\boldsymbol{u} - \boldsymbol{x}|$ on input the basis matrix $\mathbf{B}$ and a target vector $\boldsymbol{u}$ in R^n. In recent years, lots of innovative cryptographic schemes and protocols have been devised with proofs of security under the assumption that there is not (probabilistic and sometimes quantum) polynomial-time algorithm to solve arbitrary instances of variants of SVP and CVP.

From a computational hardness perspective, SVP, CVP and other related variants are NP-hard under deterministic (e. g.,CVP) or randomized (e. g.,SVP) reductions[4]. Even some approximation variants of these problems are proven to be NP-hard if the approximation factor is within some specific range. Despite of these facts, finding new algorithms to solve lattice problems exactly are still interesting and meaningful both because many applications (e. g., in mathematics and communication theory) involve lattices in relatively small dimensions, and

because approximation algorithms for high dimensional lattices for which the exact solution is infeasible typically involve the exact solution of low dimensional sub-problems.

Recently a sub-category of lattices, the ideal lattice, is discovered to have indispensible values in innovative cryptography applications, e. g., the wonderful fully homomorphic encryption scheme for secure cloud computing[2], stimulating lots of works in cryptography theory and practices. On the one hand, such schemes are based-on some computational hardness hypothesis on some problems in ideal lattices, e. g., SVP or CVP's hardness, on the other hand, few deep knowledge is known on these points. Since the ideal lattice has plenty of rich intrinsic algebraic properties the general lattice doesn't have, it's reasonable to ask whether its related problems, e. g., SVP and CVP, are really as hard as those of general lattices, or "how easy" are they in comparison with their counterparts in general lattices? No matter what the answer (positive or negative) to this question would be, it will have fundamental significance to ideal lattice theory and applications.

In this paper we work on this question in case of SVP and CVP problems in an algorithmic approach.

Roadmap In this paper we construct the generic algorithms for exactly solving SVP and CVP of ideal lattices by exploiting the algebraic properties uniquely owned by ideal lattices. Sect.2 briefly summarizes the current SVP and CVP solvers for general lattices and an overview on the innovations in our work. Sect.3 provide necessary foundations for our constructions. For logic clearness, we provide a high level algorithm description in Sect.4 at first and then present all low level technical details in Sect.5. Sect.6 concludes and points out some future works.

2 Related Works

To find the exact solution to lattice problems, so far three main families of SVP and CVP solvers exist which are listed in Table 1. With our knowledge, there're no generic algorithms for ideal lattice problems, except some ones modified from the solvers for non-ideal lattices which doesn't essentially exploit the ideal lattice's algebraic properties.

Among the solvers in Table 1, MV and Kannan algorithms are deterministic while AKS algorithms are randomized. All algorithms work in ℓ^2-norm (AKS algorithm can work in other norms, e. g., ℓ_∞). The core of MV algorithm[6] is to compute the Voronoi cell of the lattice[1], whose knowledge facilitates the tasks to solve SVP and CVP. Kannan algorithm[7] relies on a deterministic procedure to enumerate all lattice vectors below a prescribed norm or within a prescribed distance to the target vector. This procedure uses the Grahm-Schmidt orthogonalization of the input lattice basis to recursively bound the integer coordinates of the candidate solutions.The AKS algorithm[8] is the first single-exponential time (random) algorithm for SVP.Recently this algorithm has been significantly improved and the currently best time complexity is $2^{2.465n+o(n)}$[3]. However, the AKS variant solver for CVP only finds the $(1+\varepsilon)$-approximate solution for arbitrary $\varepsilon > 0$ in time complexity bounded by $(2 + 1/\varepsilon)^{O(n)}$[9, 10].

It's already known that when the lattice dimension n is fixed, there are polynomial time-complicated solvers for lattice problems, e. g.,SVP/CVP. i. e., lattice problem's computational hardness only depends on dimension n(Tab.1).

Some related works show that there are important differences in computational complexity between the lattice problems of general and ideal lattices. For

example, some decisional problems of the ideal lattice family with constant root discriminant is in P while the counterparts of general lattice are NP-hard[11]. However, (with our knowledge) there is not search or optimization SVP/CVP (see the concepts in Sect.3.1) solver exploiting the ideal lattice algebraic features and performing significantly better than the best known solvers for general lattices.

Overview on innovations of our approach: construction and performance

Our algorithms constructed in this paper are to find the exact solutions to SVP and CVP in ideal lattices.In this paper we only deal with the case of real number field, i. e., the number field which the input ideal belongs to is contained in R.

Our solver works on the input $(L/K, A)$ where L/K is a finite-degree extension of number field with degree n, A is an (fractional) ideal in L, K is fixed and (L, A) is arbitrarily given. In other words, our solver can work for any finite-degree relative extension, not only the special case of L/Q (where Q is the rational number field).

In construction aspects, our solver, by exploiting the relationships between the so-called local and global number fields, reduces solving SVP(CVP) of the input ideal A in field L to solving a set of (at most n) SVP(CVP) of the ideals A_i in field L_i with relative degree $1 \leq n_i < n$ and $\sum_i n_i = n$. Roughly speaking, by tensor-producting L with a local field K_P where P is an appropriately selected (not unique) prime ideal in the ground field K, the tensor product (as a n-dimensional vector space on the local field K_P) can be always decomposed into a set of sub-spaces of dimension $n_i < n$ which are orthogonal each other and $\sum_i n_i = n$. Furthermore, this orthogonal decomposition is metric-preserving and by constructing appropriate injective homomorphisms all operations in intermediate local fields can be replaced by those in some intermediate global fields(i. e., ordinary number fields), so that the solution to the original problem can be effectively reconstructed from the solutions to the sub-problems. This procedure can proceed recursively down to a set of (at most n) sub-problems of ideal lattices with dimensions as low as possible. In particular, in case of Galois extension L/K, each recursion can decrease the problem's dimension by at least half.

Table 1: The existed families of SVP and CVP solvers for general lattices

Solvers	***Time complexity upper bound***	***Space complexity upper bound***	***Remarks***
Kannan [3, 7, 12]	$n^{O(n)}$	*poly(n)*	deterministic; the O-constant is improved as small as $1/2e$
MV[3, 6]	$2^{2n+o(n)}$	$2^{O(n)}$	deterministic
AKS [3, 8–10]	SVP: $2^{2.465n+o(n)}$ CVP: $(2+1/\varepsilon)^{O(n)}$	SVP: $2^{1.325n+o(n)}$ CVP: $(1+1/\varepsilon)^{O(n)}$	randomized; solves $(1+\varepsilon)$-CVP only

In performance aspects, our SVP(CVP) solver's space-complexity is polynomial. Its time-complexity's explicit dependence on the dimension (relative extension degree n of the number fields) is also polynomial. More precisely, our

solver's time-complexity is

$$poly(n, |S|, N_{PG}, N_{PT}, N_d, N_l)$$

where $|S|$ is bit-size of the input data and N_{PG}, N_{PT}, N_d, N_l are the number of calls to the oracles(Sect.5.5) for some relatively simpler problems (some of them are decisional, e. g., ideal's primality testing in the extended field L). This feature implies that if such oracles can be implemented by efficient algorithms (with time-complexity polynomial in n), which is really possible in some situations, our solver will perform in this case with time-complexity polynomial in n. Even there is no efficient implementations for these oracles, this solver's time-complexity may still be significantly lower than those for general lattices (e. g., Tab.1), because their implementations may be only sub-exponential in time-complexity.

3 Preliminaries

In this section we present all basic notions and facts fundamental to our work in this paper. For more details we refer readers to [4](for general theory on lattices), [13–16](for algebraic number theory) and [17] (for abstract algebra, e. g., the general notions and facts on (Detekind) rings, ideals, unique factorization domains, fields and Galois theory).

3.1 Lattices, SVP and CVP

The set of rational integers is denoted by Z and rational numbers by Q. A lattice is a finitely generated discrete subset in Euclidean space. More explicitly, in the Euclidean space R^n with a positive non-singular bilinear form $<.,.>$, a n-dimensional *rational lattice*, denoted $\Lambda(\mathbf{B})$ where $\mathbf{B}$ is a matrix of rank n with column vectors $(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$, is the set of vectors $\{x_1\boldsymbol{b}_1 + \ldots + x_n\mathbf{b}_n : x_1, \ldots, x_n \in Z\}$ where the values $< \boldsymbol{b}_i, \boldsymbol{b}_j >$ are all rational numbers. The lattice with basis $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ is denoted $Z\boldsymbol{b}_1 + \ldots + Z\boldsymbol{b}_n$. A lattice is called *integral* if $< \boldsymbol{b}_i, \boldsymbol{b}_j >$ are all integers.

For any vector $\boldsymbol{u} = (u_1, \ldots, u_n)$ in R^n, its norm $< \boldsymbol{u}, \boldsymbol{u} >^{1/2}$ is denoted $|\boldsymbol{u}|$. It's easy to verify that the squared norm of any lattice vector in an integral lattice is always an integer.

Lattice Problems Given a lattice $\Lambda(\mathbf{B}) = Z\boldsymbol{b}_1 + \ldots + Z\boldsymbol{b}_n$, let

$$\lambda_1(\Lambda) \equiv \min\{|\boldsymbol{x}| : \boldsymbol{x} \text{ in } \Lambda \text{ and non-zero}\} \tag{3.1}$$

be the minimal value of the norms of non-zero lattice vectors in $\Lambda(\mathbf{B})$. The optimization shortest vector problem with respect to the norm $||$ is to find $\lambda_1(\Lambda)$. The search shortest vector problem is to find a lattice vector $\boldsymbol{x}$ in Λ such that $|\boldsymbol{x}| = \lambda_1(\Lambda)$. Given a lattice $\Lambda(\mathbf{B})$ and a rational target vector $\boldsymbol{u}$ in Q^n, let

$$dist(\Lambda; \boldsymbol{u}) \equiv min\{|\boldsymbol{x} - \boldsymbol{u}| : \boldsymbol{x} \text{ in } \Lambda\} \tag{3.2}$$

be the minimum distance between $\boldsymbol{u}$ and all lattice vectors in Λ. The *optimization closest vector problem* with respect to the norm $||$ is to find $dist(\Lambda; \boldsymbol{u})$. The *search closest vector problem* is to find a lattice vector $\boldsymbol{x}$ in Λ such that $|\boldsymbol{x} - \boldsymbol{u}| = dist(\Lambda; \boldsymbol{u})$.

There are many other lattice-related problems[18, 19]. For example, the *covering radius of a lattice*, $\mu(\Lambda)$, is defined as the maximal distance between any vector and the lattice. The covering radius problem is to find

$$\mu(\Lambda) \equiv \max\{dist(\Lambda; \boldsymbol{u}) : \boldsymbol{u} \; in \; Q^n\} \tag{3.3}$$

In this paper we focus on the algorithms to solve SVP and CVP. It has been known that these problems are computationally hard[4, 19].We focus on constructing the algorithms for SVP and CVP (both in optimization and search version) for ideal lattices, a sub-category of the general lattices with rich algebraic structures originating from number theory.

3.2 Number Fields and Ideal Lattices

A *number field* $K = Q(\alpha)$ is an extension of the rational number field Q, by adding a root α of a polynomial $f(x) \in Z[x]$. $f(x)$ is called α's *minimal polynomial* if it has the minimal degree among the polynomials in $Z[x]$ with α as a root. Such a polynomial is unique up to a constant factor in Z and is always prime (irreducible) in $Z[x]$. The minimal polynomial $f(x)$'s degree is called the degree of field extension K/Q and denoted by $[K : Q]$.

As a subset in the real(R) or complex(C) number field, the arithmetic operations $a \pm b$, ab, a/b in K can be simply understood as the operations in R or C. Another helpful and equivalent (isomorphic) picture is to regard K as the quotient set of $K[x]/(f(x))$ with its arithmetic operations as polynomial addition, subtraction and multiplication modulo $f(x)$ (dividing by $g(x) \neq 0 \bmod f(x)$ equals multiplying by $G(x)$ where $G(x)g(x) = 1 mod f(x)$). In this setting, the generator α in K corresponds to x in $K[x]/(f(x))$.

As in the general theory on finite-degree field extension, the number field K can be regarded as a vector space on the ground field Q in dimension $n = [K : Q]$. As a result, we can introduce the trace and norm to any element in the number field K, i. e., for any z in K we consider the linear operator $T(z)x = zx$: $K \to K$ derived by z and define $Tr(z)$ and $N(z)$ as the trace and determinant of $T(z)$ respectively. An important fact is that both $Tr(z)$ and $N(z)$ fall in Q, and both of them fall in Z when z is in O_K which is defined in sequel.

Within the number field K, there is an important subset, called K's *integral ring*, defined as

$$O_K \equiv \{z \; in \; K : \; there \; exist \; a_0, \ldots, a_{n-1} \; in \; Z \; such \; that \; a_0 + a_1 z + \ldots + a_{n-1} z^{n-1} + z^n = 0\} \tag{3.4}$$

O_K is a ring with the following properties[14–17]:

(1)K is O_K's fractional field, i. e., for any element u in K there is a and b in O_K such that $u = a/b$.

(2)For an (integral) ideal A in O_K(including O_K itself), there always exist a set of Z-linear independent elements $\omega_1, \ldots, \omega_n$ in A where $n = [K : Q]$, called A's integral basis, such that every element in A can be uniquely represented as a Z-coefficient linear combination on $\omega_1, \ldots, \omega_n$. This fact is denoted as $A = Z\omega_1 + \ldots + Z\omega_n$.

For O_K, such basis is called K's integral basis and the determinant of the matrix $Tr(\omega_i \omega_j)$, denoted d_K, is called the determinant of K, which is one of the most important invariant of K.

(3)For number field K, there are exactly $n = [K : Q]$ field embeddings (injective homomorphisms) mapping K into C which are fixed in Q element-wise, among which $\rho_1, \ldots, \rho_{r_1}$ embed K into R and the other $2r_2$ ones $\tau_1, \ldots, \tau_{2r_2}$

(where each τ_j is complex conjugate to τ_{j+r_2}) embed K into C. Now comes one of the central facts and notions in this paper:

Any ideal A is a discrete and finitely-generated subset in $R^{r_1} \times C^{r_2}$ by mapping z in A to $(\rho_1(z), \ldots, \rho_{r_1}(z)$,
$\tau_1(z), \ldots, \tau_{2r_2}(z))$ in $R^{r_1} \times C^{r_2}$, or equivalently by mapping z to the real vector $(\rho_1(z), \ldots, \rho_{r_1}(z), Re\tau_1(z), \ldots,$
$Re\tau_{r_2}(z), Im\tau_1(z), \ldots, Im\tau_{r_2}(z))$ in R^n. As a result, the ideal A can be embedded into R^n as a lattice of dimension n. When associating A with the positive-definite and non-degenerate bilinear form

$$< x, y > \equiv Tr(x\bar{y}) \; where \; \bar{y} \; denotes \; y's \; complex \; conjugation \tag{3.5}$$

we call A(strictly speaking, its image under the above embedding) an ***ideal lattice***. In consequence, we can setup the same problems as in Sect.3.1, e. g., SVP and CVP for ideal lattices.

It's easy to see that for any ideal A in O_K, the ideal lattice is always integral.

(4)For any ideal A in O_K, the quotient ring O_K/A is always finite and its cardinality is denoted $N(A)$. In fact, let $A = Z\omega_1 + \ldots + Z\omega_n$, then $N(A)^2 d_K = det(Tr(\omega_i\omega_j))$=the squared volume of the fundamental domain in the ideal lattice A.

(5)An ideal $P(\neq O_K)$ is called prime, if xy in P then always at least one of x and y is in P. For number field K, every prime ideal P in O_K is maximal, i. e., it is not contained in any ideal other than O_K.

Prime ideals are construction stones for number field arithmetic. For any prime ideal P, the quotient ring O_K/P is actually always a finite field with cardinality p^f where p is a prime integer and $(p) \equiv pZ = P \cap Z$. As a result, $N(A) = p^f$ and O_K/P is a f-degree extension of F_p.

(6)Every ideal A in O_K can be uniquely decomposed as the multiplication of a finite set of prime ideals, i. e., for any ideal A there exist finite prime ideals $P_1, \ldots, P_N$ and positive rational integers $e_1, \ldots, e_N$ such that (in the sense of ideals multiplication)

$$A = P_1^{e_1} \ldots P_N^{e_N}$$

where both $P_1, \ldots, P_N$ and $e_1, \ldots, e_N$ are uniquely determined by A.

(7)For a subset A in K, if $a \pm b$ is always in A for both a, b in A and za is always in A for any z in O_K, then A is called a *fractional ideal*. For a fractional ideal A, there always exists (not unique) some rational integer m such that mA is in O_K, i. e., mA is an integral ideal.

For two (integral or fractional) ideals A and B, if there exists an integral ideal C such that $A = BC$, we denote $B|A$. Otherwise we denote $B \nmid A$. A useful fact is that $B|A$ iff $A \subset B$.

With the same embeddings specified in (3) and the bilinear form in (3.5) associated with a fractional ideal A, A also becomes a lattice in R^n, so all the lattice problems, e. g., SVP and CVP, are meaningful to fractional ideals.

Note: Hereafter we interchangeably use the terminology "ideal" and "ideal lattice" .

With the viewpoint of extension from Q to K, one of the most subtle phenomena is when and how a prime number p (irreducible in Z) becomes reducible in the extended number field K. Such phenomena is used as a critical tool in our approach and we briefly present the facts about it in next section in a more general viewpoint.

3.3 More General Model: Relative Extension and Prime Ideal Decomposition

The theory sketched in Sect.3.2 can be deepen to notions and principles in a more general model. Let K be a number field with its integral ring O_K(or more generally, a fractional field of a *Dedekind domain* O_K[16, 17]), $L = K(\alpha)$ is an extension of K by adding a root α of a polynomial $f(x) \in O_K[x]$. $f(x)$ is called α's *minimal polynomial* if it has the minimal degree among the polynomials in $O_K[x]$ with α as a root. Such a polynomial is unique up to a constant factor in O_K and is prime (irreducible) in $O_K[x]$. The minimal polynomial $f(x)$'s degree is called the degree of field extension $L/K$and denoted by $[L : K]$.

L/K is called *relative extension* from the ground field K. The theory in Sect.3.2 is only about the case where the ground field is Q. As in the case of K/Q, an equivalent (isomorphic) picture about the arithmetic in L is to regard it as the quotient set of $O_K[x]/(f(x))$ with the operations as polynomial addition, subtraction and multiplication modulo $f(x)$.

Regarding L as a vector space on K with dimension $n = [L : K]$, we can introduce the *relative trace* and norm for any element z in L as what is done in 3.2 and denote these as $Tr_{L/K}(z)$ and $N_{L/K}(z)$ respectively[14–16]. For any relative extension $L/M/K$, an important fact is that:

$$\begin{aligned} Tr_{L/K}(z) &= Tr_{M/K}(Tr_{L/M}(z)) \\ N_{L/K}(z) &= N_{M/K}(N_{L/M}(z)) \end{aligned} \tag{3.6}$$

for any z in L.

Given z's minimal polynomial $g(t) = (-1)^m g_0 + g_1 z + \ldots + g_{m-1}t^{m-1} + t^m$ *in* $K[t]$(hence $m|n$), z's trace and norm can be computed by

$$Tr_{L/K}(z) = -(n/m)g_{m-1},\ N_{L/K}(z) = g_0^{n/m} \tag{3.7}$$

For relative extension L/K, there is an important subset, called O_K's integral closure in L, defined as:

$$O_L \equiv \{z \textit{ in } L : \textit{ there exist } a_0, \ldots, a_{n-1} \textit{ in } O_K \textit{ such that } a_0 + a_1 z + \ldots + a_{n-1} z^{n-1} + z^n = 0\} \tag{3.8}$$

O_L is a ring with the following important properties[11, 14–16]:

(1)L is O_L's fractional field.

(2)For an (integral) ideal A in O_L(including O_L itself), there may not exist any set of O_K-linear independent elements $\omega_1, \ldots, \omega_n$ in A where $n = [K : Q]$ such that every element in A can be uniquely represented as a O_K-coefficient linear combination on $\omega_1, \ldots, \omega_n$, unless when O_K is the so-called principal ideal ring.

(3)For any relative extension L/K of degree n, there are exactly n field (relative) embeddings (injective homomorphisms) mapping L into C which are fixed in K element-wise, among which $\rho_1, \ldots, \rho_{r_1}$ embed L into R and the other $2r_2$ ones $\tau_1, \ldots, \tau_{2r_2}$ (where each τ_j is complex conjugate to τ_{j+r_2}) embed L into C.

With these n K-embeddings $\sigma_1, \ldots, \sigma_n$, the trace and norm of an element can be computed by

$$Tr_{L/K}(z) = \sigma_1(z) + \ldots + \sigma_n(z),\ N_{L/K}(z) = \sigma_1(z) \ldots \sigma_n(z) \tag{3.9}$$

As long as K is a number field, L is also a number field with degree $[L : Q] = [L : K][K : Q]$ and O_L defined in (3.8) is exactly the set of $\{z$ in L: there

exist $a_0, \ldots, a_{m-1}$ in Z such that $a_0 + a_1 z + \ldots + a_{m-1} z^{m-1} + z^m = 0\}$ where $m = [L : Q]$. Therefore any ideal A in O_L can be regarded, by the number field L's embeddings into C, as a lattice of dimension $[L : Q]$ in $R^{[L:Q]}$ with the positive-definite and non-degenerate bilinear form

$$< x, y > \equiv Tr_{L/Q}(x\bar{y}) \; where \; \bar{y} \; denotes \; y's \; complex \; conjugation \tag{3.10}$$

Because L is a number field, as a result, every prime ideal M in O_L is maximal and O_L/M is a (finite) field. The important property of the unique factorization on prime ideals is certainly also true for any ideal in O_L.

(4)Let P be a prime ideal in O_L , generally the ideal PO_L may be no longer prime in O_L . As an ideal in O_L , there is the following law about PO_L's decomposition:

For any prime ideal P in O_K , there exist a finite set of prime ideals $M_1, \ldots, M_r$ in O_L such that $M_1 \cap O_K = \ldots = M_r \cap O_K = P$ and PO_L decomposes into prime ideals multiplication on and only on these $M_1, \ldots, M_r$:

$$PO_L = M_1^{e_1} \ldots M_r^{e_r} \tag{3.11}$$

Furthermore, $e_1 f_1 + \ldots + e_r f_r = [L : K]$ where $f_i = [O_L/M_i : O_K/P]$=the degree of the extension from the finite field O_K/P to O_L/M_i. Integers $e_1, \ldots, e_r$ are called *ramification indices* for P on $M_1, \ldots, M_r$ (or $M_1, \ldots, M_r$ on P).

Remarks on Galois Extension: When L/K is a Galois extension, the decomposition law (3.11) can be further refined. In this case we always have $e_1 = \ldots = e_r \equiv e$ and $f_1 = \ldots = f_r \equiv f$. Furthermore, Galois group $G_{L/K}$ is transitive on $M_1, \ldots, M_r$, i. e., for any M_i, M_j there exists g in $G_{L/K}$ such that $M_i = g(M_j)$.

3.4 Valuations, p-adic Completions and Local-Global Relations

Section 3.2-3.3 presented number theory on the so-called *global field*. Now we turn to number theory on the so-called *local field*.

General Notions and Facts Let K be a field, R^+ be the set of all non-negative real numbers, a (multiplicative) valuation on K is a mapping $|.|: K \to R^+$ with the following properties:

$$|xy| = |x||y|; |x| = 0 \; iff \; x = 0; \; |x + y| \leq |x| + |y| \; for \; any \; x \; and \; y \; in \; K$$

When $|n| \leq 1$ for all $n = 0, \pm 1, \pm 2, \pm 3, \ldots$, $|.|$ is called *non-Archimedean* valuation, otherwise called *Archimedean*. For non-Archimedean valuation, the third property in the above is equivalent to the inequality

$$\begin{gathered} |x + y| \leq \max(|x|, |y|) \; for \; any \; x \; and \; y \; in \; K \\ Or \; equivalently \; |x + y| = \max(|x|, |y|) \; for \; any \; x \; and \; y \; in \; K \; and \; |x| \neq |y| \end{gathered} \tag{3.12}$$

An equivalent non-Archimedean valuation model is the index valuation, i. e., a mapping $w : |.|: K \to R$ satisfying $w(xy) = w(x) + w(y); w(x) = +\infty \; iff \; x = 0; w(x + y) \geq \min(w(x), w(y))$ for any x and y in K. Obviously, for any $a > 1$ $w(x) = -\log_a |x|$ gives the correspondance between these two models.

Note: Hereafter we freely interchange the use of these two valuation models at convenience.

Two (multiplicative) valuations $|.|_1$ and $|.|_2$ on filed K is called *equivalent* if there exists a positive real number $a > 0$ such that $|x|_1 = |x|_2^a$ for all x in K. For two non-Archimedean valuations $|.|_1$ and $|.|_2$, this definition equals the statement that $|x|_1 \leq 1$ iff $|x|_2 \leq 1$ for any x in K.

A valuation $|.|$ is called *discrete* if the image of $|.|$ is discrete in R.

Given a non-Archimedean valuation $|.|$(or its equivalent index valuation w) on field K, the subset

$$J_K \equiv \{x\ in\ K : |x| \leq 1\} = \{x\ in\ K : w(x) \geq 0\} \tag{3.13a}$$

is a ring with the unique maximal ideal[13, 16]:

$$M_K \equiv \{x\ in\ K : |x| < 1\} = \{x\ in\ K : w(x) > 0\} \tag{3.13b}$$

The field J_K/M_K is called the valuation's *residue class field*.

For number field K/Q with degree $n = [K : Q]$ we have the following important general facts about valuations on it[13]:

(1)Each (real or complex) Q-embedding σ_j: $K \to C$ (r.f. Sect.3.2(3)) derives an Archimedean (multiplicative) valuation on K by $|x|_j \equiv |\sigma_j(x)|$ where the latter $|.|$ is the ordinary complex valuation $|z| = ((Rez)^2 + (Imz)^2)^{1/2}$. Furthermore, two derived Archimedean valuations $|.|_j$ and $|.|_i$ are equivalent iff $\sigma_j(.)$ and $\sigma_i(.)$ are complex conjugate each other.

(2)Each prime ideal P in O_K derives a discrete non-Archimedean (index) valuation on K by

$$w_P(x) \equiv e\ where\ P^e|(x)\ and\ P^{e+1} \nmid (x)(r.f.\ notations\ in\ Sect.3.2(7))$$

This is called the P-adic valuation. Furthermore, different prime ideals P_i, P_j derive distinct (inequivalent) P-adic valuations w_{P_i}, w_{P_j}.

(3)The valuations presented in (1) and (2) enumerates all valuations on the number field K. As a result, there are finite (exactly $r_1 + r_2$) number of Archimedean valuations and infinite distinct non-Archimedean valuations, each corresponding to a prime ideal.

Example On rational number field Q, the only Archimedean valuation $|.|$ is the ordinary absolute value and each non-Archimedean valuation is corresponding to a prime number p, i. e., the p-adic valuation. For example, with the standard p-valuation we have, for any integer m:

$$|m|_p = p^{-e}\ if\ p^e|m\ but\ p^{e+1} \nmid m$$

In particular, $|m|_p = 1$ iff m and p are co-prime.

Completeness and Local Field Let K be a field with a (Archimedean or non-Archimedean) valuation $|.|$. Since $|.|$ derives a metric on K by $d(x, y) \equiv |x - y|$, the standard metric-completion procedure derives a $|.|$-completion on K, denoted $K_{||}$, which is also a field with K as a dense subfield in it.

Let K be a number field. The completion by anyone of its Archimedean valuations is R or C, depending on whether K is a subfield in R or not. Let P be a prime ideal in O_K, the P-adic completion of K, denoted K_P and called K's *localization* on P (local field), has the following properties[13, 16]:

(1)K_P is a complete and discrete valued field. Further more, K_P/Q_p is a finite-degree extension where p is a prime number such that $(p) \equiv pZ = P \cap Z$ and Q_p is the p-adic completion of the field of rational numbers Q.

(2)For K_P's valuation ring (r.f., (3.13a)) we have

$$\begin{aligned} J_{K,P} \equiv & \{x \ in \ K_P : |x|_P \leq 1\} \equiv \{x \ in \ K_P : w_P(x) \geq 0\} \\ = & \{x \ in \ K_P : \ there \ exist \ a_0, \ldots, a_{n-1} \ in \ Q_p \ such \ that \ w_p(a_i) \geq 0 \ for \ all \ i \\ & and \ a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} + x^n = 0\} \end{aligned} \tag{3.14a}$$

Furthermore $J_{K,P}$ is a principal ideal domain with the unique maximal ideal:

$$M_{K,P} = \{x \ in \ K_P : \ |x|_P < 1\} = \{x \ in \ K_P : \ w_P(x) > 0\} \tag{3.14b}$$

Hence there exists a element π, called K_P's *prime element*, such that $M_{K,P} = (\pi)$. Actually π can be any element in $M_{K,P}$ with the greatest $|.|_P$-value.

(3)Given an ideal B in $J_{K,P}$, there exists a unique integer $m \geq 0$ such that $B = M_{K,P}^m$. In consequence, all integral ideals in $J_{K,P}$ constitute a chain $\ldots \subset M_{K,P}^4 \subset M_{K,P}^3 \subset M_{K,P}^2 \subset M_{K,P}$.

(4)The residue class field of K_P, i. e., $J_{K,P}/M_{K,P}$, is a finite field with characteristic p (the p specified in (1)) and isomorphic to O_K/P.

(5)There is a homomorphism Ω mapping the ideals in O_K to ideals in $J_{K,P}$, defined as:

$$\Omega(A) = M_{K,P}^e, \ if \ P^e | A \ but \ P^{e+1} \nmid A; \ \Omega(A) = J_{K,P} \text{ if } P \text{ and } A \text{ are co-prime} \tag{3.15}$$

It's easy to verify that $\Omega(AB) = \Omega(A)\Omega(B)$ and Ω can be easily prolonged onto the multiplicative group of fractional ideals on K. Ω "*localizes*" an ideal A in global field K to a (principal) ideal $\Omega(A)$ in K_P and this localization is non-trivial iff P is a prime factor of A.

Local-Global Relations Now back to Sect.3.3(4), let both L and K be number fields and L/K a field extension of degree $n = [L : K]$, P a prime ideal in O_K. There exist a finite set of prime ideals $M_1, \ldots, M_r$ in O_L and integers $e_1, \ldots, e_r \geq 1$ such that :

$$\begin{aligned} M_1 \cap O_K = \ldots = M_r \cap O_K = P \\ P O_L = M_1^{e_1} \ldots M_r^{e_r} \\ e_1 f_1 + \ldots + e_r f_r = n \end{aligned} \tag{3.16}$$

where $f_i = [O_L/M_i : O_K/P]$=the degree of the extension from the finite field O_K/P to O_L/M_i.

Let L_{M_j} be the M_j-adic completion of L with its valuation ring denoted by J_{M_j}, prime element η_j(i. e.,$J_{M_j} = (\eta_j)$), $j = 1, \ldots, r$, K_P be the P-adic completion of K with its valuation ring denoted by $J_{K,P}$ and prime element π, now we can state more important and deep details about this decomposition law[13]:

(1)Each L_{M_j} is an extension of K_P and $[L_{M_j} : K_P] = e_j f_j$, $j = 1, \ldots, r$. In particular, each L_{M_j} is a vector space on local field K_P in dimension $e_j f_j$.

(2)For each j, the residue class field of L_{M_j} is an extension of the residue class field of K_P with degree f_j, i. e., $[J_{M_j}/(\eta_j) : J_{K,P}/(\pi)] = f_j$.

(3)For each j, the ground field prime element is decomposed in the extended local field with ramification index e_j, i. e., $(\pi) = (\eta_j)^{e_j}$ in J_{M_j}.

(4)For each j, there is a prolongation from the P-adic valuation on K_P to L_{M_j} specified by

$$|y|_{M_j} = |N_{L_{M_j}/K_P}(y)|_P^{1/e_j f_j} \ for\ any\ y\ in\ L_{M_j}. \tag{3.17}$$

where $|.|_P$ denotes the P-adic multiplicative valuation on K_P. It's easy to see that $|y|_{M_j} = |y|_P$ when y is in K_P. Furthermore, $|y|_{M_j}$ in (3.17) is the only prolongation of $|.|_P$ onto L_{M_j}.

(5)For each j, L_{M_j}'s valuation ring J_{M_j} is exactly the integral closure of K_P's valuation ring $J_{K,P}$, i. e.,

$$\begin{aligned} J_{M_j} &\equiv \{y\ in\ L_{M_j} : |y|_{M_j} \le 1\} \equiv \{y\ in\ L_{M_j} : w_{M_j}(y) \ge 0\} \\ &= \{y\ in L_{M_j} :\ there\ exist\ a_0, \ldots, a_{m-1}\ such\ that\ w_P(a_i) \ge 0 (i.e.,\ in\ J_{K,P}) \\ &\quad for\ all\ i\ and\ a_0 + a_1 x + \ + a_{m-1} y^{m-1} + y^m = 0\} \end{aligned} \tag{3.18}$$

(6)Let $L = K\omega_1 + \ldots + K\omega_n$ and w.l.o.g., all ω_i's are in O_K. Denote the vector space $K_P\omega_1 + \ldots + K_P\omega_n$ on field K_P by $K_P \otimes_K L$ (tensor product on K) and denote the direct summation between vector spaces by $\oplus$, there is a K_P-linear isomorphism ψ between $K_P \otimes L$ and $L_{M_1} \oplus \ldots \oplus L_{M_r}$ where each L_{M_i} is a (distinct) vector space on K_P in dimension $e_j f_j$:

$$\psi : K_P \otimes_K L \cong L_{M_1} \oplus \ldots \oplus L_{M_r} \tag{3.19}$$

Furthermore, denote the element corresponding in (3.19) as $y \cong (y_1, \ldots, y_r)$ then for any y in L we have

$$Tr_{L/K}(y) = Tr_{L_{M_1}/K_P}(y_1) + \ldots + Tr_{L_{M_r}/K_P}(y_r) \tag{3.20a}$$

$$N_{L/K}(y) = N_{L_{M_1}/K_P}(y_1) \ldots N_{L_{M_r}/K_P}(y_r) \tag{3.20b}$$

Let $y^{(1)} \cong (y_1^{(1)}, \ldots, y_r^{(1)})$ and $y^{(2)} \cong (y_1^{(2)}, \ldots, y_r^{(2)})$, at element level the isomorphism has:

$$y^{(1)} \pm y^{(2)} \cong (y_1^{(1)} \pm y_1^{(2)}, \ldots, y_r^{(1)} \pm y_r^{(2)}) \tag{3.21a}$$

$$y^{(1)} y^{(2)} \cong (y_1^{(1)} y_1^{(2)}, \ldots, y_r^{(1)} y_r^{(2)}) \tag{3.21b}$$

Combined with (3.20a) and (3.21a) we have

$$Tr_{L/K}(xy) = Tr_{L_{M_1}/K_P}(x_1 y_1) + \ldots + Tr_{L_{M_r}/K_P}(x_r y_r) \tag{3.22}$$

for L's any element $x \cong (x_1, \ldots, x_r)$ and $y \cong (y_1, \ldots, y_r)$. In other words, (3.19) presents an orthogonal decomposition of the K_P-vector space $K_P \otimes_K L$.

(7)Let A be any (integral or fractional) ideal in L, then A is a finitely generated module on the Dedekind domain. There exist L's K-basis $\omega_1, \ldots, \omega_n$ and a set of K's ideals $I_1, \ldots, I_n$ such that[17, 20]

$$A = I_1\omega_1 + \ldots + I_n\omega_n \tag{3.23}$$

Such $\omega_1, \ldots, \omega_n$ are called A's pseudo-basis and in general they are not in A. Different pseudo-basis share the same cardinality n and it is known how to transform from one pseudo-basis to another[20].

Let A has a pseudo-basis representation in (3.23), define $J_{K,P} \otimes_K A \equiv I_P^{(1)}\omega_1 + \ldots + I_P^{(n)}\omega_n$ where $I_P^{(i)} = I_i$'s image under the localization mapping Ω in (3.15) in K. Let Ω_j be the localization mapping in (3.15) in L_{M_j}, i. e., mapping the ideals in L to ideals in L_{M_j}, then we have the following fact.

Theorem 3.1. *[21] If* A*'s pseudo-basis* $\omega_1, \ldots, \omega_n$ *are in* O_L*, then the* K_P*-linear isomorphism* ψ *in* (3.19) *deduces:*

$$\psi : J_{K,P} \otimes_K A \cong \Omega_1(A) \oplus \ldots \oplus \Omega_r(A) \tag{3.24}$$

□

4 Local-Global Algorithm to Solve SVP and CVP in Ideal Lattices: High Level Descriptions

In this section we construct our algorithms to solve SVP and CVP in ideal lattices. Only the search version is considered because the optimization version can be solved in exactly the same way. Furthermore, we only focus on SVP because the same approach can be easily applied to CVP.

4.1 Problem

The search shortest vector problem in ideal lattice is presented in the following. Instead of only dealing with the case K/Q, our algorithm works for any finite-degree relative extension L/K where K is fixed and L is arbitrary, both are number fields.

Problem SVP(A,L/K)

Parameter: A number field K.
Input: K's extended field $L = K(\alpha)$ with the generator α's minimal polynomial $f(t) = t^n + a_1 t^{n-1} + \ldots + a_{n-1}t + a_0$ in $O_K[t]$, and an ideal A in L.
Note: In this paper we only deal with the case of real number field, i. e., L is contained in R.

For the ideal A on input, we always assume a given pseudo-basis representation, i. e., a set of L's K-basis $\omega_1, \ldots, \omega_n$ in O_L and a set of K's ideals $I_1, \ldots, I_n$ such that $A = I_1\omega_1 + \ldots + I_n\omega_n$.
Output: An element y^* in A such that

$$Tr_{L/K}(y^{*2}) = \min\{Tr_{L/K}(y^2) : \text{ all non-zero } y\text{'s in A}\}$$

4.2 High Level Algorithm

Before going to the technically involved solver construction, we briefly present the motivation. The idea comes from a simple fact that, although lattice problems (e. g., SVP, CVP, CRP, etc) are computationally hard in general cases, a subset of them, in particular the problems of the orthogonal lattice family, can be always solved with polynomial-complexity algorithms. Of course for a general lattice in R^n neither it is always orthogonal nor it can be even decomposed to a set of sub-lattices orthogonal each other, however, for ideal lattices originating

from number field, (3.19)-(3.24) shows that there exists some "orthogonal decomposition" structure exploitable to develop a solver more efficient than those of general lattice problems. Doing such exploitations as far as possible is exactly what will proceed in this paper.

Now we present the whole algorithm's logic at a high level, then working out all technical details in sequel. In the following, all notations are inherited from Sect.3 and "s.t." means "such that". By "global field" we mean any number field and "local field" means the completion of a number field under some of its prime ideal induced valuation.

Algorithm for SVP(A,L/K): High-Level

(1)Given L and A on input, find a prime ideal P in O_K such that:

$$PO_L \textit{ is not prime in } O_L; \tag{4.1a}$$

$$P \textit{ is unramified in } O_L, \textit{ i.e.}, \tag{4.1b}$$
$$\text{all its ramification indices } e_1 = \ldots = e_r = 1;$$

$$P \nmid \sharp(O_L/O_K[\alpha]). \tag{4.1c}$$

(2)Given L and P obtained from last step, find the local fields $L_{M_1}, \ldots, L_{M_r}$ associated with P's all decomposition prime ideals $M_1, \ldots, M_r$ in O_L, integers $f_1, \ldots, f_r \geq 1$ s.t. :

$$PO_L = M_1 \ldots M_r$$

$f_i = [O_L/M_i : O_K/P] = [L_{M_i}$'s residue class field : K_P's residue class field$]$

Secondly, find K_P-linear isomorphism ψ and its component mappings $\psi_1, \ldots, \psi_r$ in (3.19)-(3.21) where each $\psi_i : L \to L_{M_i}$, i. e., $y \cong (y_1, \ldots, y_r)$ means $\psi(y) = (\psi_1(y), \ldots, \psi_r(y))$.

(3)Given L, P and $L_{M_1}, \ldots, L_{M_r}$, integers $f_1, \ldots, f_r \geq 1$ obtained from last step, find K's extended fields $L_1, \ldots, L_r$ and field embeddings $\varphi_1, \ldots, \varphi_r$ with $\varphi_i : \psi_i(L) \to L_i$, s.t.:

$$\text{Each } L_i \text{ is a global field with extension degree } [L_i : K] = f_i; \tag{4.2a}$$

$$\text{For each } i \text{ and } y \text{ in } L: \ Tr_{L_i/K}(\varphi_i\psi_i(y)) = Tr_{L_{M_i}/K_P}(\psi_i(y)); \tag{4.2b}$$

(4)Given all the results obtained, for each i set $\lambda_i \equiv \varphi_i\psi_i : L \to L_i$ and $A_i \equiv \lambda_i(A)$ which is an ideal in L_i. Do:

For each $i = 1, \ldots, r$ find a non-zero x_i^* in A_i s.t.

$$Tr_{L_i/K}(x_i^{*2}) = \min\{Tr_{L_i/K}(x^2) : \text{all non-zero } x\text{' s in } A_i\} \tag{4.3}$$

ie, solve the SVP for ideal lattice A_i in field L_i in a strictly lower dimension $f_i (< n)$;

Find a x_m^* among $x_1^*, \ldots, x_r^*$ s.t.

$$Tr_{L_m/K}(x_m^{*2}) = \min\{Tr_{L_i/K}(x_i^{*2}) : i = 1, \ldots, r\};$$

Find y^* in A such that

$$\lambda_m(y^*) = x_m^* \textit{ and } \lambda_i(y^*) = 0 \textit{ for all } i \neq m; \tag{4.4}$$

Output(y*).

Such obtained y^* is indeed the solution because

$$\begin{aligned}
&\min\{Tr_{L/K}(y^2) : \text{ all non-zero } y\text{'s in } A\} \\
=&\min\{Tr_{L_{M_1}/K_P}(y_1^2) + \ldots + Tr_{L_{M_r}/K_P}(y_r^2) : \text{any } y_i \text{ in } \psi_i(A) \\
&\text{and } y_i = 0 \text{ doesn't hold simultaneously}\} \; by(3.20), (3.21) and (3.24) \\
=&\min\{Tr_{L_1/K}(x_1^2) + \ldots + Tr_{L_r/K}(x_r^2) : \text{any } x_i \text{ in } A_i \\
&\text{and } x_i = 0 \text{ doesn't hold simultaneously}\} \; by(4.2) \\
=&\min_{1\le i\le r} \min\{Tr_{L_i/K}(x_i^2) : \text{ any } x_i \text{ in } A_i \text{ and non-zero}\} \\
=&\min_{1\le i\le r} Tr_{L_i/K}(x_i^{*2})
\end{aligned}$$

Note that in step♯2 we don't need P's decomposition prime ideals per se, but just some information about their local fields $L_{M_1}, \ldots, L_{M_r}$ where each $L_{M_i} = K_P[t]/(f_i(t))$ with some irreducible polynomial $f_i(t)$ in $K_P[t]$. In the low-level constructions it can be seen that even $f_i(t)$ is not needed but just the polynomial $h_i(t) = f_i(t) \mod P$ in $K[t]$ instead

In conclusion, this algorithm reduces an ideal lattice SVP instance of dimension n to a set of $r(\le n)$ ideal lattice SVP instances of strictly lower dimensions. It's already known that lattice problem's computational hardness is only dominated by its dimension n (in other words, there are known algorithms in polynomial time and space complexity to solve lattice problems like SVP and CVP for any fixed dimension[3–5, 7–9, 22]), this feature of our algorithm is significantly helpful to raise the solver's efficiency in solving ideal lattice SVP.

For all those derived sub-instances the ground field are all K, the same as that in the original SVP instance, so (4.3) in step♯4 can be recursively solved by this algorithm down to some appropriately lower dimensions, calling some existed solver at these levels or continue the recursion down to 1-dimensional SVP sub-instances.

Remarks:

(1)For CVP of ideal lattices, i. e., on input the extended (real) field $L = K(\alpha)$, ideal A in L and an element z in L, to find y^* in A s.t.

$$Tr_{L/K}((z - y^*)^2) = \min\{Tr_{L/K}((z - y)^2) : \; all \; y's \; in \; A\}$$

Because:

$$\begin{aligned}
&\min\{Tr_{L/K}((z - y)^2) : \text{ all non-zero y's in } A\} \\
=&\min\{Tr_{L_{M_1}/K_P}((z - y_1)^2) + \ldots + Tr_{L_{M_r}/K_P}((z - y_r)^2) : \\
&any \; y_i \; in \; \psi_i(A)\} \; by(3.20), (3.21), (3.24) \\
=&\min\{Tr_{L_1/K}((\lambda_1(z) - x_1)^2) + \ldots + Tr_{L_r/K}((\lambda_r(z) - x_r)^2) : \\
&any \; x_i \; in \; A_i\} \; by(4.2) \\
=&\min_{1\le i\le r} \min\{Tr_{L_i/K}((\lambda_i(z) - x_i)^2) : \; any \; x_i \; in \; A_i\} \\
=&\min_{1\le i\le r} Tr_{L_i/K}((\lambda_i(z) - x_i^*)^2)
\end{aligned}$$

solving the CVP of ideal lattices can be done by a similar algorithm following the logics of that for SVP. For this reason, we will only focus on solving SVP

hereafter.
(2)In the first step, if such a prime ideal P is found that completely splits in the extended field L, i. e., $PO_L = M_1 \dots M_n$, then solving the SVP instance in this case is reduced to solving n 1-dimensional SVP instances of some ideals in K.
(3)In case of Galois extension L/K, the decomposition law (4.1) will have $e_1 = \dots = e_r \equiv e = 1$ and $f_1 = \dots = f_r \equiv f$. Since $ref = n$ and $r \geq 2$, we always have $f = n/r \leq n/2$, i. e., each reduction can decrease the instance's dimension by at least half and at most $O(\log n)$ recursions are needed.

For example, supposing that each recursion reduces the dimensions (the intermediate fields' extension degrees on K) by half, then after m recursions the original n-dimensional SVP instance will be decomposed to 2^m number of $n/2^m$-dimensional SVP instances. As a result, the time complexity would be at most $2^m 2^{O(n/2^m)}$ by calling some single-exponential time-complexity generic solvers on these $n/2^m$-dimensional SVP instances(e. g., the elegant solver in [6]), substantially more efficient than the time-complexity of $2^{O(n)}$ if the n-dimensional original instance is directly solved.
(4)In the case of Galois extension L/K, the fact that Galois group $G_{L/K}$ is transitive on $M_1, \dots, M_r$ in (4.1), i. e., for any M_i, M_j there exists g in $G_{L/K}$ such that $M_i = g(M_j)$, can significantly simplify lots of details in our algorithm's construction.
(5)In general cases (L/K may not be Galois), to make the sub-instances' dimensions as low as possible at each recursion, it's helpful to find a prime ideal P in O_K not only satisfying those requirements in step♯1 but also the objective that $\max_{j=1,\dots,r} f_j$ is as small as possible, where r, $f_1, \dots, f_r$ are those integers appearing in step♯2.

5 Low Level Details in the Algorithm

Now we turn from the high-level descriptions to low-level technical details, each step discussed in a subsection. We begin with the relatively easy step♯2, ♯3 and ♯4 and finally end with step♯1.

5.1 Solving Subproblems in Step♯2

In this step we solve such problems: Given $L = K(\alpha)$ with α's minimal monic polynomial $f(t) \in K[t]$ and unramified prime ideal P in O_K where $P \nmid \sharp(O_L/O_K[\alpha])$, firstly, find irreducible polynomials $h_1(t), \dots, h_r(t) \in K[t]$ s.t. $h_i(t) = f_i(t) \mod P$ where $L_{M_i} = K_P[t]/(f_i(t))$'s are local fields associated with P's all decomposition prime ideals $M_1, \dots, M_r \subset O_L$. Note that in this situation naturally (i. e.,due to P's unramification) each $degh_i(t) = degf_i(t) = [O_L/M_i : O_K/P]$=[$L_{M_i}$'s residue class field : K_P's residue class field]. Secondly, find K_P-linear isomorphism ψ and its component mappings $\psi_1, \dots, \psi_r$ in (3.19)-(3.21) where each $\psi_i : L \to L_{M_i}$, i. e., $y \cong (y_1, \dots, y_r)$ means $\psi(y) = (\psi_1(y), \dots, \psi_r(y))$.

Solution to the 1st sub-problem:

Decompose $f(t) \mod P$ by calling any appropriate polynomial factorization algorithm modulo the prime ideal(e. g., those in [20, 23, 24]),i. e., to compute distinct monic irreducible polynomials $h_1(t), \dots, h_r(t) \in (O_K/P)[t]$(hence irreducible in $K[t]$) s.t.

$$f(t) = h_1(t), \dots, h_r(t) \mod P \tag{5.1}$$

Proof of the solution's correctness: Suppose in $K_P[t]$ there is the factorization of $f(t)$:

$$f(t) = f_1(t) \dots f_s(t) \tag{5.2}$$

where $f_1(t), \dots, f_s(t) \in K_P[t]$ are distinct monic irreducible polynomials. By the famous Hensel's lemma [13](and O_K/P is the residue class field of K_P) it follows that $r = s$ and $h_i(t) = f_i(t) \mod P$ for $i = 1, \dots, r$ and since $h_i(t)$'s and $f_i(t)$'s are all monic, we have $degf_i(t) = degh_i(t)$.

In addition, under the condition $P \nmid \sharp(O_L/O_K[\alpha])$ we have [23, 24]:

$$PO_L = M_1 \dots M_r$$

where each prime ideal factor $M_i = (P, h_i(\alpha))$ in O_L. In particular, each M_i-adic local field $L_{M_i} = K_P[t]/(f_i(t))$ and $[L_{M_i} : K_P] = degf_i(t) = degh_i(t)$. □

Remark on Complexity of the Polynomial Factorization Algorithm for (5.1):

(5.1) can be solved via lots of algorithms, for example, the algorithm in [24] is a good solver which time-complexity is polynomial in the degree n and the number of basic arithmetic operations in the (finite) field O_K/P. It's also an elegant random algorithm which successful probability is at least 4/9.

Solution to the 2nd sub-problem:

For any $y(t) \in K_P[t]/(f(t)) = K_P \otimes_K L$, set $\psi(y) = (\psi_1(y), \dots, \psi_r(y))$ where

$$\psi_i(y(t)) \equiv y(t) \mod f_i(t) \tag{5.3}$$

Proof of the solution's correctness: By $K_P \otimes_K L = K_P \otimes_K K[t]/(f(t)) = K_P[t]/(f(t))$ and (5.2), it follows from the Chinese Remainder Theorem that there is isomorphism

$$K_P \otimes_K L \cong K_P[t]/(f_1(t)) \oplus \dots \oplus K_P[t]/(f_r(t)) = L_{M_1} \oplus \dots \oplus L_{M_r}$$

where the K_P-linear isomorphism ψ's components $\psi_i(y(t)) \equiv y(t) \mod f_i(t)$, $i = 1, \dots, r$ and obviously $\psi_i(y \pm z) \equiv \psi_i(y) \pm \psi_i(z)$, $\psi_i(yz) \equiv \psi_i(y)\psi_i(z)$ in L_{M_i} for any $y = y(t)$, $z = z(t)$ in L_{M_i} and i. Furthermore, $T(y)z \equiv yz = y_1z_1 \oplus \dots \oplus y_rz_r = T(y_1)z_1 \oplus \dots \oplus T(y_r)z_r$, i. e., there is always the diagonalization $T(y) = T(y_1) \oplus \dots \oplus T(y_r)$ so (3.20) holds (but (3.20b) is not needed). In particular, each ψ_i's restriction on L can be computed by:

$$\psi_i(y(t)) \equiv y(t) \mod h_i(t), \ for\ any\ y(t) \in K[t]/(f(t)) = L \tag{5.4}$$

and $\psi_i(L) = L_i$. □

5.2 Solving Subproblems in Step♯3

Given L, unramified prime ideal P in O_K and local fields associated with PO_L's all prime factors $M_1, \dots, M_r$ in O_L, i.e., $L_{M_1}, \dots, L_{M_r}$ each with an irreducible polynomial $h_i(t)$ in $K[t]$ s.t. $h_i(t) = f_i(t) \mod P$ and $L_{M_i} = K_P[t]/(f_i(t))$, integers $f_1, \dots, f_r \geq 1$, we need to find K's extended fields $L_1, \dots, L_r$ and field embeddings $\varphi_1, \dots, \varphi_r$ satisfying (4.2). We solve this for each $i = 1, \dots, r (r \leq n)$ so the sub-problem is re-specified as:

Given L, unramified prime ideal P in O_K and a local field associated with one of PO_L's prime factor M in O_L, i. e., L_M with an irreducible polynomial $h_M(t)$ in $K[t]$ s.t. $h_M(t) = f_M(t) \mod P$ and $L_M = K_P[t]/(f_M(t))$ of extension degree $f \geq 1$, find K's extended (global) field $L^*$of degree $[L^* : K] = [L_M : K_P]$ and a field embedding $\varphi_M : \psi_M(L) \to L_M$ where ψ_M denotes the ψ's component-mapping on L_M s.t. $Tr_{L^*/K}(\varphi_M\psi_M(y)) = Tr_{L_M/K_P}(\psi_M(y))$ for any y in L^*.

Solution:

$$Set\ L^* \equiv K[t]/(h_M(t))\ and\ \varphi_M = id. \tag{5.5}$$

Proof of the solution's correctness: Obviously L^* is global because $h_M(t) \in K[t]$. Now prove L^* is dense in L_M and $[L^* : K] = [L_M : K_P]$. Since $L_M = K_P[t]/(f_M(t))$ is a unramified (local field) extension with extension degree $f = degf_M(t)$ and $f_M(t)$ is irreducible in $K_P[t]$ with leading coefficient 1, $h_M(t) = f_M(t) \mod P$ so by Hensel lemma $h_M(t)$ is irreducible in $(O_K/P)[t]$ with the same degree f and leading coefficient 1. In consequence[13, Chapter 14; 16, Chapter2], this unramified extension L_M/K_P induces a finite field extension $O_L/M = (O_K/P)[t]/(h_M(t))$ of the same degree f and vice versa, a one-to-one correspondence up to isomorphism.

As a result, we have $K_P[t]/(f_M(t)) = K_P[t]/(h_M(t))$ and in particular $h_M(t)$ is irreducible in $K[t]$ so $[L^* : K] = f = [L_M : K_P]$. By definition $L^* = K[t]/(h_M(t))$ we have that L_M is densely contained in the field $K_P[t]/(h_M(t)) = K_P[t]/(f_M(t)) = L_M$. Furthermore, $K_P \otimes_K L^* = K_P[t]/(h_M(t)) = K_P[t]/(f_M(t)) = L_M$ so $Tr_{L^*/K}(y) = Tr_{L_M/K_P}(y)$ for any y in L^* by (3.19).

Finally, $\psi_M(L) = L^*$ so $\varphi_M = id$. □

Remark: If L is contained in R, so is L^*. In fact, L is real so for L's any prime ideal M, $\sqrt{-1}$ is not in the M-adic completeness of L, i. e., $\sqrt{-1}$ is not in L_M. As a result, $\sqrt{-1}$ is not in L^* which is dense in L_M, i. e., L^* is real.

5.3 Solving subproblems in Step♯4

In step♯4 we need to solve two sub-problems. Firstly, given an ideal A (with its pseudo-basis) in L and a surjective homomorphism $\psi_m : L \to L_m$, compute the ideal $\psi_m(A)$ in L_m. Secondly the sub-problem (4.4), i. e., given $x^*(t)\ in\ L_m = K[t]/(h_m(t))$ find $y^*(t)$ in L s.t.

$$y^*(t) = x^*(t) \mod h_m(t),\ y^*(t) = 0 \mod h_j(t)\ for\ all\ j \neq m \tag{5.6}$$

Solution to the 1st sub-problem

(Ideal's homomorphism image).On input an ideal A with the pseudo-basis representation,i. e., a set of L' s K-basis $\omega_1, \ldots, \omega_n$ in O_L and a set of K's ideals $I_1, \ldots, I_n$ such that $A = I_1\omega_1 + \ldots + I_n\omega_n$, do:

Compute $b_i = \psi_m(\omega_i)$, $i = 1, \ldots, n$.

Find the maximal subset of K-linear independent members, w.l.o.g., denoted $b_1, \ldots, b_{d_m}$ where $d_m = [L_m : K]$, and the integers β, λ_{ij} in O_K s.t.

$$\beta b_i = \sum_{1 \le j \le d_m} \lambda_{ij} b_j \quad i = d_m + 1, \ldots, n$$

(e. g., this step can be accomplished by Gauss elimination algorithm regarding the b_i's as vectors in the d_m-dimensional K-linear space L_m);

Compute the ideal $J_j = \beta I_j + \sum_{1+d_m \le i \le n} \lambda_{ij} I_i$ for each $j = 1, \ldots, d_m$;

Compute and output the ideal

$$\psi_m(A) = \sum_{1 \le j \le d_m} J_j b_j / \beta.$$

Proof of the solution's correctness: Since $A = I_1\omega_1 + \ldots + I_n\omega_n$ and ψ_m is a K-homomorphism, we have $\psi_m(A) = I_1 b_1 + \ldots + I_n b_n$ so

$$\begin{aligned}\beta\psi_m(A) &= \beta I_1 b_1 + \ldots + \beta I_{d_m} b_{d_m} + I_{d_m+1}\beta b_{d_m+1} + \ldots + I_n \beta b_n \\ &= \beta I_1 b_1 + \ldots + \beta I_{d_m} b_{d_m} + I_{d_m+1} \sum_{1 \le j \le d_m} \lambda_{d_m+1,j} b_j + \ldots + I_n \sum_{1 \le j \le d_m} \lambda_{n,j} b_j \\ &= \sum_{1 \le j \le d_m} (\beta I_j + \sum_{1+d_m \le i \le n} \lambda_{ij} I_i) = \sum_{1 \le j \le d_m} J_j b_j.\end{aligned}$$

and note that b_i's are all in O_{L_m} since ω_i's are all in O_L. □

Solution to the 2nd sub-problem:

Find $g^*(t)$ in $K[t]$ s.t.

$$g^*(t) = x^*(t) \mod h_m(t), g^*(t) = 0 \mod h_j(t) \text{ for all } j \ne m$$

by the standard algorithm derived from Chinese Remainder Theorem. Then set $y^*(t) \equiv g^*(t) \mod f(t)$

The solution's correctness can be verified by direct calculations.

5.4 Solving Subproblems in Step♯1

Now we turn to this problem: given L and A on input, find a prime ideal P in O_K such that:

$$PO_L \text{ is not prime in } O_L; \tag{5.7a}$$

$$P \text{ is unramified in } O_L, \text{i. e., all its ramification indices } e_1 = \ldots = e_r = 1; \tag{5.7b}$$

$$P \nmid \sharp(O_L/O_K[\alpha]). \tag{5.7c}$$

Before constructing the solver, we specify the following oracles at first.

Oracle-PG_K where K is a number field: Generates a prime ideal at random in O_K. The input is void and each output is probabilistically independent of any others.

Orcale-$PT_L(M)$ where L is a number field: on input any ideal M in O_L, tests whether M is prime or not.

Oracle-$d_K(L)$: On input any L where L/K is a number field extension of finite degree, outputs the relative discriminant $d_{L/K}$, an integral ideal in O_K which is the greatest common divisor of $det(Tr_{L/K}(a_i a_j))$ of all K-linear independent integers $a_1, \ldots, a_n$ in O_L.

Oracle-$l_K(L, \alpha)$: On input any $L = K(\alpha)$ where L/K is a number field extension with finite degree n, outputs $\sharp(O_L/O_K[\alpha])$, the cardinality of the finite quotient set $O_L/O_K[\alpha]$.

Solution

(I) Compute the relative discriminant $d_{L/K}$= **Oracle-**$d_K(L)$;
Compute l=**Oracle-**$l_K(L, \alpha)$:
(II) Do{
P=**Oracle-**PG_K; /*generate prime ideal P in O_K*/
}while ($P|d_{L/K}$ or $P|l$);
/*equivalently, $d_{L/K}$ is a subset of P or $l \in P$.*/
(III) If **Orcale-**$PT_L(PO_L)$ is true /*i. e., P is prime in O_L */
Then goto II;
output(P);

Proof of the solution's correctness By general algebraic number theory, a prime ideal P in O_K is ramified in the integral closure O_L of the field extension L/K iff it divides the relative discriminant $d_{L/K}$[13, 14, 16]. As a result, the output prime ideal P is unramified in O_L and obviously satisfies all other requirements in (5.7). □

Remarks on implementation of the oracles: In general, how to implement all the above oracles is not completely clear with our best knowledge. However, in the important case that $L = Q(\alpha) \cong Q[t]/(f(t))$ where the polynomial $f(t)$ is monic and irreducible in $Z[t]$, $K = Q$ (*hence* $O_K = Z$), we can have further arguments about their implementations.

(1)**Oracle-**$l_Q(L, \alpha)$ can be completely implemented by **Oracle-**$d_Q(L)$. If fact, in this case there is the formula

$$\sharp(O_L/Z[\alpha]) = |N_{L/Q}(f'(\alpha))/d_{L/Q}|^{1/2} \tag{5.8}$$

where $|.|$ is the ordinary absolute value.

Proof. When $L = Q(\alpha) \cong Q[t]/(f(t))$, (due to the fact that $O_K = Z$ is a principal ideal domain) there exist a set of integral basis $\xi_1, \ldots, \xi_n$ s.t. $O_L = Z\xi_1 + \ldots + Z\xi_n$ and the determinant $d_{L/Q} = det(Tr_{L/Q}(\xi_i \xi_j))$, i. e., $|d_{L/Q}|$ is the squared volume of the lattice O_L's fundamental domain. Note that $Z[\alpha] =$

$Z + Z\alpha + Z\alpha^2 + \ldots + Z\alpha^{n-1}$ ($\alpha \in O_L$) is a sub-lattice in O_L so its squared fundamental domain's volume's squared

$$|det(Tr_{L/Q}(\alpha^{i-1}\alpha^{j-1}))| = \sharp(O_L/Z[\alpha])^2|d_{L/Q}|$$

On the other hand, $|det(Tr_{L/Q}(\alpha^{i-1}\alpha^{j-1}))| = |det(\alpha^{(i)j-1)}|^2$=the square of the Vandermond determinant of α's conjugates $\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(n-1)} = |\prod_{1\leq i<j\leq n}(\alpha^{(i)} - \alpha^{(j)})|^2 = |f'(\alpha^{(1)})\ldots f'(\alpha^{(n)})| = |N_{L/Q}(f'(\alpha))|$, which proves (5.8).

(2) **Oracle-$d_Q(L)$**: In this case there exist the algorithms to compute O_L's integral basis $\xi_1, , \xi_n$ and the determinant $d_{L/Q}$, e. g., the algorithm 6.1.8 in [25]. It's worthwhile to note that the performance-dominating step in this algorithm is to factorize the rational integer[25] which bit-size in our algorithm's context is $poly(n)$, as a result, this oracle's intrinsic complexity maybe only as hard as integer factorization.

For elative extension L/K where $K \neq Q$, it's worthwhile to mention the special case $d_{L/K} = O_K$ (which can never happen if K is Q) and hence $d_{L_j/K} = O_K$ for all the intermediate fields L_j during the algorithm's recursion, e. g., K's Hilbert class field $L = K(\mu^{1/q})$ where q divides K's class number $h(K)$. In this situation the oracle-$d_K(.)$ is trivial and the decision $P|d_{L/K}$ (always false) can be simply omitted from the algorithm. As a result, the algorithm's complexity can be significantly reduced (r.f., Sect.5.5).
(3) **Orcale-$PT_L(M)$**: On input any ideal M in O_L, decide whether M is prime or not. For this oracle's counterpart in rational number field Q, i. e., rational integer's primality testing, there are not only practically efficient but also deterministic polynomial time-complexity algorithms [26, 27]. Although so far it's unknown how to efficiently implement Orcale-$PT_L(.)$ in arbitrary number field L, it's reasonable to expect that it's complexity would be lower than SVP/CVP.

(4) *Oracle-PG_Q*: Generates a prime number at random in Z, a problem with known efficient solvers.

5.5 Computational Complexity

Let $|S|$ denote the input size of the ideal lattice Problem $SVP(A, L/K)$, N_{PG}, N_{PT}, N_d and N_l denote the number of callings to Oracle-PG_K, Orcale-PT_L, Oracle-d_K and Oracle-l_K in the algorithm. From the constructions in Sect.4 and Sect.5, it's easy to see that all the subroutines and operations in the algorithm are only those with time and space complexity polynomial in the input size, except the above four oracles which intrinsic computational complexity may be non-polynomial. Furthermore, the recursion depth of the (high level) algorithm is only $O(n)$ where $n = [L : K]$=the dimension of the input ideal lattice A. In summary, we can have the following conclusions.

Theorem 5.1. *(1)Given any number field K, there exists the algorithm to solve (exactly) SVP on input any extended field L and ideal A in O_L with time complexity*

$$poly(n, |S|, N_{PG}, N_{PT}, N_d, N_l) \tag{5.9}$$

and space complexity poly$(n, |S|)$ where $n = [L : K]$. (2)For CVP of ideal lattices, we have exactly the same conclusion. □

Corollary 5.2 *(1)Given any number field* K*, there exists the algorithm to solve (exactly) SVP on input any extended field* L_μ *and ideal* A_μ *in* O_{L_μ} *from the family* $\{(L_\mu, A_\mu) : d_{L_\mu/K} = O_K\}$ *with time complexity* $poly(n_\mu, |S|, N_{PG}, N_{PT}, N_l)$ *and space complexity* $poly(n_\mu, |S|)$ *where* $n_\mu = [L_\mu : K]$*. (2)For CVP of ideal lattices, we have exactly the same conclusion.* □

Remark: It is known that there exists the infinite family (e. g.the Hilbert class field extension tower) $\{(L_\mu, A_\mu) : d_{L\mu/K} = O_K\}$ which extension degree n_μ is upper-boundless. For such input family, the algorithm constructed in this paper would be efficient (polynomial in time) as long as the Oracle-PG_K, Orcale-PT_L and Oracle-l_K can be implemented efficiently, which possiblity seems positive.

Now back to the case of L/Q, because there exist efficient algorithms to implement Oracle-PG_Q, i. e., to efficiently generate prime integers, we have:

Corollary 5.3 *(1)There exists the algorithm to solve (exactly) SVP on input any number field* L *and ideal* A *in* O_L *with time complexity*

$$poly(n, |S|, N_{PT}, N_d, N_l)$$

and space complexity $poly(n, |S|)$ *where* $n = [L : K]$*. (2)For CVP of ideal lattices, we have exactly the same conclusion.* □

6 Conclusions and Future Works

We construct an innovative SVP(CVP) solver for ideal lattices in case of any relative extension of number fields L/K of degree n where $L = K(\alpha)$ is real. By this construction, solving SVP/CVP of ideal lattices is efficiently reduced to solving SVP/CVP of strictly lower dimensional ideal lattices and the problems of generating prime ideals in the ground field K, testing the ideal's primality in the extended field L, calculating the relative discriminant $d_{L/K}$ and the cardinality of $O_L/O_K[\alpha]$. The solver's space-complexity is polynomial and its time-complexity's explicit dependence on the dimension n is also polynomial.

As a result, the first open problems are to construct the algorithms to implement the above oracles, which also have independent values in theory and applications. The second and more interesting open problem is that, for some of the oracles computationally hard to implement, whether its hardness can be still preserved against the quantum computing model. An answer to this problem will imply whether the ideal lattice problems' hardness is solid for post-quantum cryptography.

Bibliography

[1] Sloane, N.J., Conway, J., et al.: Sphere packings, lattices and groups. 3rd Ed. Springer-Verlag (1998)
[2] Gentry, C.: Fully homomorphic encryption using ideal lattices. Proc. 41st ACM STOC (2009) 169–178
[3] Hanrot, G., Pujol, X., Stehlé, D.: Algorithms for the shortest and closest lattice vector problems. Proc. IWCC (2011)
[4] Micciancio, D., Goldwasser, S.: Complexity of Lattice Problems: a cryptographic perspective. Kluwer Academic Publishers, Boston, Massachusetts (2002)
[5] Nguyen, P.Q., Valle, B.: The LLL algorithm: survey and applications. Springer-Verlag (2009)
[6] Micciancio, D., Voulgaris, P.: A deterministic single exponential time algorithm for most lattice problems based on voronoii cell computations. SIAM J. Comput (2012) Special Issue on STOC'2010.
[7] Kannan, R.: Minkowski's convex body theorem and integer programming. Mathematics of operations research **12**(3) (1987) 415–440
[8] Ajtai, M., Kumar, R., Sivakumar, D.: A sieve algorithm for the shortest lattice vector problem. In: Proceedings of the thirty-third annual ACM symposium on Theory of computing, ACM (2001) 601–610
[9] Ajtai, M., Kumar, R., Sivakumar, D.: Sampling short lattice vectors and the closest lattice vector problem. In: IEEE Conference on Computational Complexity. (2002) 53–57
[10] Nguyen, P.Q., Vidick, T.: Sieve algorithms for the shortest vector problem are practical. Journal of Mathematical Cryptology **2**(2) (2008) 181–207
[11] Peikert, C., Rosen, A.: Lattices that admit logarithmic worst-case to average-case connection factors. In: Proc. STOC. (2007) 478–487
[12] Kannan, R.: Lattice translates of a polytope and the frobenius problem. Combinatorica **12**(2) (1992) 161–177
[13] Hasse, H.: Number theory. 3rd Ed. Springer-Verlag (1969)
[14] Hecke, E.: Lectures on the theory of algebraic numbers. Springer-Verlag (1981)
[15] Ireland, K., Rosen, M.I.: A classical introduction to modern number theory. Springer-Verlag (1990)
[16] Lang, S.: Algebraic number theory, 2nd ed. Springer-Verlag (1994)
[17] Rotman, J.J.: Advanced modern algebra. Prentice-Hall Inc (2002)
[18] Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. Springer-Verlag (2010)
[19] Micciancio, D.: Efficient reductions among lattice problems. Proc. SODA'08 (2008) 84–93
[20] Cohen, H.: Advanced topics in computational number theory. Springer-Verlag (2000)
[21] Li, W.C.W.: Number theory with applications. World Scientific Singapore (1996)
[22] Haviv, I., Regev, O.: Hardness of the covering radius problem on lattices. In: IEEE CCC'06. 145–158
[23] Pohst, M., Zassenhaus, H.: Algorithmic algebraic number theory. Cambridge University Press (1989)
[24] Roblot, X.F.: Polynomial factorization algorithms over number fields. Journal of Symbolic Computation **2002**(11) 1–14

[25] Cohen, H.: A course in computational algebraic number theory. Springer-Verlag (1993)
[26] Schoof, R.: Four primality testing algorithms. In: Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography, Cambridge University Press (2008) 101–126
[27] Agrawal, M., Kayal, N., Saxena, N.: Primes is in P. Annals of mathematics (2004) 781–793