Subfield Algorithms for Ideal- and Module-SVP Based on the Decomposition Group

Christian Porter[1], Andrew Mendelsohn[2], and Cong Ling[3]

[1] Department of EEE, Imperial College London, London, SW7 2AZ, United Kingdom.
c.porter17@imperial.ac.uk
[2] Department of EEE, Imperial College London, London, SW7 2AZ, United Kingdom.
andrew.mendelsohn18@imperial.ac.uk
[3] Department of EEE, Imperial College London, London, SW7 2AZ, United Kingdom.
c.ling@imperial.ac.uk

Abstract. Whilst lattice-based cryptosystems are believed to be resistant to quantum attack, they are often forced to pay for that security with inefficiencies in implementation. This problem is overcome by ring- and module-based schemes such as Ring-LWE or Module-LWE, whose keysize can be reduced by exploiting its algebraic structure, allowing for neater and faster computations. Many rings may be chosen to define such cryptoschemes, but cyclotomic rings, due to their cyclic nature allowing for easy multiplication, are the community standard. However, there is still much uncertainty as to whether this structure may be exploited to an adversary's benefit. In this paper, we show that the decomposition group of a cyclotomic ring of arbitrary conductor may be utilised in order to significantly decrease the dimension of the ideal (or module) lattice required to solve a given instance of SVP. Moreover, we show that there exist a large number of rational primes for which, if the prime ideal factors of an ideal lie over primes of this form, give rise to an "easy" instance of SVP. However, it is important to note that this work does not break Ring-LWE or Module-LWE, since the security reduction is from worst case ideal or module SVP to average case Ring-LWE or Module-LWE respectively, and is one way.

Keywords: Ideal Lattice · Module Lattice · Ring-LWE · Module-LWE · Shortest Vector Problem.

1 Introduction

Cryptosystems based on lattices are one of the leading alternatives to RSA and ECC that are conjectured to be resistant to quantum attacks. Considered to be the genesis of the study of lattice cryptosystems, in 1996, Ajtai constructed a one-way function, and proved the average-case security related to the worst-case complexity of lattice problems [1]. Later, in 2005, Regev proposed the computational problem known as "Learning With Errors" (LWE) and showed that

LWE is as hard to solve as several worst-case lattice problems [2]. Whilst these problems are believed to be difficult to crack even given access to a quantum computer, their main drawback is their impracticality to implement in cryptosystems due to the large key sizes required to define them.

For this reason, lattices with algebraic structure are often favoured to define cryptosystems over conventional lattices. In particular, cryptosystems often employ the use of cyclotomic polynomials as their cyclic nature allows for much less cumbersome computations. Such lattices come in two main varieties: ideal lattices, whose structures are formed entirely by embedding an ideal of a number field into real or complex space, and module lattices, which are free modules defined over an algebraic ring and can be thought of as a compromise between classical and ideal lattices. Perhaps the most well-known cryptosystem based on algebraic structure is the NTRU cryptosystem. Developed in 1996 by Hoffstein, Pipher and Silverman [3], the NTRU cryptosystem uses elements of the convolution ring $\mathbb{Z}[x]/(x^p - 1)$ and offers efficient encryption and decryption of messages, making it one of the most popular lattice-based cryptosystems even to this day. In [13], noting that the ring $\mathbb{Z}[x]/(x^p - 1)$ could be deemed insecure due to the fact that $x^p - 1$ is not irreducible, Stehlé and Steinfeld updated NTRU to incorporate a cyclotomic ring in place of the aforementioned ring. The computational problem involved in breaking NTRU can be thought of as a rank 2 module problem over a cyclotomic ring. More recently, an algebraic variant of LWE called Ring-LWE (RLWE) was developed by Lyubashevsky, Peikert and Regev in 2010 [4]. It has been shown that the security of this scheme relies heavily on the hardness of ideal lattice reduction [5]. Moreover, the work by Ajtai was also generalised to the ring case by Micciancio in 2004 [9]. Using an arbitrary ring in place of a classical lattice, he managed to show that obtaining a solution to the ring-based alternative to the knapsack problem on the average was at least as hard as the worst-case instance of various approximation problems over cyclic lattices, even for rings with relatively small degree over $\mathbb{Z}$. Whilst there are a myriad of other schemes that make use of algebras to define a cryptosystem (see for example [6], [7], [8]), concerns have been raised regarding the security of such schemes. Whilst the algebraic structure might allow for easier computations, the additional structure given by an algebra could be exploited to allow for easier reduction of lattices based on algebras.

As we have already mentioned, cyclotomic polynomials exhibit many properties that are desirable in cryptography. In particular, cryptographers largely favour power-of-two cyclotomic rings, that is, cyclotomic rings with conductor $N = 2^n$ for some integer n. This is largely a consequence of a few properties exhibited by power-of-two cyclotomic rings, for example, $N/2$ is also a power of two and arithmetic in the ring can be performed with ease using the N-dimensional FFT. However, restricting cryptosystems to only using power-of-two cyclotomic rings has its drawbacks. The most obvious of these drawbacks is the increase in dimension of the ideal lattice when moving from one power-of-two cyclotomic ring to the next, which doubles with each successive ring, and the cryptosystem may require a lattice of intermediate security: for example, ideal lattices of the

cyclotomic ring of conductor 1024 have dimension 512, but the next power-of-two cyclotomic ring is of conductor 2048, and so ideal lattices defined in this ring have dimension 1024, which is a significant jump. For this reason amongst others, cryptographers have begun to move away from power-of-two cyclotomic rings to cyclotomic rings of more general conductor. However, this migration from power-of-two cyclotomics is relatively novel, and as such literature regarding the reduction of ideal lattices based on cyclotomic rings of general conductor is still heavily lacking.

1.1 Previous Works

There have been a variety of studies into the shortest vector problem (SVP) in lattices generated by ideals. In 2016, Cramer, Ducas, Peikert and Regev published a paper detailing an attack on ideals generated by principal ideals of prime-power cyclotomic rings [21]. They presented a technique involving the use of the log-unit lattice, and showed that a generator could be recovered that is a solution to approx-SVP with factor $2^{O(\sqrt{N})}$ using only a polynomial-time reduction algorithm such as the LLL algorithm. Simultaneously, largely inspired by Bernstein's work on subfield attacks against ideal lattices [11], Albrecht, Bai and Ducas proposed a different method by which to attack the NTRU cryptosystem with overstretched parameters - that is, the NTRU encryption scheme with much larger modulus [12]. Their method entailed an attack on the NTRU cryptosystem by attacking a sublattice, defined by a public key attained by "norming down" the public key of the original lattice to a subfield, and then "lifting" a solution on the sublattice to a solution for the original cryptosystem which, provided the solution is sufficiently good in the sublattice, may yield a short lattice vector in the full lattice. Indeed, there are many examples of previous works which detail lattice attacks against ideal lattices. For a detailed list regarding previous research into the reduction of ideal lattices, we refer the reader to the "previous works" section of [10].

Recently, Pan, Xu, Wadleigh and Cheng pioneered a remarkable technique to approach the problem of SVP in prime and general ideal lattices, obtained from power-of-two cyclotomics [10]. Their method involved manipulating the decomposition group of prime ideals in order to significantly reduce the dimension of the lattice required to solve SVP for. Their primary contributions were in two parts: the first part of the paper took a number field L that is Galois over $\mathbb{Q}$ and showed that, given a prime ideal of its ring of integers $\mathcal{O}_L$, if Hermite-SVP can be solved for a certain factor in a sublattice generated by a subideal, this yields a solution for Hermite-SVP in the original ideal lattice with a larger factor, where the factor's increase depends only on the square root of the degree of L over $\mathbb{Q}$ divided by the size of the decomposition group. The second part of their paper is dedicated to ideals over the ring of integers of cyclotomic fields of conductor $N = 2^{n+1}$. Under the so-called coefficient embedding, they showed that using a subgroup of the decomposition group of a prime ideal, the shortest vector in the ideal is equivalent to the shortest vector in a subideal constructed in the paper, and so solving SVP over such ideals is easy given an oracle to solve SVP

in lattices of dimension equivalent to the dimension of the ideal lattice generated by the subideal. Moreover, they showed that if such a prime ideal lies above a rational prime p of the form $p \equiv \pm 3 \mod 8$ then the shortest vector is of length p, and is very easy to determine. In the final section, they showed that their method also worked for general ideals by considering the prime decomposition of an ideal.

1.2 Our Results

In this paper, we generalise the results of Pan et. al., both in their work on Hermite-SVP for prime ideal lattices and solving SVP exactly for prime ideals in cyclotomic ideals. The first half of the paper is dedicated to the Hermite-SVP in ideal lattices. Whilst Pan et. al. only covered the case for lattices based on prime ideals lying above unramified primes, we extend their result to the case of general ideals whose prime ideal factors all lie over unramified primes, showing that by solving Hermite-SVP on a subideal with some factor γ, the solution may be lifted to yield a solution for Hermite-SVP in the original lattice with factor γ', where γ'/γ depends only on the factor given by Pan et. al. multiplied by a value determined by certain properties of the ideal and its decomposition group. We take this notion even more generally, and consider a module over the ring of integers of a Galois field and provide two methods by which one may attain a solution to the module variant of Hermite-SVP which can be lifted to a solution in the original module for Hermite-SVP with an upper bound, where the new constant is given in terms of the old factor multiplied by some factor dependent only on the ideals used to describe the module in the pseudo-basis representation.

The second half of the paper focuses on prime ideals of cyclotomic rings. Our work extends the results of Pan et. al. to prime ideal lattices constructed from more cyclotomic rings of more general conductors, covering the cases of a general composite conductor $N = s2^{n+1}$ and $s'p^{n+1}$ for some odd prime p, odd integer $s \geq 3$ and integer s', $\gcd(s', p) = 1$, which, combined with the work of Pan et. al., covers the case for any conductor N. In particular, our work shows that if the prime ideal in question lies above certain primes, then the dimension in which we have to solve SVP decreases significantly.

Theorem 1. *Let $N = s2^{n+1}$, where n is a positive integer and $s \geq 3$ is an odd integer. Let $\mathfrak{p}$ be a prime ideal in the ring $\mathbb{Z}[\zeta_N]$ and suppose that $\mathfrak{p}$ contains a rational prime ρ, where $\rho^{\phi(s)} \equiv 3 \mod 4$. Then, given an oracle that can solve SVP for $\phi(s)$-dimensional lattices, a shortest nonzero vector in $\mathfrak{p}$ can be found in time poly$(\phi(N), \log_2 \rho)$ under the canonical embedding.*

Theorem 2. *Let $N = sp^{n+1}$, where n is a positive integer, p is an odd prime and s is a positive integer such that $\gcd(s, p) = 1$. Let $\mathfrak{p}$ be a prime ideal in the ring $\mathbb{Z}[\zeta_N]$ and suppose that $\mathfrak{p}$ contains a rational prime ρ, where $\rho^{\phi(s)} = lp + a$ for some integers l, a, $\gcd(l, p) = \gcd(a, p) = 1$. Then, given an oracle that can solve SVP for $(p-1)\phi(s)$-dimensional lattices, a shortest nonzero vector in $\mathfrak{p}$ can be found in time poly$(\phi(N), \log_2 \rho)$ under the canonical embedding.*

As with the case for conductor $N = 2^{n+1}$, we must ask whether the "average case" of prime ideal SVP over such cyclotomic rings is easy. This question in itself is ill-defined, and depends on how we define the distribution from which we choose the prime ideal. As we show in section 5, if we were to pick our ideal by uniformly choosing an ideal from the set of prime ideals whose rational prime lies below a certain bound, the probability of choosing an easily solvable ideal lattice is non-negligible. However, if we are to uniformly choose from the distribution of ideals of norm less than a certain bound, the probability of choosing an easily solvable ideal lattice is negligible.

In the last few sections, we also cover the case of general cyclotomic ideals and modules defined over a pseudo basis of ideals and vectors. For the case of general ideals, in a similar fashion to that in Pan et. al.'s work, we analyse SVP by studying the prime decomposition of ideals, and show that the shortest nonzero vector in a general ideal can be found by finding the shortest nonzero vector in a subideal of a smaller dimension. Moreover, the algorithm used to tackle SVP in such a lattice does not use the prime decomposition of the ideal, which is the most computationally complex step after SVP. In the module case, we do not explicitly construct an algorithm to perform SVP, however we show that using the structure theorem for finitely generated modules over a principal ideal domain it is possible to construct an isomorphism such that SVP in the original module can be found by finding the shortest nonzero vector in a module which has smaller dimension as a lattice after canonically embedding the module.

Whilst this work may initially appear to destabilise the security of cryptosystems based on cyclotomic ideals or modules, we must point out that this work does not break Ring-LWE or respectively Module-LWE. Though Ideal-SVP and Module-SVP respectively underpin the security of Ring-LWE and Module-LWE respectively, our work does not directly impact the security of these schemes, since the worst-case to average-case security reduction is one-way.

1.3 Paper organisation

The paper is organised as follows. Section 2 covers the mathematical preliminaries, including a definition of lattices and their various properties, some basic algebraic number theory and ideal lattices. The preliminary section ends with some useful lemmas regarding the factorisation of polynomials over finite fields. Section 3 covers a reduction Hermite-SVP in ideal lattices and module lattices based over a Galois extension of $\mathbb{Q}$. In section 4, we present a reduction of SVP for prime ideals of cyclotomic rings of general conductor, and show that some special cases of prime ideals are much easier to perform SVP for than others. In section 5, we show that our method for prime ideal lattices may be lifted to the case of general ideal lattices of cyclotomic rings. In section 6, we show that modules over cyclotomic rings may be subject to a similar reduction of SVP under a suitable isomorphism map. In section 7, we discuss the average-case hardness of SVP for ideal and module lattices of cyclotomic rings.

2 Mathematical Preliminaries

2.1 Lattices and the Shortest Vector Problem

A lattice is a discrete additive subgroup of $\mathbb{R}^D$. A lattice L has a basis $B = \{\mathbf{b}_1, \ldots, \mathbf{b}_d\}, \mathbf{b}_i \in \mathbb{R}^D$ for some integer $d \leq D$, and every lattice point may be represented by the linear sum of basis vectors over the integers, that is,

$$L = L(B) = \left\{ \sum_{i=1}^{d} x_i \mathbf{b}_i : x_i \in \mathbb{Z} \right\}.$$

We say that L is full-rank if $d = D$. The determinant of L, $\det(L)$, is the square root of the volume of the fundamental parallelopiped generated by the lattice basis. If L is full-rank, then $\det(L) = |\det(B)|$.
In cryptography, the security of a lattice-based cryptosystem in most cases boils down to the computational hardness of the shortest vector problem (SVP). The problem goes as follows: given a lattice L with basis B, find the shortest nonzero vector in L with respect to the Euclidean (or otherwise specified) norm. Most cryptosystems, however, loosen the requirement of finding the shortest nonzero vector, and require the assailant to find a nonzero vector within some range of the shortest vector. One such problem is known as the Hermite-SVP, and goes as follows.

Definition 1. *Let L be a rank N lattice. The γ-Hermite-SVP is to find a nonzero lattice vector $\mathbf{v} \in L$ that satisfies*

$$\|\mathbf{v}\| \leq \gamma \det(L)^{1/N},$$

for some approximation factor $\gamma \geq 1$.

As opposed to the shortest lattice vector, the determinant of a lattice is well-defined and can be verified easily. Moreover, as discussed in [10], a solution to Hermite-SVP can be lifted to a solution for a variety of different SVP-related problems.

2.2 Algebraic Number Theory

An algebraic number field L is a finite extension of $\mathbb{Q}$ by some algebraic integer α, that is, the solution to a polynomial in $\mathbb{Z}[x]$. The degree of L over $\mathbb{Q}$ is equivalent to the degree of the minimal polynomial of α in $\mathbb{Q}(x)$. We denote by $\mathcal{O}_L$ the ring of integers of L, which is the maximal order of L. It is well known in algebraic number theory that any algebraic number field L is a $\mathbb{Q}$-vector space over the power basis $\{1, \theta, \theta^2, \ldots, \theta^{N-1}\}$ for some $\theta \in L$, and similarly the ring of integers $\mathcal{O}_L$ may be expressed as a $\mathbb{Z}$-module over a power basis $\{1, \theta', \ldots, \theta'^{N-1}\}$ for some $\theta' \in \mathcal{O}_K$ [30].

For a positive integer N, the cyclotomic polynomial $\Phi_N(x)$ is the polynomial given by

$$\Phi_N(x) = \prod_{k=1:\gcd(k,N)=1}^{N} \left(x - \exp\left(\frac{2\pi i k}{N}\right)\right),$$

or in other words, the polynomial whose roots are all the primitive Nth roots of unity. For ease of notation, we generally let $\zeta_N = \exp\left(\frac{2\pi i}{N}\right)$ denote the Nth root of unity. The field $L = \mathbb{Q}(\zeta_N)$ obtained by appending ζ_N to $\mathbb{Q}$ is called the cyclotomic field of conductor N, and such a field is of degree $\phi(N)$ over $\mathbb{Q}$, where

$$\phi(N) = N \prod_{p|N:p \text{ prime}} \left(1 - \frac{1}{p}\right)$$

is Euler's totient function, which measures the number of integers less than or equal to N which are coprime to N.
The embeddings σ of a number field L are the injective homomorphisms from L to $\mathbb{C}$ which fix $\mathbb{Q}$. The number of distinct embeddings is equivalent to the degree of L over $\mathbb{Q}$, and an embedding σ is said to be a real embedding if $\sigma(L) \subset \mathbb{R}$, and is said to be a complex embedding if $\sigma(L) \not\subset \mathbb{R}$. We define the *canonical embedding* Σ_L from a number field L of degree N to $\mathbb{C}^N$ by

$$\Sigma_L : L \to \mathbb{C}^N \quad a \mapsto (\sigma_1(a), \sigma_2(a), \ldots, \sigma_N(a)).$$

Moreover, we respectively define the trace and norm of an element in L by

$$\text{Trace}_{L/\mathbb{Q}}(a) := \sum_{i=1}^{N} \sigma_i(a), \quad \text{Norm}_{L/\mathbb{Q}}(a) = \prod_{i=1}^{N} \sigma_i(a).$$

Defining by $\overline{a}$ the complex conjugate of an element $a \in L$, note that $\beta(x, y) := \text{Trace}_{L/\mathbb{Q}}(x\overline{y})$ for all $x, y \in L$ defines a positive-definite bilinear form on the $\mathbb{Q}$-vector space generated by L.

Another way of embedding a number field L into $\mathbb{C}^N$ is using the so-called *coefficient embedding*. By expressing L by a $\mathbb{Q}$-vector space over a power basis $\{1, \alpha, \ldots, \alpha^{N-1}\}$, we may take any element $a = \sum_{i=0}^{N-1} a_i \alpha^i$ where $a_i \in \mathbb{Q}$ and define the embedding map

$$a \mapsto (a_0, a_1, \ldots, a_{N-1}).$$

It is important to note that the coefficient embedding depends on the choice of basis for L. Also, if $\mathcal{O}_K = \mathbb{Z}[\alpha]$ then $\mathcal{O}_K$ maps to $\mathbb{Z}^N$ under the coefficient embedding.

2.3 Ideal Lattices

An ideal $\mathcal{I}$ is a subring of the ring of integers $\mathcal{O}_L$. We say that an ideal $\mathfrak{p}$ is prime if, for any $ab \in \mathfrak{p}$ for $a, b \in \mathcal{O}_L$, then either a or b is an element of $\mathfrak{p}$. Under

the canonical embedding, an ideal forms a lattice in $\mathbb{R}^N$, and we call lattices constructed in this way *ideal lattices*. The volume of an ideal lattice $\mathcal{I}$ in $\mathbb{R}^N$ is $\text{Norm}_{L/\mathbb{Q}}(\mathcal{I})disc(L/\mathbb{Q})$, where $\text{Norm}_{L/\mathbb{Q}}(\mathcal{I})$ is the norm of the ideal $\mathcal{I}$ and is equivalent to the cardinality of $\mathcal{O}_L/\mathcal{I}$ (roughly speaking, the "density" of the ideal in $\mathcal{O}_L$), and $disc(L/\mathbb{Q})$ is the discriminant of L over $\mathbb{Q}$, which is equivalent to the volume of the lattice generated after embedding $\mathcal{O}_L$ via the canonical embedding.

In lattice-based cryptography, the cyclotomic number field $L = \mathbb{Q}(\zeta_N)$ is frequently used to define an ideal lattice. The ring of integers of L is $\mathcal{O}_L = \mathbb{Z}[\zeta_N]$ for any conductor N [29]. Suppose that the cyclotomic polynomial $\Phi_N(x)$ factors in the finite field as

$$\Phi_N(x) = \prod_{i=1}^{g} f_i(x)^e \mod p$$

for some rational prime p, where $f_i(x)$ are irreducible mod p. Then the ideal $p\mathcal{O}_L$ factors as

$$p\mathcal{O}_L = (\mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_g)^e,$$

where each $\mathfrak{p}_i = \langle p, f(\zeta_N)\rangle$ are prime ideals. We say the ideal $\mathfrak{p}_i$ *lies over* p. If $e > 1$, then p is said to be *ramified* in $\mathcal{O}_L$, and otherwise ($e = 1$) p is *unramified* in $\mathcal{O}_L$. As such, we are motivated to study the factorisation of cyclotomic polynomials over finite fields in order to better study the structure of prime ideals. However, before we delve into more technical details regarding the factorisation of polynomials over finite fields, we introduce the following definition, which will be a recurring theme throughout the paper, and will be a powerful tool to help tackle SVP in ideal lattices.

Definition 2. *Let $L/\mathbb{Q}$ be a finite Galois extension of degree N, and let G be the Galois group of L over $\mathbb{Q}$. The* decomposition group *D of a prime ideal $\mathfrak{p}$ is a subgroup of G satisfying*

$$D = \{\sigma \in G : \sigma(\mathfrak{p}) = \mathfrak{p}\},$$

that is, the embeddings of L that fix $\mathfrak{p}$. Then the decomposition field K of $\mathfrak{p}$ is defined by

$$K = \{x \in L : \forall \sigma \in D, \sigma(x) = x\},$$

that is, the subfield of L that is fixed by the decomposition group.

2.4 Factorisation of Cyclotomic Polynomials over Finite Fields

The following lemmas will be used throughout section 4 onwards. Lemmas 1-3 are standard in the study of finite fields, and we point the reader to [24] for more details, and also for any terminology regarding finite fields. Lemma 4 is stated and proved in [27].

Lemma 1. *Let q be a power of a prime and N be a positive integer such that $\gcd(q, N) = 1$. Then the Nth cyclotomic polynomial $\Phi_N(x)$ can be factorised into $\phi(N)/m$ distinct monic irreducible polynomials of the same degree m over $\mathbb{F}_q$, where m is the least positive integer such that $q^m \equiv 1 \mod N$.*

Lemma 2. *Let $f_1(x), f_2(x), \ldots, f_N(x)$ be distinct monic irreducible polynomials over $\mathbb{F}_q$ of degree m and order e, and let $t \geq 2$ be an integer whose prime factors divide e but not $\frac{q^m-1}{e}$. Assume that $q^m \equiv 1 \mod 4$ if $t \equiv 0 \mod 4$. Then $f_1(x^t), f_2(x^t), \ldots, f_N(x^t)$ are all distinct monic irreducible polynomials of degree mt and order et.*

Lemma 3. *Let $f(x)$ be an irreducible polynomial over $\mathbb{F}_q$ of degree m and with $f(0) \neq 0$. Then the order of $f(x)$ is equal to the order of any root of $f(x)$ in the multiplicative group $\mathbb{F}^*_{q^m}$.*

Lemma 4. *Let p be an odd prime, and q be a prime power such that $q \equiv 1 \mod p$. If m, n are positive integers satisfying $p^n \mid q^{p^{n-m}} - 1$ and $p \nmid \frac{q^{p^{n-m}}-1}{p^n}$, then $p^{n+1} \mid q^{n+1-m} - 1$ and $p \nmid \frac{q^{p^{n+1-m}}-1}{p^{n+1}}$.*

3 Solving Hermite-SVP for general ideal lattices in a Galois extension

In this section, we generalise the results of Pan et. al., specifically their contributions on Hermite-SVP in prime ideal lattices. We consider first general ideal lattices, and then modules with a pseudo-basis of ideals and vectors with entries in the overlying number field.

Definition 1. Let $L/\mathbb{Q}$ be a finite Galois extension and $I \subset \mathcal{O}_L$ an ideal, expressible as $\mathcal{I} = \mathfrak{p}_1 ... \mathfrak{p}_g$, where each $\mathfrak{p}_i$ lies above unramified rational prime p_i. Let $D_\mathcal{I} = \{\sigma \in Gal(L/\mathbb{Q}) : \sigma(\mathcal{I}) = \mathcal{I}\}$, and $K_\mathcal{I} = L^{D_\mathcal{I}} = \{x \in L : \sigma(x) = x, \text{ for all } \sigma \in D_\mathcal{I}\}$. These are called the *decomposition group* and *decomposition field* of $\mathcal{I}$, respectively.

Theorem 3. *Let $L/\mathbb{Q}$ be a finite Galois extension of degree N and $\mathcal{I} = \mathfrak{p}_1 ... \mathfrak{p}_g$ an ideal of O_L, where each $\mathfrak{p}_i$ lies over an unramified rational prime p_i such that p_i has g_i distinct prime ideal factors in O_L. If $K_\mathcal{I}$ is the decomposition field of $\mathcal{I}$, then a solution to Hermite-SVP with factor γ in the sublattice $\mathfrak{c} = \mathcal{I} \cap O_{K_\mathcal{I}}$ under the canonical embedding of $K_\mathcal{I}$ will also be a solution to Hermite-SVP in $\mathcal{I}$ with factor $\gamma \frac{\sqrt{N/r} Norm_{L/\mathbb{Q}}(\mathcal{I})^{1/r-1/N}}{Norm_{K_\mathcal{I}/\mathbb{Q}}(disc(L/K_\mathcal{I}))^{1/2N} (p_1^{(f^L_{p_1} - f^{K_\mathcal{I}}_{p_1})1/r} \ldots p_g^{(f^L_{p_g} - f^{K_\mathcal{I}}_{p_g})1/r})}$ under the canonical embedding of L.*

Consider the following diagram:

$$\begin{array}{ccccc} \mathcal{O}_L & \hookrightarrow & L & \xrightarrow{\Sigma_L} & \mathbb{C}^N \\ \uparrow & & \uparrow & & \uparrow \beta' \\ \mathcal{O}_{K_I} & \hookrightarrow & K_I & \xrightarrow{\Sigma_{K_I}} & \mathbb{C}^{[K_I:\mathbb{Q}]} \end{array}$$

Here β' is chosen to make the diagram commute. Each embedding of K_I extends to $N/[K_I:\mathbb{Q}]$ embeddings of L. Then β' simply repeats the coordinates of Σ_{K_I} N/r times, for $r = [K_I:\mathbb{Q}]$, by the definition of K_I. So $\|\beta'(x)\| = \sqrt{N/r}\|x\|$, for any $x \in \Sigma_{K_I}(K_I)$. Set $\mathfrak{c} = I \cap \mathcal{O}_{K_I}$. Then $det(\mathfrak{c}) = \mathrm{Norm}_{K_I/\mathbb{Q}}(\mathfrak{c})\sqrt{|disc(K_I/\mathbb{Q})|}$. So Hermite-SVP solution $v \in \mathfrak{c}$ satisfies $\|v\| \leq \gamma(\mathrm{Norm}_{K_I/\mathbb{Q}}(\mathfrak{c})\sqrt{|disc(K_I/\mathbb{Q})|})^{1/r}$. Also note $disc(L/\mathbb{Q}) = disc(K_I/\mathbb{Q})^{N/r}\mathrm{Norm}_{K_I/\mathbb{Q}}(disc(L/K_I))$. Then

$$\begin{aligned}
\|\beta'(v)\| &\leq \sqrt{N/r}\|v\| \leq \sqrt{N/r}\gamma \cdot (\mathrm{Norm}_{K_I/\mathbb{Q}}(\mathfrak{c})\sqrt{|disc(K_I/\mathbb{Q})|})^{1/r} \\
&= \sqrt{N/r}\gamma \cdot \mathrm{Norm}_{K_I/\mathbb{Q}}(\mathfrak{c})^{1/r}\Big(\frac{disc(L/\mathbb{Q})^{r/N}}{\mathrm{Norm}_{K_I/\mathbb{Q}}(disc(L/K_I))^{r/N}}\Big)^{1/2r} \\
&= \sqrt{N/r}\gamma \cdot \mathrm{Norm}_{K_I/\mathbb{Q}}(\mathfrak{c})^{1/r}\frac{disc(L/\mathbb{Q})^{1/2N}}{\mathrm{Norm}_{K_I/\mathbb{Q}}(disc(L/K_I))^{1/2N}} \\
&= \gamma\frac{\sqrt{N/r}}{\mathrm{Norm}_{K_I/\mathbb{Q}}(disc(L/K_I))^{1/2N}} \cdot \mathrm{Norm}_{K_I/\mathbb{Q}}(\mathfrak{c})^{1/r}disc(L/\mathbb{Q})^{1/2N} \\
&= \gamma\frac{\sqrt{N/r}}{\mathrm{Norm}_{K_I/\mathbb{Q}}(disc(L/K_I))^{1/2N}} \cdot \big(\mathrm{Norm}_{K_I/\mathbb{Q}}(\mathfrak{c})^{N/r}\sqrt{disc(L/\mathbb{Q})}\big)^{1/N}.
\end{aligned}$$

The norm is multiplicative: $\mathrm{Norm}_{K_I/\mathbb{Q}}(I) = \mathrm{Norm}_{K_I/\mathbb{Q}}(\mathcal{P}_1)...\mathrm{Norm}_{K_I/\mathbb{Q}}(\mathcal{P}_g)$, where $\mathcal{P}_i = \mathfrak{p}_i \cap K_I$. All the $\mathfrak{p}_i$ lie above unramified primes p_i, so we can write $e^L_{p_i} = 1$. Moreover, we have $\mathrm{Norm}_{L/\mathbb{Q}} = \mathrm{Norm}_{K_I/\mathbb{Q}} \circ \mathrm{Norm}_{L/K_I}$. As a result, $\mathrm{Norm}_{L/\mathbb{Q}}(I) = p_1^{f^L_{p_1}}...p_g^{f^L_{p_g}}$, where $f^L_{p_i}$ is the inertial degree of p_i in $\mathcal{O}_L$. Also, $\mathrm{Norm}_{K_I/\mathbb{Q}}(\mathfrak{c}) = p_1^{f^{K_I}_{p_1}}...p_g^{f^{K_I}_{p_g}}$. Thus $\mathrm{Norm}_{L/\mathbb{Q}}(I) = p_1^{f^L_{p_1}}...p_g^{f^L_{p_g}} = (p_1^{f^{K_I}_{p_1}}...p_g^{f^{K_I}_{p_g}}) \cdot (p_1^{f^L_{p_1}-f^{K_I}_{p_1}}...p_g^{f^L_{p_g}-f^{K_I}_{p_1}}) = \mathrm{Norm}_{K_I/\mathbb{Q}}(\mathfrak{c}) \cdot (p_1^{f^L_{p_1}-f^{K_I}_{p_1}}...p_g^{f^L_{p_g}-f^{K_I}_{p_g}})$, so we can rewrite $\mathrm{Norm}_{K_I/\mathbb{Q}}(\mathfrak{c}) = \mathrm{Norm}_{L/\mathbb{Q}}(I)/(p_1^{f^L_{p_1}-f^{K_I}_{p_1}}...p_g^{f^L_{p_g}-f^{K_I}_{p_g}})$. Then we have, setting $\gamma' = \gamma\frac{\sqrt{N/r}}{\mathrm{Norm}_{K_I/\mathbb{Q}}(disc(L/K_I))^{1/2N}}$,

$$\begin{aligned}
\|\beta'(v)\| &\leq \gamma\frac{\sqrt{N/r}}{\mathrm{Norm}_{K_I/\mathbb{Q}}(disc(L/K_I))^{1/2N}} \cdot \big(\mathrm{Norm}_{K_I/\mathbb{Q}}(\mathfrak{c})^{N/r}\sqrt{disc(L/\mathbb{Q})}\big)^{1/N} \\
&= \gamma' \cdot \Big(\big(\mathrm{Norm}_{L/\mathbb{Q}}(I)/(p_1^{f^L_{p_1}-f^{K_I}_{p_1}}...p_g^{f^L_{p_g}-f^{K_I}_{p_g}})\big)^{N/r}\sqrt{disc(L/\mathbb{Q})}\Big)^{1/N} \\
&= \gamma' \cdot \big(\mathrm{Norm}_{L/\mathbb{Q}}(I)^{N/r}/(p_1^{(f^L_{p_1}-f^{K_I}_{p_1})N/r}...p_g^{(f^L_{p_g}-f^{K_I}_{p_g})N/r})\sqrt{disc(L/\mathbb{Q})}\big)^{1/N} \\
&= \gamma'\frac{\mathrm{Norm}_{L/\mathbb{Q}}(I)^{1/r-1/N}}{(p_1^{(f^L_{p_1}-f^{K_I}_{p_1})1/r}...p_g^{(f^L_{p_g}-f^{K_I}_{p_g})1/r})} \cdot \big(\mathrm{Norm}_{L/\mathbb{Q}}(I)\sqrt{disc(L/\mathbb{Q})}\big)^{1/N}.
\end{aligned}$$

Note that when $\mathcal{I} = \mathfrak{p}$, K_I is the regular decomposition field, and $f^{K_I}_p = 1$ and $f^L_p = N/r$, so $\mathrm{Norm}_{L/\mathbb{Q}}(I)^{1/r-1/N} = p^{N/r(1/r-1/N)} = p^{N/r^2-1/r}$ and $p^{(f^L_p-f^{K_I}_p)1/r)} = p^{N/r^2-1/r}$, and we have recovered the result of the original paper.

3.1 Solving Hermite-SVP for module lattices defined over a Galois extension

The above method can be extended to the case of $\mathcal{O}_L$-modules. We propose two separate methods by which we can approach this problem, yielding different bounds in each, which may be individually useful depending on the considered module. As before, L is a field that is a Galois extension of $\mathbb{Q}$ with ring of integers $\mathcal{O}_L$. Suppose $\mathcal{I}_1, \ldots, \mathcal{I}_d \subset \mathcal{O}_L$ are some ideals of $\mathcal{O}_L$, and $\mathbf{b}_1, \ldots, \mathbf{b}_d \in L^D$ for some integer $d \leq D$. An $\mathcal{O}_L$-module M is defined as the direct sum

$$M = \bigoplus_{k=1}^{d} \mathcal{I}_k \mathbf{b}_k,$$

which is a $\mathbb{Z}$-module of finite dimension. We define the volume of M by

$$\mathrm{Vol}(M) = \mathrm{Norm}_{L/\mathbb{Q}}(\det(B^\dagger B)) \prod_{k=1}^{d} \mathrm{Norm}_{L/\mathbb{Q}}(\mathcal{I}_k)^2,$$

where B is the matrix composed of the columns $\mathbf{b}_1, \ldots, \mathbf{b}_d$, and $\dagger$ denotes the Hermitian transpose. Suppose that each $\mathbf{b}_k$ may be expressed as $\mathbf{b}_k = (b_{k,1}, \ldots, b_{k,D})$. Letting $\overline{x}$ denote the complex conjugate of x and $\langle \cdot, \cdot \rangle$ denote standard inner product of two complex vectors, the positive-definite quadratic form generated by the module M after embedding is given by

$$\begin{aligned} q(x_1, \ldots, x_d) &= \mathrm{Trace}_{L/\mathbb{Q}} \left(\left\langle \sum_{k=1}^{d} x_k \mathbf{b}_k, \sum_{k=1}^{d} x_k \mathbf{b}_k \right\rangle \right) \\ &= \mathrm{Trace}_{L/\mathbb{Q}} \left(\sum_{k,l=1}^{d} x_k \overline{x_l} \left(\sum_{i=1}^{D} b_{k,i} \overline{b_{l,i}} \right) \right), \end{aligned}$$

where $x_k \in \mathcal{I}_k$. We define the module variant of Hermite-SVP with approximation $\gamma \geq 1$ to find an element in M such that

$$q(x_1, \ldots, x_d) \leq \gamma \mathrm{Vol}(M)^{\frac{1}{2d[L:\mathbb{Q}]}}.$$

As in the previous subsection, denote by $K_{\mathcal{I}_l}$ the decomposition field of the ideal $\mathcal{I}_l$, and let K be the minimum field containing all $K_{\mathcal{I}_l}$. Then we must have

$$\begin{aligned} &\mathrm{Trace}_{L/\mathbb{Q}} \left(\sum_{k,l=1}^{d} x_k \overline{x_l} \left(\sum_{i=1}^{D} b_{k,i} \overline{b_{l,i}} \right) \right) \\ &= \mathrm{Trace}_{K/\mathbb{Q}} \left(\mathrm{Trace}_{L/K} \left(\sum_{k,l=1}^{d} x_k \overline{x_l} \left(\sum_{i=1}^{D} b_{k,i} \overline{b_{l,i}} \right) \right) \right) \\ &= \mathrm{Trace}_{K/\mathbb{Q}} \left(\sum_{k,l=1}^{d} x_k \overline{x_l} \left(\sum_{i=1}^{D} \mathrm{Trace}_{L/K} \left(b_{k,i} \overline{b_{l,i}} \right) \right) \right). \end{aligned}$$

Let $\mathfrak{c}_l = \mathcal{I}_l \cap \mathcal{O}_{K_{\mathcal{I}_l}}$ for all $1 \leq l \leq d$, and consider the module

$$M' = \bigoplus_{k=1}^{d} \mathfrak{c}_k \mathbf{b}'_k,$$

where $\mathbf{b}'_k$ are vectors in $L^{D[L:K]}$ such that $\langle \mathbf{b}'_k, \mathbf{b}'_l \rangle = \sum_{i=1}^{D} \mathrm{Trace}_{L/K}\left(b_{k,i}\overline{b_{l,i}}\right)$ for all $1 \leq k, l \leq d$. The quadratic form generated by M' is a subset of the quadratic form generated by M, given by

$$q'(y_1, \ldots, y_d) = \mathrm{Trace}_{K/\mathbb{Q}}\left(\sum_{k,l=1}^{d} y_k \overline{y_l}\left(\sum_{i=1}^{D} \mathrm{Trace}_{L/K}(b_{k,i}\overline{b_{l,i}})\right)\right),$$

for $y_k \in \mathfrak{c}_k$, and the volume of M' in the space generated by embedding L^D is

$$\mathrm{Vol}(M') = \mathrm{Norm}_{L/\mathbb{Q}}(\det(G)) \prod_{k=1}^{d} \mathrm{Norm}_{L/\mathbb{Q}}(\mathfrak{c}_k)^2.$$

Letting $\mathcal{I}_l = \mathfrak{p}_1^{(l)}\mathfrak{p}_2^{(l)} \ldots \mathfrak{p}_{g_l}^{(l)}$ be the prime decomposition of the ideal $\mathcal{I}_l$, where $\mathfrak{p}_k^{(l)}$ are (not necessarily distinct) prime ideals, we have

$$\mathrm{Norm}_{K_{\mathcal{I}_l}}(\mathcal{I}_l) = \prod_{k=1}^{g_l} \mathrm{Norm}_{K_{\mathcal{I}_l}}(\mathcal{P}_k^{(l)}),$$

where $\mathcal{P}_k^{(l)} := \mathfrak{p}_k^{(l)} \cap K_{\mathcal{I}_l}$. Assume that each $\mathfrak{p}_k^{(l)}$ lies over an unramified prime $p_k^{(l)}$, then $e^L_{p_k^{(l)}} = 1$ for each l, k. Moreover, we have $\mathrm{Norm}_{L/\mathbb{Q}} = \mathrm{Norm}_{K_{\mathcal{I}_l}/\mathbb{Q}} \circ \mathrm{Norm}_{L/K_{\mathcal{I}_l}}$. As a result, for all $1 \leq l \leq d$,

$$\mathrm{Norm}_{L/\mathbb{Q}}(\mathcal{I}_l) = \prod_{k=1}^{g_l} {p_k^{(l)}}^{f^L_{p_k^{(l)}}},$$

where $f^L_{p_k^{(l)}}$ is the inertial degree of $p_k^{(l)}$ in $\mathcal{O}_L$. Also,

$$\mathrm{Norm}_{K_{\mathcal{I}_l}/\mathbb{Q}}(\mathfrak{c}_l) = \prod_{k=1}^{g_l} {p_k^{(l)}}^{f^{K_{\mathcal{I}_l}}_{p_k^{(l)}}}.$$

Thus

$$\begin{aligned}\mathrm{Norm}_{L/\mathbb{Q}}(\mathcal{I}_l) = \prod_{k=1}^{g_l} {p_k^{(l)}}^{f^L_{p_k^{(l)}}} &= \prod_{k=1}^{g_l} {p_k^{(l)}}^{f^{K_{\mathcal{I}_l}}_{p_k^{(l)}}} \prod_{k=1}^{g_l} {p_k^{(l)}}^{f^L_{p_k^{(l)}} - f^{K_{\mathcal{I}_l}}_{p_k^{(l)}}} \\ &= \mathrm{Norm}_{K_{\mathcal{I}_l}/\mathbb{Q}}(\mathfrak{c}_l) \prod_{k=1}^{g_l} {p_k^{(l)}}^{f^L_{p_k^{(l)}} - f^{K_{\mathcal{I}_l}}_{p_k^{(l)}}},\end{aligned}$$

so we may rewrite

$$\mathrm{Norm}_{K_{\mathcal{I}_l}/\mathbb{Q}}(\mathfrak{c}_l) = \mathrm{Norm}_{L/\mathbb{Q}}(\mathcal{I}_l) \prod_{k=1}^{g_l} {p_k^{(l)}}^{-\left(f^L_{p_k^{(l)}} - f^{K_{\mathcal{I}_l}}_{p_k^{(l)}}\right)}.$$

We assume that we have a tuple $(y_1, \ldots, y_d), y_k \in \mathfrak{c}_k$, that satisfies

$$q'(y_1, \ldots, y_d) \leq \gamma \mathrm{Vol}(M')^{\frac{1}{2d[L:\mathbb{Q}]}}.$$

Then, by definition of the volume of M',

$$\begin{aligned} q'(y_1, \ldots, y_d) &\leq \gamma \left(\mathrm{Norm}_{L/\mathbb{Q}}(\det(B^\dagger B)) \prod_{k=1}^{d} \mathrm{Norm}_{L/\mathbb{Q}}(\mathfrak{c}_k)^2 \right)^{\frac{1}{2d[L:\mathbb{Q}]}} \\ &= \gamma \left(\frac{\mathrm{Norm}_{L/\mathbb{Q}}(\det(B^\dagger B)) \prod_{l=1}^{d} \mathrm{Norm}_{L/\mathbb{Q}}(\mathcal{I}_l)^{2[L:K_{\mathcal{I}_l}]}}{\prod_{k=1}^{g_l} {p_k^{(l)}}^{[L:K_{\mathcal{I}_l}]\left(f^L_{p_k^{(l)}} - f^{K_{\mathcal{I}_l}}_{p_k^{(l)}}\right)}} \right)^{\frac{1}{2d[L:\mathbb{Q}]}} \\ &= \gamma \mathrm{Vol}(M)^{\frac{1}{2d[L:\mathbb{Q}]}} \frac{\prod_{l=1}^{d} \mathrm{Norm}_{L/\mathbb{Q}}(\mathcal{I}_l)^{\frac{[L:K_{\mathcal{I}_l}]-1}{d[L:\mathbb{Q}]}}}{\prod_{k=1}^{g_l} {p_k^{(l)}}^{\frac{[L:K_{\mathcal{I}_l}]-1}{d[L:\mathbb{Q}]}\left(f^L_{p_k^{(l)}} - f^{K_{\mathcal{I}_l}}_{p_k^{(l)}}\right)}}. \end{aligned}$$

Since all $y_k \in \mathfrak{c}_k \subseteq \mathcal{I}_k$, we have $q(y_1, \ldots, y_d) = q'(y_1, \ldots, y_d)$, and so we arrive at the following theorem.

Theorem 4. *Let $L/\mathbb{Q}$ be a finite Galois extension of degree $[L : \mathbb{Q}]$ and let $\mathcal{I}_1, \mathcal{I}_2, \ldots, \mathcal{I}_d$ be ideals of $\mathcal{O}_L$, expressible as $\mathcal{I}_k = \mathfrak{p}_1^{(k)}\mathfrak{p}_2^{(k)} \ldots \mathfrak{p}_{g_k}^{(k)}$, where each $\mathfrak{p}_l^{(k)}$ is a (not necessarily distinct) prime ideal lying above an unramified rational prime $p_l^{(k)}$ such that $p_l^{(k)}$ has $g_l^{(k)}$ distinct prime ideal factors in $\mathcal{O}_L$. Let $\langle \mathcal{I}_k, \mathbf{b}_k \rangle_{k=1}^d$ define a pseudo-basis of a module M, where*

$$M = \bigoplus_{k=1}^{d} \mathcal{I}_k \mathbf{b}_k.$$

Here, $\mathbf{b}_k \in L^D$ for some integers $d \leq D$. If $K_{\mathcal{I}_l}$ is the decomposition field of the ideal $\mathcal{I}_l$, define $\mathfrak{c}_l = \mathcal{I}_l \cap \mathcal{O}_{K_{\mathcal{I}_l}}$. Define by M' the module given by

$$M' = \bigoplus_{k=1}^{d} \mathfrak{c}_k \mathbf{b}'_k,$$

where $\mathbf{b}'_k$ are defined so that $\langle \mathbf{b}'_k, \mathbf{b}'_l \rangle = \sum_{i=1}^{D} Trace_{L/K}\left(b_{k,i}\overline{b_{l,i}}\right)$ for all $1 \leq k, l \leq d$. Then, given a tuple $(y_1, \ldots, y_d), y_k \in \mathfrak{c}_k$ that acts as a solution to Hermite-SVP with factor γ in the space generated by embedding L^D in the module M' (where

we define Hermite-SVP for modules as in the definition in this subsection), the tuple yields a solution to Hermite-SVP in the module M with factor γ', where

$$\gamma' = \gamma \prod_{l=1}^{d} Norm_{L/\mathbb{Q}}(\mathcal{I}_l)^{\frac{[L:K_{\mathcal{I}_l}]-1}{d[L:\mathbb{Q}]}} \prod_{k=1}^{g_l} p_k^{(l)^{-\frac{[L:K_{\mathcal{I}_l}]-1}{d[L:\mathbb{Q}]}\left(f^L_{p_k^{(l)}} - f^{K_{\mathcal{I}_l}}_{p_k^{(l)}}\right)}}.$$

Alternatively, the method below leads to a similar result for a different γ' :

Theorem 5. *Let $M \subset L^d$ be a finitely generated, torsion-free $\mathcal{O}_L$-module. Then there exists a submodule $M' \subset M$, a subfield $K \subset L$, and fractional $\mathcal{O}_L$-ideals I_i such that a solution to Hermite-SVP with factor γ in M' is a solution to Hermite-SVP in M with factor $\gamma' = \frac{\gamma\sqrt{r/r'}\sqrt{disc(L/\mathbb{Q})}^{\frac{k-1}{rk}} N^{1/r}}{\sqrt[2r]{Norm_{K/\mathbb{Q}}(disc(L/K))}}$, where $r = [L:\mathbb{Q}]$, $r' = [K:\mathbb{Q}]$, for $\bar{I}_i = I_i \cap K$ and $N = Norm_{L/\mathbb{Q}(\bar{I}_i)}/Norm_{L/\mathbb{Q}}(I_i)$.*

Proof. Let $M \subset L^d$ be a finitely generated, torsion-free $\mathcal{O}_L$-module, with generators $x_1, ..., x_k$. Then by the structure theorem for finitely generated modules over Dedekind domains, $M \cong \oplus_{i=1}^k I_i$, for I_i rank one projective $\mathcal{O}_L$-modules, i.e. fractional ideals. Set $H = \{\sigma \in Gal(L/\mathbb{Q}) : \sigma(I_i) = I_i \text{ for } i = 1, ..., k\}$. Let K be the fixed field of H. Write $[L:\mathbb{Q}] = r$, and set $[K:\mathbb{Q}] = r'$. Define the sublattice M' isomorphic to the direct sum $M' \cong \oplus_{i=1}^k (I_i \cap K)$, which is an $\mathcal{O}_K$-module. Then we have the following diagram, where Σ denotes the canonical embedding of the module, applied to each summand in the direct sum of M and M':

$$\begin{array}{ccccc} M & \hookrightarrow & L^d & \xrightarrow{\Sigma_{L^d}} & \mathbb{C}^{dr} \\ \uparrow & & \uparrow & & \beta\uparrow \\ M' & \hookrightarrow & K^d & \xrightarrow{\Sigma_{K^d}} & \mathbb{C}^{dr'} \end{array}$$

Here Σ_{K^d} is the canonical embedding of K applied coordinatewise to the module, and because of the definition of K, β is the repetition of each coordinate r/r' times, i.e. for $v \in K^d$, $\|\beta(v)\| = \sqrt{r/r'}\|v\|$. Now, suppose $v \in M'$ is a solution to Hermite-SVP, so $\|v\| \leq \gamma \cdot det(M')^{1/kr'}$. Then, writing $I_i \cap K = \bar{I}_i$, we have

$$\begin{aligned} \|\beta(v)\| &= \sqrt{r/r'}\|v\| \\ &\leq \sqrt{r/r'}\gamma \cdot det(M')^{1/kr'} = \gamma\sqrt{r/r'} \cdot det\big(\oplus_{i=1}^k (I_i \cap K)\big)^{1/kr'} \\ &= \gamma\sqrt{r/r'} \cdot \prod_{i=1}^k det\big(\bar{I}_i\big)^{1/kr'} = \gamma\sqrt{r/r'} \cdot \big(\prod_{i=1}^k det(\bar{I}_i)\big)^{1/kr'} \\ &= \gamma\sqrt{r/r'} \cdot \big(\prod_{i=1}^k \mathrm{Norm}_{K/\mathbb{Q}}(\bar{I}_i)\sqrt{|disc(K/\mathbb{Q})|}\big)^{1/kr'} \\ &= \gamma\sqrt{r/r'} \cdot \big(\sqrt{|disc(K/\mathbb{Q})|}\big)^{1/r'} \big(\prod_{i=1}^k \mathrm{Norm}_{K/\mathbb{Q}}(\bar{I}_i)\big)^{1/kr'}. \end{aligned}$$

Using the fact that $disc(L/\mathbb{Q}) = disc(K/\mathbb{Q})^{r/r'}\mathrm{Norm}_{K/\mathbb{Q}}(disc(L/K))$, we rearrange for $disc(K/\mathbb{Q})^{1/r'} = \sqrt[r]{disc(L/\mathbb{Q})/\mathrm{Norm}_{K/\mathbb{Q}}(disc(L/K))}$ and say

$$\begin{aligned}
\|\beta(v)\| &\leq \gamma\sqrt{r/r'} \cdot \left(\sqrt{|disc(K/\mathbb{Q})|}\right)^{1/r'} \left(\prod_{i=1}^{k} \mathrm{Norm}_{K/\mathbb{Q}}(\bar{I}_i)\right)^{1/kr'} \\
&= \gamma\sqrt{r/r'} \cdot \sqrt[2r]{disc(L/\mathbb{Q})/\mathrm{Norm}_{K/\mathbb{Q}}(disc(L/K))} \left(\prod_{i=1}^{k} \mathrm{Norm}_{K/\mathbb{Q}}(\bar{I}_i)\right)^{1/kr'} \\
&= \frac{\gamma\sqrt{r/r'}}{\sqrt[2r]{\mathrm{Norm}_{K/\mathbb{Q}}(disc(L/K))}} \cdot \sqrt[2r]{disc(L/\mathbb{Q})} \left(\prod_{i=1}^{k} \mathrm{Norm}_{K/\mathbb{Q}}(\bar{I}_i)\right)^{1/kr'} \\
&= \frac{\gamma\sqrt{r/r'}\sqrt{disc(L/\mathbb{Q})}^{\frac{k-1}{rk}}}{\sqrt[2r]{\mathrm{Norm}_{K/\mathbb{Q}}(disc(L/K))}} \cdot \sqrt{disc(L/\mathbb{Q})}^{1/rk} \left(\prod_{i=1}^{k} \mathrm{Norm}_{K/\mathbb{Q}}(\bar{I}_i)\right)^{1/kr'}.
\end{aligned}$$

We can write $\mathrm{Norm}_{K/\mathbb{Q}}(\bar{I}_i) = N^{r'/r}\mathrm{Norm}_{L/\mathbb{Q}}(I_i)^{r'/r}$, where N is as in the statement of the theorem. Moreover, setting $\tilde{\gamma} = \frac{\gamma\sqrt{r/r'}\sqrt{disc(L/\mathbb{Q})}^{\frac{k-1}{rk}}}{\sqrt[2r]{\mathrm{Norm}_{K/\mathbb{Q}}(disc(L/K))}}$, we plug both into our expression for

$$\begin{aligned}
\|\beta(v)\| &\leq \frac{\gamma\sqrt{r/r'}\sqrt{disc(L/\mathbb{Q})}^{\frac{k-1}{rk}}}{\sqrt[2r]{\mathrm{Norm}_{K/\mathbb{Q}}(disc(L/K))}} \cdot \sqrt{disc(L/\mathbb{Q})}^{1/rk} \left(\prod_{i=1}^{k} \mathrm{Norm}_{K/\mathbb{Q}}(\bar{I}_i)\right)^{1/kr'} \\
&= \tilde{\gamma} \cdot \sqrt{disc(L/\mathbb{Q})}^{1/rk} \left(\prod_{i=1}^{k} N^{r'/r}\mathrm{Norm}_{L/\mathbb{Q}}(I_i)^{r'/r}\right)^{1/kr'} \\
&= \tilde{\gamma}N^{1/r} \cdot \sqrt{disc(L/\mathbb{Q})}^{1/rk} \left(\prod_{i=1}^{k} \mathrm{Norm}_{L/\mathbb{Q}}(I_i)\right)^{1/rk} \\
&= \tilde{\gamma}N^{1/r} \cdot \left(\prod_{i=1}^{k} \mathrm{Norm}_{L/\mathbb{Q}}(I_i)\sqrt{disc(L/\mathbb{Q})}\right)^{1/rk} = \gamma' \cdot det(M)^{1/rk},
\end{aligned}$$

so letting $\gamma' = \tilde{\gamma}N^{1/r} = \frac{\gamma\sqrt{r/r'}\sqrt{disc(L/\mathbb{Q})}^{\frac{k-1}{rk}}N^{1/r}}{\sqrt[2r]{\mathrm{Norm}_{K/\mathbb{Q}}(disc(L/K))}}$, v is a solution to Hermite-SVP in M with approximation factor γ'. □

4 Prime Ideals of Cyclotomic Fields

4.1 The Cyclotomic Field $L = \mathbb{Q}(\zeta_{s2^{n+1}})$

We let s be some positive odd integer, $s \geq 3$. The following is Theorem 2.2 from [26].

Theorem 6. *Let q be an odd prime power, and let $s \geq 3$ be any odd number such that $\gcd(q, s) = 1$, and let $q^{\phi(s)} = m2^A + 1$ for some odd m, $A \geq 1$. Then, for any $A - 1 \leq n$ and for any irreducible factor $f(x)$ of $\Phi_{s2^A}(x)$ over $\mathbb{F}_q$,*

then $f(x^{2^{n-A+1}})$ is also irreducible over $\mathbb{F}_q$. Moreover, all irreducible factors of $\Phi_{s2^{n+1}}(x)$ are obtained in this way.

Theorem 7. *For any prime ideal $\mathfrak{p} = \langle \rho, f(\zeta_{s2^{n+1}}) \rangle$ of $\mathcal{O}_L$ for some rational prime ρ, $\gcd(\rho, s) = \gcd(\rho, 2) = 1$ and irreducible polynomial $f(x)$ of $\Phi_{s2^{n+1}}$ in $\mathbb{F}_\rho[x]$, write $\rho^{\phi(s)} = m2^A + 1$ where m is an odd integer and $A \geq 1$, and let $r = \min\{A-1, n\}$. Then, given an oracle that can solve SVP for $\phi(s2^{r+1})$-dimensional lattices, a shortest nonzero vector in $\mathfrak{p}$ can be found in $poly(\phi(s2^{n+1}), \log_2 \rho)$ time with the canonical embedding.*

Proof. We assume that $n \geq A$ otherwise the theorem is vacuously true, so $r = A - 1$. Let

$$G = \{\sigma_i : \gcd(i, 2) = \gcd(i, s) = 1\}$$

denote the Galois group of L over $\mathbb{Q}$, where

$$\sigma_i : \mathbb{Q}(\zeta_{s2^{n+1}}) \to \mathbb{Q}(\zeta_{s2^{n+1}}),$$
$$\sigma_i(\zeta^k_{s2^{n+1}}) = \zeta^{ki}_{s2^{n+1}}.$$

By Theorem 6, for any factor $f(x)$ of $\Phi_{s2^{n+1}}(x)$ that is irreducible in $\mathbb{F}_\rho[x]$, there exists a polynomial $g(x)$ that is a factor of $\Phi_{s2^{r+1}}(x)$ that is irreducible over $\mathbb{F}_\rho[x]$ such that $f(x) = g(x^{2^{n-r}})$. Then the prime ideal lattice $\mathfrak{p}$ can be represented by

$$\langle \rho, f(\zeta_{s2^{n+1}}) \rangle = \langle \rho, g(\zeta_{s2^{r+1}}) \rangle.$$

For any $1 \leq k \leq 2^{n-r-1}$, the map $\sigma_{ks2^{r+1}+1}$ fixes $\zeta^{l2^{n-r}}_{s2^{n+1}}$ for any integer $0 \leq l < s2^{r+1}$. Moreover, since $\gcd(ks2^{r+1} + 1, 2) = \gcd(ks2^{r+1}, s) = 1$, each subset H_k of G generated $\sigma_{ks2^{r+1}+1}$ forms a cyclic group, and so the set $H = H_1 \times H_2 \times \cdots \times H_{2^{n-r-1}}$ forms a subgroup of the decomposition group of $\mathfrak{p}$, since both ρ and $f(\zeta_{s2^{n+1}}) = g(\zeta^{2^{n-r}}_{2^{n+1}})$ are fixed by each $\sigma_i \in H$. $K = \mathbb{Q}(\zeta^{2^{n-r}}_{s2^{n+1}})$ must be the fixed field of the group H, as for all $i \in \left(\mathbb{Z}/s2^{n+1}\mathbb{Z}\right)^\times$,

$$\sigma_i(\zeta^{2^{n-r}}_{s2^{n+1}}) = \zeta^{2^{n-r}}_{s2^{n+1}} \iff i \equiv 1 \mod s2^{r+1}.$$

Note that $\mathcal{O}_K$ has the $\mathbb{Z}$-basis $\{1, \zeta^{2^{n-r}}_{s2^{n+1}}, \zeta^{2(2^{n-r})}_{s2^{n+1}}, \ldots, \zeta^{(\phi(s2^{r+1})-1)(2^{n-r})}_{s2^{n+1}}\}$. Letting $\mathfrak{c} = \mathfrak{p} \cap \mathcal{O}_K$, we claim that

$$\mathfrak{p} = \bigoplus_{k=0}^{2^{n-r}} \zeta^k_{s2^{n+1}} \mathfrak{c}.$$

For any $a \in \mathfrak{p}$, there exist integers z_i, w_i such that

$$\begin{aligned}
a &= \sum_{i=0}^{\phi(s2^{n+1})-1} z_i \zeta_{s2^{n+1}}^i f(\zeta_{s2^{n+1}}) + \sum_{i=0}^{\phi(s2^{n+1})-1} w_i \zeta_{s2^{n+1}} \rho \\
&= \sum_{k=0}^{2^{n-r}-1} \zeta_{s2^{n+1}}^k \sum_{j=0}^{\phi(s2^{r+1})-1} \left(z_{k+j2^{n-r}} \zeta_{s2^{n+1}}^{j2^{n-r}} f(\zeta_{s2^{n-r}}) + w_{k+j2^{n-r}} \zeta_{s2^{n+1}}^{j2^{n-r}} \rho \right) \\
&= \sum_{k=0}^{2^{n-r}-1} \zeta_{s2^{n+1}}^k \left(\left(\sum_{j=0}^{\phi(s2^{r+1})-1} z_{k+j2^{n-r}} \zeta_{s2^{n+1}}^{j2^{n-r}} \right) f(\zeta_{s2^{n+1}}) \right. \\
&\left. + \left(\sum_{j=0}^{\phi(s2^{r+1}-1} w_{k+j2^{n-r}} \zeta_{s2^{n+1}}^{j2^{n-r}} \right) \rho \right),
\end{aligned}$$

which proves our claim. Now, for any $x_k \in \mathfrak{c}, 0 \leq k \leq 2^{n-r}-1$, let $x = \sum_{k=0}^{2^{n-r}-1} x_k \zeta_{s2^{n+1}}^k \in \mathfrak{p}$. Then the quadratic form induced by the ideal lattice $\mathfrak{p}$ is given by

$$\begin{aligned}
\mathrm{Trace}_{L/\mathbb{Q}}(x\overline{x}) &= \mathrm{Trace}_{L/\mathbb{Q}} \left(\sum_{k,l=0}^{2^{n-r}-1} x_k \overline{x_l} \zeta_{s2^{n+1}}^{k-l} \right) \\
&= \sum_{i=0:\gcd(i,s)=\gcd(i,2)=1}^{s2^{n+1}-1} \sum_{k,l=0}^{2^{n-r}-1} \sigma_i \left(x_k \overline{x_l} \zeta_{s2^{n+1}}^{k-l} \right) \\
&= \sum_{i=0:\gcd(i,s)=\gcd(i,2)=1}^{s2^{r+1}-1} \sum_{j=0}^{2^{n-r}-1} \sum_{k,l=0}^{2^{n-r}-1} \sigma_{i+js2^{r+1}}(x_k \overline{x_l}) \zeta_{s2^{n+1}}^{(i+js2^{r+1})(k-l)} \\
&= \sum_{i=0:\gcd(i,s)=\gcd(i,2)=1}^{s2^{r+1}-1} \sum_{j=0}^{2^{n-r}-1} \sum_{k,l=0}^{2^{n-r}-1} \sigma_i(x_k \overline{x_l}) \zeta_{s2^{n+1}}^{(i+js2^{r+1})(k-l)},
\end{aligned}$$

but note that we have

$$\sum_{j=0}^{2^{n-r}-1} \zeta_{s2^{n+1}}^{(i+js2^{r+1})(k-l)} = \sum_{j=0}^{2^{n-r}-1} \zeta_{s2^{n+1}}^{i(k-l)} \zeta_{2^{r+1}}^{j(k-l)} = \begin{cases} 2^{n-r} & \text{if } k=l, \\ 0 & \text{otherwise.} \end{cases}$$

Hence

$$\begin{aligned}
\mathrm{Trace}_{L/\mathbb{Q}}(x\overline{x}) &= 2^{n-r} \sum_{i=0:\gcd(i,s)=\gcd(i,2)=1}^{s2^{r+1}-1} \sum_{k=0}^{2^{n-r}-1} \sigma_i(x_k \overline{x_k}) \\
&= 2^{n-r} \sum_{k=0}^{2^{n-r}-1} \mathrm{Trace}_{K/\mathbb{Q}}(x_k \overline{x_k}),
\end{aligned}$$

and so $\lambda_1(\mathfrak{p}) = \lambda_1(\mathfrak{c})$, as required. The algorithm below summarises how to find the shortest nonzero vector in a prime ideal lattice $\mathfrak{p}$. The most time-consuming step in the algorithm below is Step 2, and all other steps may be performed in $\text{poly}(\phi(s2^{n+1}), \log_2 \rho)$ time. □

Algorithm 1: SVP algorithm for prime ideal lattices of $\mathbb{Z}[\zeta_{s2^{n+1}}]$

input : A prime ideal $\mathfrak{p} = \langle \rho, f(\zeta_{s2^{n+1}}) \rangle$ in $\mathbb{Z}[\zeta_{s2^{n+1}}]$, where ρ is odd and $\gcd(\rho, s) = 1$.

output: A shortest vector in the corresponding prime ideal lattice.

1 Compute the ideal $\mathfrak{c}$ generated by ρ and $f(\zeta_{s2^{n+1}})$ in $\mathcal{O}_K$ where $K = \mathbb{Q}(\zeta_{s2^{n+1}}^{2^{n-r}})$.
2 Find a shortest vector v in the $\phi(s2^{r+1})$-dimensional lattice $\mathfrak{c}$.
3 Output v.

4.2 The Cyclotomic Field $L = \mathbb{Q}(\zeta_{sp^{n+1}})$

The following theorem is a generalisation of Theorem 2 in [27].

Theorem 8. *Let s, p, q be positive integers such that p is an odd prime, q is a prime power and $\gcd(s, p) = \gcd(q, p) = 1$. Suppose $q^{\phi(s)} \equiv a \mod p$, for some integer $\gcd(a, p) = 1$ and set $q^{\phi(s)} = mp^A + a$ for some integer m such that $\gcd(m, p) = 1$ and some integer $A \geq 0$. Then for any $n \geq A - 1$ and any irreducible factor $f(x)$ of the cyclotomic polynomial $\Phi_{p^A s}(x)$ over $\mathbb{F}_q$, $f(x^{n-A+1})$ is also irreducible. Moreover, all the irreducible factors of $\Phi_{p^{n+1}s}(x)$ are obtained in this way.*

Proof. See Appendix A. □

Theorem 9. *For any prime ideal $\mathfrak{p} = \langle \rho, f(\zeta_{sp^{n+1}}) \rangle$ where ρ is a positive rational prime, $\gcd(\rho, s) = \gcd(\rho, p) = 1$ and irreducible polynomial $f(x)$ of the cyclotomic polynomial $\Phi_{sp^{n+1}}(x)$ in $\mathbb{F}_\rho[x]$, assume that $\rho^{\phi(s)} \equiv a \mod p$ for some $\gcd(a, p) = 1$ and set $\rho^{\phi(s)} = mp^A + a$ for some positive integer m such that $\gcd(m, p) = 1$ and some integer $A \geq 1$ and let $r = \min\{A - 1, n\}$. Then, given an oracle that can solve SVP for $\phi(sp^{r+1})$-dimensional lattices, a shortest nonzero vector in $\mathfrak{p}$ can be found in $\text{poly}(\phi(sp^{n+1}), \log_2 \rho)$ time with the canonical embedding.*

Proof. We assume that $n \geq A$ otherwise the theorem is vacuously true. Let

$$G = \{\sigma_i, 1 \leq i \leq sp^{n+1} - 1 : \gcd(i, p) = \gcd(i, s) = 1\}$$

denote the Galois group of L over $\mathbb{Q}$, where

$$\sigma_i : \mathbb{Q}(\zeta_{sp^{n+1}}) \to \mathbb{Q}(\zeta_{sp^{n+1}}),$$
$$\sigma_i(\zeta_{sp^{n+1}}^k) = \zeta_{sp^{n+1}}^{ki}.$$

By Theorem 8, for any factor $f(x)$ of $\Phi_{sp^{n+1}}(x)$ that is irreducible in $\mathbb{F}_\rho[x]$, there exists a polynomial $g(x)$ that is a factor of $\Phi_{sp^{r+1}}(x)$ that is irreducible over $\mathbb{F}_\rho[x]$ such that $f(x) = g\left(x^{p^{n-r}}\right)$. Then the prime ideal $\mathfrak{p}$ can be represented by

$$\langle \rho, f(\zeta_{sp^{n+1}}) \rangle = \langle \rho, g(\zeta_{sp^{r+1}}) \rangle.$$

For any $1 \leq k \leq p^{n-r-1}$, the map $\sigma_{ksp^{r+1}+1}$ fixes $\zeta_{sp^{n+1}}^{lp^{n-r}}$ for any integer $0 \leq l < sp^{r+1}$. Moreover, since $\gcd(ksp^{r+1}+1, p) = \gcd(ksp^{r+1}, s) = 1$, each subset H_k of G generated by $\sigma_{ksp^{r+1}+1}$ forms a cyclic group, and so the set $H = H_1 \times H_2 \times \cdots \times H_{p^{n-r-1}}$ forms a subgroup of the decompositiong group of $\mathfrak{p}$, since both ρ and $f(\zeta_{sp^{n+1}}) = g\left(\zeta_{sp^{n+1}}^{p^{n-r}}\right)$ are fixed by each $\sigma_i \in H$. Then $K = \mathbb{Q}(\zeta_{sp^{n+1}}^{n-r})$ must be the fixed field of the group H, as for all $i \in \left(\mathbb{Z}/sp^{n+1}\mathbb{Z}\right)^\times$,

$$\sigma_i(\zeta_{sp^{n+1}}^{p^{n-r}}) = \zeta_{sp^{n+1}}^{p^{n-r}} \iff i \equiv 1 \mod sp^{r+1}.$$

Note that $\mathcal{O}_K$ has the $\mathbb{Z}$-basis $\{1, \zeta_{sp^{n+1}}^{p^{n-r}}, \zeta_{sp^{n+1}}^{2p^{n-r}}, \ldots, \zeta_{sp^{n+1}}^{(\phi(sp^{r+1})-1)p^{n-r}}\}$. Letting $\mathfrak{c} = \mathfrak{p} \cap \mathcal{O}_K$, we claim that

$$\mathfrak{p} = \bigoplus_{k=0}^{p^{n-r}-1} \zeta_{sp^{n+1}}^k \mathfrak{c}.$$

For any $a \in \mathfrak{p}$, there exist integers z_i, w_i such that

$$\begin{aligned}
a &= \sum_{i=0}^{\phi(sp^{n+1})-1} z_i \zeta_{sp^{n+1}}^i f(\zeta_{sp^{n+1}}) + \sum_{i=0}^{\phi(sp^{n+1})-1} w_i \zeta_{sp^{n+1}} \rho \\
&= \sum_{k=0}^{p^{n-r}-1} \zeta_{sp^{n+1}}^k \sum_{j=0}^{\phi(sp^{r+1})-1} \left(z_{k+jp^{n-r}} \zeta_{sp^{n+1}}^{jp^{n-r}} f(\zeta_{sp^{n-r}}) + w_{k+jp^{n-r}} \zeta_{sp^{n+1}}^{jp^{n-r}} \rho \right) \\
&= \sum_{k=0}^{p^{n-r}-1} \zeta_{sp^{n+1}}^k \left(\left(\sum_{j=0}^{\phi(sp^{r+1})-1} z_{k+jp^{n-r}} \zeta_{sp^{n+1}}^{jp^{n-r}} \right) f(\zeta_{sp^{n+1}}) \right. \\
&\quad \left. + \left(\sum_{j=0}^{\phi(sp^{r+1})-1} w_{k+jp^{n-r}} \zeta_{sp^{n+1}}^{jp^{n-r}} \right) \rho \right),
\end{aligned}$$

which proves our claim. Now, for any $x_k \in \mathfrak{c}, 0 \leq k \leq p^{n-r}-1$, let $x = \sum_{k=0}^{p^{n-r}-1} x_k \zeta_{sp^{n+1}}^k \in \mathfrak{p}$. Then the quadratic form induced by the ideal lattice

$\mathfrak{p}$ is given by

$$\begin{aligned}
\mathrm{Trace}_{L/\mathbb{Q}}(x\overline{x}) &= \mathrm{Trace}_{L/\mathbb{Q}}\left(\sum_{k,l=0}^{p^{n-r}-1} x_k\overline{x_l}\zeta_{sp^{n+1}}^{k-l}\right) \\
&= \sum_{i=0:\gcd(i,s)=\gcd(i,p)=1}^{sp^{n+1}-1} \sum_{k,l=0}^{p^{n-r}-1} \sigma_i(x_k\overline{x_l}\zeta_{sp^{n+1}}^{k-l}) \\
&= \sum_{i=0:\gcd(i,s)=\gcd(i,p)=1}^{sp^{r+1}-1} \sum_{j=0}^{p^{n-r}-1} \sum_{k,l=0}^{p^{n-r}-1} \sigma_{i+jsp^{r+1}}(x_k\overline{x_l})\zeta_{sp^{n+1}}^{(i+jsp^{r+1})(k-l)} \\
&= \sum_{i=0:\gcd(i,s)=\gcd(i,p)=1}^{sp^{r+1}-1} \sum_{j=0}^{p^{n-r}-1} \sum_{k,l=0}^{p^{n-r}-1} \sigma_i(x_k\overline{x_l})\zeta_{sp^{n+1}}^{(i+jsp^{r+1})(k-l)},
\end{aligned}$$

but note that we have

$$\sum_{j=0}^{p^{n-r}-1} \zeta_{sp^{n+1}}^{(i+jsp^{r+1})(k-l)} = \sum_{j=0}^{p^{n-r}-1} \zeta_{sp^{n+1}}^{i(k-l)}\zeta_{p^{r+1}}^{j(k-l)} = \begin{cases} p^{n-r} & \text{if } k=l, \\ 0 & \text{otherwise.} \end{cases}$$

Hence

$$\begin{aligned}
\mathrm{Trace}_{L/\mathbb{Q}}(x\overline{x}) &= p^{n-r} \sum_{i=0:\gcd(i,s)=\gcd(i,p)=1}^{sp^{r+1}-1} \sum_{k=0}^{p^{n-r}-1} \sigma_i(x_k\overline{x_k}) \\
&= p^{n-r} \sum_{k=0}^{p^{n-r}-1} \mathrm{Trace}_{K/\mathbb{Q}}(x_k\overline{x_k}),
\end{aligned}$$

and so $\lambda_1(\mathfrak{p}) = \lambda_1(\mathfrak{c})$, as required. The algorithm below summarises how to find the shortest nonzero vector in a prime ideal lattice $\mathfrak{p}$. The most time-consuming step in the algorithm below is Step 2, and all other steps may be performed in $\mathrm{poly}(\phi(sp^{n+1}), \log_2 \rho)$ time. □

Algorithm 2: SVP algorithm for prime ideal lattices of $\mathbb{Z}[\zeta_{sp^{n+1}}]$

input : A prime ideal $\mathfrak{p} = \langle \rho, f(\zeta_{sp^{n+1}})\rangle$ in $\mathbb{Z}[\zeta_{sp^{n+1}}]$, where $\gcd(p,\rho) = \gcd(\rho, s) = 1$ and $\rho^{\phi(s)} \equiv \pm 1 \mod p$.

output: A shortest vector in the corresponding prime ideal lattice.

1 Compute the ideal $\mathfrak{c}$ generated by ρ and $f(\zeta_{sp^{n+1}})$ in $\mathcal{O}_K$ where $K = \mathbb{Q}(\zeta_{sp^{n+1}}^{p^{n-r}})$.

2 Find a shortest vector v in the $\phi(sp^{r+1})$-dimensional lattice $\mathfrak{c}$.

3 Output v.

4.3 Some Special Prime Ideals of Cyclotomic Rings

Theorem 10. *Let $L = \mathbb{Q}(\zeta_{s2^{n+1}})$ be a cyclotomic field for some positive odd integer $s \geq 3$ and some integer $n \geq 0$. Let $\mathfrak{p}$ denote a prime ideal lying over a positive rational odd prime ρ such that $\rho^{\phi(s)} \equiv 3 \mod 4$. Then, given an oracle that can solve SVP for $\phi(s)$-dimensional lattices, a shortest nonzero vector in $\mathfrak{p}$ can be found in poly$(\phi(s2^{n+1}), \log_2 \rho)$ time with the canonical embedding.*

Proof. For some integer $N > 1$, we must have $\rho^{\phi(s)} \equiv 2l+1 \mod 2^N$, and so for some integer k, we have $\rho^{\phi(s)} = 1+2l+2^N k = 1+2(2^{N-1}k+l)$. Since $2^{N-1}k+l$ is an odd integer and N is taken totally arbitrarily, the claim holds by Theorem 7. □

Theorem 11. *Let $L = \mathbb{Q}(\zeta_{sp^{n+1}})$ be a cyclotomic field for some positive integer $s \neq 1$ such that $\gcd(s, p) = 1$, an odd prime p and some integer $n \geq 0$. Let $\mathfrak{p}$ denote a prime ideal lying over a positive rational odd prime ρ such that $\rho^{\phi(s)} = lp+a$ for some integers l, a, $\gcd(l, p) = \gcd(a, p) = 1$. Then, given an oracle that can solve SVP for $(p-1)\phi(s)$-dimensional lattices, a shortest nonzero vector in $\mathfrak{p}$ can be found in poly$(\phi(sp^{n+1}), \log_2 \rho)$ time with the canonical embedding.*

Proof. For some integer $N > 1$, we must have $\rho^{\phi(s)} equiv lp + a \mod p^N$, and so for some integer k, we have $\rho^{\phi(s)} = ma + pl + p^N k = a + p(p^{N-1}k + l)$. Since $\gcd(p^{N-1}k + l, p) = 1$ and N is taken totally arbitrarily, the claim holds by Theorem 9. □

5 General Ideals of Cyclotomic Rings

5.1 The Cyclotomic Field $L = \mathbb{Q}(\zeta_{s2^{n+1}})$

As before, we set s to be some odd integer greater than or equal to 3.

Theorem 12. *Let $\mathcal{I}$ be a nonzero ideal of $\mathbb{Z}[\zeta_{s2^{n+1}}]$ with prime factorisation*

$$\mathcal{I} = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_t,$$

where $\mathfrak{p}_i = (f_i(\zeta_{s2^{n+1}}), \rho_i)$ for rational primes ρ_i are (not necessarily distinct) prime ideals. If ρ_i is odd, write $\rho_i^{\phi(s)} = m_i 2^{A_i} + 1$, for some integer m_i such that $\gcd(m_i, 2) = 1$ and let $r = \max\{r_i\}$, where

$$r_i = \begin{cases} \min\{A_i - 1, n\}, & \text{if } \rho \equiv 1 \mod 2, \\ n & \text{if} \rho = 2. \end{cases}$$

Then SVP in the lattice generated by $\mathcal{I}$ can be solved via solving SVP in a $\phi(s2^{r+1})$-dimensional lattice.

Proof. If $r = n$ the theorem vacuously holds, so we assume otherwise. We may assume WLOG that $r = r_1$. Following the notation of Theorem 7, we denote by

$$G = \{\sigma_i : 1 \leq i \leq s2^{n+1} - 1, \gcd(i, 2) = \gcd(i, s) = 1\}$$

the Galois group of L, and consider the subgroup $H = H_1 \times H_2 \times \cdots \times H_{2^{n-r-1}}$, where H_k is the cyclic group generated by $\langle \sigma_{ks2^{r+1}+1} \rangle$, which is a subgroup of the decomposition group of every $\mathfrak{p}_i$, since $\sigma_{ks2^{r+1}+1}(\rho_i) = \rho_i$, $\sigma_{ks2^{r+1}+1}(f_i(\zeta_{s2^{n+1}})) = \sigma_{ks2^{r+1}+1}(g_i(\zeta_{s2^{r+1}})) = g_i(\zeta_{s2^{r+1}}) = f_i(\zeta_{s2^{n+1}})$, where $g_i(x)$ is an irreducible factor of $\Phi_{s2^{A_i}}(x)$. As shown in Theorem 7, the fixed field of H is $K = \mathbb{Q}(\zeta_{s2^{n+1}}^{2^{n-r}})$, which has ring of integers $\mathcal{O}_K = \mathbb{Z}[\zeta_{s2^{n+1}}^{2^{n-r}}]$. Let $\mathfrak{c} = \mathcal{I} \cap \mathcal{O}_K$. We claim that for any $a \in \mathcal{I}$, there exist $a^{(k)} \in \mathfrak{c}$ for $0 \leq k \leq 2^{n-r} - 1$ such that

$$a = \sum_{k=0}^{2^{n-r}-1} \zeta_{s2^{n+1}}^{k} a^{(k)}.$$

We prove the claim via induction. When $t = 1$, the claim holds by Theorem 7, so we assume the claim holds for $t - 1$. Letting $\overline{\mathcal{I}} = \mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_{t-1}$, we have $\mathcal{I} = \mathfrak{p}_t \mathcal{I}$. It suffices to show that for any xy, $x \in \overline{\mathcal{I}}, y \in \mathfrak{p}_t$, there exist $b^{(k)} \in \mathcal{I} \cap \mathcal{O}_K$ for $0 \leq k \leq 2^{n-r} - 1$ such that $xy = \sum_{k=0}^{2^{n-r}-1} \zeta_{s2^{n+1}}^{k} b^{(k)}$. By the induction assumption, there exist $x^{(i)} \in \overline{\mathcal{I}} \cap \mathcal{O}_K$, $y^{(j)} \in \mathfrak{p}_t \cap \mathcal{O}_K$, $0 \leq i, j \leq 2^{n-r} - 1$ such that $x = \sum_{i=0}^{2^{n-r}-1} \zeta_{s2^{n+1}}^{i} x^{(i)}$ and $y = \sum_{j=0}^{2^{n-r}-1} \zeta_{s2^{n+1}}^{j} y^{(j)}$. Hence, we have

$$\begin{aligned}
xy &= \sum_{i,j=0}^{2^{n-r}-1} \zeta_{s2^{n+1}}^{i+j} x^{(i)} y^{(i)} \\
&= \sum_{k=0}^{2^{n-r}-1} \zeta_{s2^{n+1}}^{k} \sum_{i+j=k} x^{(i)} y^{(j)} + \sum_{k=2^{n-r}}^{2\cdot 2^{n-r}-2} \zeta_{s2^{n+1}}^{k} \\
&= \sum_{k=0}^{2^{n-r}-1} \zeta_{s2^{n+1}}^{k} \sum_{i+j=k} x^{(i)} y^{(j)} + \sum_{k=0}^{2^{n-r}-2} \zeta_{s2^{n+1}}^{k} \sum_{i+j=k+2^{n-r}} \zeta_{s2^{n+1}}^{2^{n-r}} x^{(i)} y^{(j)} \\
&= \sum_{k=0}^{2^{n-r}-2} \zeta_{s2^{n+1}}^{k} \left(\sum_{i+j=k} x^{(i)} y^{(j)} + \sum_{i+j=k+2^{n-r}} \zeta_{s2^{n+1}}^{2^{n-r}} x^{(i)} y^{(j)} \right) \\
&+ \zeta_{s2^{n+1}}^{2^{n-r}-1} \sum_{i+j=2^{n-r}-1} x^{(i)} y^{(j)}.
\end{aligned}$$

By letting

$$b^{(k)} = \sum_{i+j=k} x^{(i)} y^{(j)} + \sum_{i+j=k+2^{n-r}} \zeta_{s2^{n+1}}^{2^{n-r}} x^{(i)} y^{(j)}$$

for $0 \leq k \leq 2^{n-r} - 2$ and

$$b^{(2^{n-r}-1)} = \sum_{i+j=2^{n-r}-1} x^{(i)} y^{(j)},$$

we have proven our claim. As in Theorem 7, we have $\lambda_1(\mathcal{I}) = \lambda_1(\mathfrak{c})$, as required. □

The following algorithm may be used to compute the shortest vector in $\mathcal{I}$.

Algorithm 3: SVP algorithm for general ideal lattices of $\mathbb{Z}[\zeta_{s2^{n+1}}]$

input : An ideal $\mathcal{I}$.
output: A shortest vector in the corresponding ideal lattice.

for $\overline{r} = 1$ **to** n **do**
  Compute a basis $(b^{(i)})_{0 \le i < \phi(s2^{\overline{r}+1})}$ of the ideal lattice $\mathfrak{c} = \mathcal{I} \cap \mathcal{O}_K$ where $K = \mathbb{Q}(\zeta_{s2^{n+1}}^{2^{n-\overline{r}}})$.
  if $(\zeta_{s2^{n+1}}^{j} b^{(i)})_{0 \le i < \phi(s2^{\overline{r}+1}), 0 \le j \le 2^{n-\overline{r}}}$ *is exactly a basis of the ideal lattice* $\mathcal{I}$ **then**
    Find a shortest vector v in the $\phi(s2^{\overline{r}+1})$-dimensional lattice $\mathfrak{c}$.
    Output v.

5.2 The Cyclotomic Field $L = \mathbb{Q}(\zeta_{sp^{n+1}})$

As before, p is a positive, odd prime and s is a positive integer such that $\gcd(s, p) = 1$.

Theorem 13. *Let $\mathcal{I}$ be a nonzero ideal of $\mathbb{Z}[\zeta_{sp^{n+1}}]$ with prime factorisation*

$$\mathcal{I} = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_t,$$

where $\mathfrak{p}_i = (f_i(\zeta_{sp^{n+1}}), \rho_i)$ for rational primes ρ_i are (not necessarily distinct) prime ideals. If $\rho_i^{\phi(s)} \equiv a \mod p$ for some $\gcd(p, a) = 1$, write $\rho_i^{\phi(s)} = m_i p^{A_i} + 1$ and let $r = \max\{r_i\}$, where

$$r_i = \begin{cases} \min\{A_i - 1, n\}, & \text{if } \rho_i^{\phi(s)} \equiv a \mod p, \\ n & \text{if } \rho = p. \end{cases}$$

Then SVP in the lattice generated by $\mathcal{I}$ can be solved via solving SVP in a $\phi(sp^{r+1})$-dimensional lattice.

Proof. If $r = n$ the theorem vacuously holds, so we assume otherwise. We may assume WLOG that $r = r_1$. Following the notation of Theorem 9, we denote by

$$G = \{\sigma_i : 1 \le i \le sp^{n+1} - 1, \gcd(i, p) = \gcd(i, s) = 1\}$$

the Galois group of L, and consider the subgroup $H = H_1 \times H_2 \times \dots \times H_{p^{n-r-1}}$, where H_k is the cyclic group generated by $\langle \sigma_{ksp^{r+1}+1} \rangle$, which is a subgroup of the decomposition group of every $\mathfrak{p}_i$, since $\sigma_{ksp^{r+1}+1}(\rho_i) = \rho_i$, $\sigma_{ksp^{r+1}+1}(f_i(\zeta_{sp^{n+1}})) = \sigma_{ksp^{r+1}+1}(g_i(\zeta_{sp^{r+1}})) = g_i(\zeta_{sp^{r+1}}) = f_i(\zeta_{sp^{n+1}})$, where $g_i(x)$ is an irreducible factor of $\Phi_{sp^{A_i}}(x)$. As shown in Theorem 9, the fixed field of H is $K = \mathbb{Q}(\zeta_{sp^{n+1}}^{p^{n-r}})$, which has ring of integers $\mathcal{O}_K = \mathbb{Z}[\zeta_{sp^{n+1}}^{p^{n-r}}]$. Let $\mathfrak{c} = \mathcal{I} \cap \mathcal{O}_K$. We claim that for any $a \in \mathcal{I}$, there exist $a^{(k)} \in \mathfrak{c}$ for $0 \le k \le p^{n-r} - 1$ such that

$$a = \sum_{k=0}^{p^{n-r}-1} \zeta_{sp^{n+1}}^{k} a^{(k)}.$$

We prove the claim via induction. When $t = 1$, the claim holds by Theorem 9, so we assume the claim holds for $t-1$. Letting $\overline{\mathcal{I}} = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_{t-1}$, we have $\mathcal{I} = \mathfrak{p}_t\mathcal{I}$. It suffices to show that for any xy, $x \in \overline{\mathcal{I}}, y \in \mathfrak{p}_t$, there exist $b^{(k)} \in \mathcal{I} \cap \mathcal{O}_K$ for $0 \leq k \leq p^{n-r} - 1$ such that $xy = \sum_{k=0}^{p^{n-r}-1} \zeta_{sp^{n+1}}^k b^{(k)}$. By the induction assumption, there exist $x^{(i)} \in \overline{\mathcal{I}} \cap \mathcal{O}_K$, $y^{(j)} \in \mathfrak{p}_t \cap \mathcal{O}_K$, $0 \leq i, j \leq p^{n-r} - 1$ such that $x = \sum_{i=0}^{p^{n-r}-1} \zeta_{sp^{n+1}}^i x^{(i)}$ and $y = \sum_{j=0}^{p^{n-r}-1} \zeta_{sp^{n+1}}^j y^{(j)}$. Hence, we have

$$\begin{aligned}
xy &= \sum_{i,j=0}^{p^{n-r}-1} \zeta_{sp^{n+1}}^{i+j} x^{(i)} y^{(i)} \\
&= \sum_{k=0}^{p^{n-r}-1} \zeta_{sp^{n+1}}^k \sum_{i+j=k} x^{(i)} y^{(j)} + \sum_{k=p^{n-r}}^{2p^{n-r}-2} \zeta_{sp^{n+1}}^k \\
&= \sum_{k=0}^{p^{n-r}-1} \zeta_{sp^{n+1}}^k \sum_{i+j=k} x^{(i)} y^{(j)} + \sum_{k=0}^{p^{n-r}-2} \zeta_{sp^{n+1}}^k \sum_{i+j=k+p^{n-r}} \zeta_{sp^{n+1}}^{p^{n-r}} x^{(i)} y^{(j)} \\
&= \sum_{k=0}^{p^{n-r}-2} \zeta_{sp^{n+1}}^k \left(\sum_{i+j=k} x^{(i)} y^{(j)} + \sum_{i+j=k+p^{n-r}} \zeta_{sp^{n+1}}^{p^{n-r}} x^{(i)} y^{(j)} \right) \\
&+ \zeta_{sp^{n+1}}^{p^{n-r}-1} \sum_{i+j=p^{n-r}-1} x^{(i)} y^{(j)}.
\end{aligned}$$

By letting

$$b^{(k)} = \sum_{i+j=k} x^{(i)} y^{(j)} + \sum_{i+j=k+p^{n-r}} \zeta_{sp^{n+1}}^{p^{n-r}} x^{(i)} y^{(j)}$$

for $0 \leq k \leq p^{n-r} - 2$ and

$$b^{(p^{n-r}-1)} = \sum_{i+j=p^{n-r}-1} x^{(i)} y^{(j)},$$

we have proven our claim. As in Theorem 9, we have $\lambda_1(\mathcal{I}) = \lambda_1(\mathfrak{c})$, as required. □

The following algorithm may be used to compute the shortest vector in $\mathcal{I}$.

6 Modules over Cyclotomic Rings

We let $L = \mathbb{Q}(\zeta_N)$ be the cyclotomic field of conductor N, where N is of the form sq^{n+1}, where q is either 2 or an odd prime and s is a positive integer, $\gcd(s, q) = 1$. Then, denoting by $\mathcal{I}_1, \dots, \mathcal{I}_d$ some ideals of $\mathbb{Z}[\zeta_N]$ and some vectors $\mathbf{b}_1, \dots, \mathbf{b}_d \in L^D$ for some $d \leq D$, we define a module over $\mathcal{O}_L$

$$M = \bigoplus_{i=1}^{d} \mathcal{I}_i \mathbf{b}_i.$$

Algorithm 4: SVP algorithm for general ideal lattices of $\mathbb{Z}[\zeta_{sp^{n+1}}]$

input : An ideal $\mathcal{I}$.
output: A shortest vector in the corresponding ideal lattice.

for $\overline{r} = 1$ **to** n **do**
  Compute a basis $(b^{(i)})_{0 \le i < \phi(sp^{\overline{r}+1})}$ of the ideal lattice $\mathfrak{c} = \mathcal{I} \cap \mathcal{O}_K$ where $K = \mathbb{Q}(\zeta_{sp^{n+1}}^{2^{n-\overline{r}}})$.
  if $(\zeta_{sp^{n+1}}^{j} b^{(i)})_{0 \le i < \phi(sp^{\overline{r}+1}), 0 \le j \le p^{n-\overline{r}}}$ *is exactly a basis of the ideal lattice* $\mathcal{I}$ **then**
    Find a shortest vector v in the $\phi(sp^{\overline{r}+1})$-dimensional lattice $\mathfrak{c}$.
    Output v.

By the structure theorem for finitely generated modules over Dedekind domains, we must have

$$M \cong \bigoplus_{i=1}^{d} \mathcal{J}_i,$$

for some rank one projective $\mathcal{O}_L$-modules $\mathcal{J}_i$, i.e. fractional ideals. By the definition of a fractional ideal, for every $\mathcal{J}_i$ there exists an $x_i \in \mathbb{Q}$ such that $x_i \mathcal{J}_i = \mathcal{J}_i' \subseteq \mathcal{O}_L$, and so

$$\mathcal{J}_i = \frac{1}{x_i} \prod_{j=1}^{g_i} \mathfrak{p}_j^{(i)},$$

where $\mathfrak{p}_j^{(i)}$ are prime ideals lying over some rational prime $\rho_j^{(i)}$, and assume we have $\gcd(\rho_j^{(i)}, N) = 1$. Now, we let

$$\rho_j^{(i)^{\phi(s)}} = \begin{cases} m2^{A_j^{(i)}} + 1 & \text{if } N = s2^{n+1}, m \text{ odd integer,} \\ mp^{A_j^{(i)}} + a & \text{if } N = sp^{n+1} \text{ for odd prime } p, \\ & \text{and } \rho_j^{(i)^{\phi(s)}} \equiv a \bmod p, \gcd(m,p) = \gcd(a,p) = 1. \end{cases}$$

Define the value $r_j^{(i)} = \min\{A_j^{(i)} - 1, n\}$. We let $r = \max_{i,j}\{r_j^{(i)}\}$ and $\mathfrak{c}_i = (x_i \mathcal{J}_i) \cap K$ where $K = \mathbb{Q}(\zeta_{sq^{r+1}})$. As we have already shown, every $\mathcal{J}_i$ may be represented as

$$x_i \mathcal{J}_i = \bigoplus_{k=0}^{q^{n-r}-1} \mathfrak{c}_i \zeta_{sq^{n+1}}^{k},$$

and so we have

$$M \cong \bigoplus_{i=1}^{d} \frac{1}{x_i} \bigoplus_{k=0}^{q^{n-r}-1} \mathfrak{c}_i \zeta_{sq^{n+1}}^{k} = \bigoplus_{k=0}^{q^{n-r}-1} \left(\bigoplus_{i=1}^{d} \frac{1}{x_i} \mathfrak{c}_i \right) \zeta_{sq^{n+1}}^{k}.$$

Denoting by f^{-1} the inverse of the isomorphism f that maps M to $\bigoplus_{i=1}^{d} \mathcal{J}_i$, we may apply f^{-1} to $\bigoplus_{i=1}^{d} \frac{1}{x_i}\mathfrak{c}_i$, from which we obtain a rank d module M' over $\mathcal{O}_K$, where K is the field that is fixed by the decomposition group of every $\mathfrak{c}_i$, and so

$$M \cong \bigoplus_{k=0}^{q^{n-r}-1} M'\zeta_{sq^{n+1}}^{k}.$$

Moreover, as we have already shown the direct sum on the right hand side can be treated as a sum of orthogonal components under the canonical embedding. Therefore, the minimum lattice vector of M under the canonical embedding is equivalent to the minimal lattice vector of M' under the canonical embedding, as an isomorphism between the modules implies they span the same set of vectors.

7 SVP Average-Case Hardness

The average case hardness of SVP over prime ideals depends on the distribution chosen which defines the ideal. We consider the following distributions.
Distribution 1: We uniformly randomly select a prime ideal lying over a rational prime ρ, where we take ρ uniformly randomly from the set

$$\{\rho < M : \rho \text{ is prime}\},$$

for some large fixed integer M.

- When $L = \mathbb{Q}(\zeta_{s2^{n+1}})$, we assume that security is compromised when $\rho^{\phi(s)} \equiv 2l + 1 \mod 2^N$, that is, we have an oracle that can solve SVP for $\phi(s)$-dimensional lattices. Now, suppose $s = \prod_{i=1}^{d} p_i^{k_i}$, for some positive integers p_i, k_i, d where p_i are distinct primes, and assume without loss of generality that $p_i \leq p_j$ for all $i \leq j$. Then for some $g \leq d$, we have $p_1, \ldots, p_g \leq M$, and so the probability of s being coprime to ρ is given by

$$1 - \frac{g}{\pi(M) - 1} \approx 1 - \frac{g}{\pi(M)} \geq 1 - \frac{g \log(M)}{MC(M)},$$

  where π denotes the prime counting function and $C(M) \leq 1$ is a positive constant that increases with the size of M [31]. We assume that we have a ρ that satisfies $\gcd(s, \rho) = 1$. By Dirichlet's theorem on arithmetic progressions, there are infinitely many primes of the form $\rho \equiv 3 \mod 4$, and approximately half of all primes take this form, so the probability of choosing an easily solvable prime ideal lattice is approximately $1/2$.
- When $L = \mathbb{Q}(\zeta_{sp^{n+1}})$ for some odd prime p, we assume that security is compromised when $\rho^{\phi(s)} \equiv lp + a \mod p^N$ for some positive integer N, that is, we have an oracle that can solve SVP for $(p-1)\phi(s)$-dimensional lattices. Similarly to before, if $s = \prod_{i=1}^{d} p_i^{k_i}$ for some positive integers p_i, k_i, d where

p_i are distinct primes not equal to p such that $p_i \leq p_j$ for all $i \leq j$, if p_g is the largest prime such that $p_g < M$, the probability that s is coprime to ρ is

$$1 - \frac{g}{\pi(M) - 1} \approx 1 - \frac{g}{\pi(M)} \geq 1 - \frac{g \log(M)}{MC(M)},$$

where π denotes the prime counting function and $C(M) \leq 1$ is a positive constant that increases with the size of M. We assume that ρ satisfies $\gcd(s, \rho) = 1$. For all primes ρ, we may find a prime of the form $l\rho + a$ where $\gcd(l, p) = \gcd(a, p) = 1$ by setting $l = \prod_{q < \rho:\ q \text{ prime}, \gcd(a,q)=1} q$. By Dirichlet's theorem on arithmetic progressions, there are infinitely many primes of this form, and so the approximate probability of picking an easily solvable prime ideal lattice is $(p-1)/p$.

Distribution 2: We fix a large M, and select a prime ideal uniformly randomly from the set

$$\{\mathfrak{p} \text{ a prime ideal} : \rho \in \mathfrak{p}, \ \ \rho \text{ is prime}, \rho < M\}.$$

- When $L = \mathbb{Q}(\zeta_{s2^{n+1}})$ for some odd integer $s \geq 3$, we assume that we have an oracle to solve SVP over $\phi(s)$-dimensional lattices, and so the "easy" SVP cases occur when our prime ideal lies over a prime ρ where $\rho^{\phi(s)} = 2l + 1$ for some odd l. However, we can't use Lemma 1 to attain a better lower bound than 1 on the number of ideals above ρ, and as such the probability of picking an easily solvable ideal is at least $\frac{1}{1+2^n\phi(s)}$.
- When $L = \mathbb{Q}(\zeta_{sp^{n+1}})$, the number of prime ideals lying over ρ is greater than or equal to $\frac{\phi(sp)}{\phi(s)} = p-1$, and since there are $p-1$ easy cases, the probability of picking an easily solvable ideal is at least $\frac{1}{1+\frac{p^n}{p-1}\phi(s)}$.

Distribution 3: We fix a large M, and select a prime ideal uniformly randomly from the set

$$\{\mathfrak{p} \text{ a prime ideal} : N(\mathfrak{p}) < M\}.$$

Our method of reduction to a 2^r-dimensional sublattice $\mathfrak{c}$ only works when p does not split completely in L, or equivalently, when $N(\mathfrak{p}) = \rho$. By Chebotarev's density theorem, the number of primes less than M that split completely in $L = \mathbb{Q}(\zeta_m)$ is approximately $\frac{M}{\phi(m)\log(M)}$, and hence there are $\frac{M}{\log(M)}$ prime ideals lying above those primes for which our reduction method cannot be applied. Now, if our algorithm is to provide a reduction, we need $N(\mathfrak{p}) = \rho^f < M$ for some positive integer m, and so the prime ideal must lie over a rational prime ρ such that $\rho < \sqrt{M}$. Hence, there are at most $\sqrt{M}$ of such primes, and as such, there are at most:

- $\phi(s)2^{n-1}\sqrt{M}$ when $L = \mathbb{Q}(\zeta_{s2^{n+1}})$ for odd, positive integer $s \geq 3$,
- $\phi(s)(p-1)p^{n-1}\sqrt{M}$ when $L = \mathbb{Q}(\zeta_{sp^{n+1}})$ for odd positive integer s and odd prime p, $\gcd(s, p) = 1$.

Then, for the relevant factor $\alpha(L)\sqrt{M}$ listed above, the density of easy instances for our algorithm is at most $\frac{\alpha(L)\log(M)}{\sqrt{M}}$, which goes to zero as M tends to infinity for all considered fields.

General Ideals and Modules: For any of the distributions covered, we can make similar assertions about the density of easy cases in general ideals and modules. If the probability of choosing an easily solvable prime ideal lattice in a given distribution is P, then given a general ideal $\mathcal{I}$ that has g distinct factors, the probability that the ideal is easily solvable is P^g, since we require that all the prime ideal factors are individually easy cases. Similarly for the module case, for a module M of rank d over $\mathcal{O}_L$, we have $M \cong \bigoplus_{i=1}^{d} \mathcal{J}_i$. Then applying the previous logic over the prime decomposition of all the ideals $\mathcal{J}_i$, if $\mathcal{J}_i$ has g_i distinct prime ideal factors, then the probability of picking an easily solvable module lattice is $P^{\prod_{i=1}^{d} g_i}$.

8 Concluding Remarks

In this paper, we have successfully generalised methods pioneered by Pan et. al. in [10]. First, we showed that a solution to Hermite SVP for a general ideal lattice may be yielded by solving Hermite-SVP with a smaller factor in a subideal by exploiting the decomposition group of the ideal. Moreover, we showed that a similar argument may be made for module lattices defined over the ring of integers of a field that is Galois over $\mathbb{Q}$, and present two methods by which we may approach the module case. For ideals of cyclotomic rings, we generalised Pan et. al.'s results to construct an efficient SVP algorithm for ideals of cyclotomic rings of arbitrary conductor, and showed that there exists certain classes of ideal lattices whose structure is significantly weaker to our algorithm than others. An open problem remains to construct an efficient SVP algorithm for the case of modules over cyclotomic rings as our work did not include an explicit construction of the isomorphism mentioned in section 7.

References

1. Ajtai, M.: Generating hard instances of lattice problems (extended abstract). In: Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing - STOC. pp. 99-108 (1996).
2. Regev, O.: On lattices, learning with errors, random linear codes and cryptography. Journal of the ACP **56**(6), pp. 1-40 (2009).
3. Hoffstein, J., Pipher, J., Silverman, J.H.: A ring-based public key cryptosystem. In: Proceedings of Algorithmic Number Theory, Third International Symposium, ANTS-III, pp. 267-288 (1998).
4. Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. In: Proceedings of Advances in Cryptology - EUROCRYPT 2010. Lecture Notes in Computer Science, vol. 6110, pp. 1-23. Springer (2010).
5. Peikert, C., Regev, O., Stephens-Davidowitz, N.: Pseudorandomness of ring-LWE for any ring and modulus. In: Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017. pp. 461-473 (2017).

6. Alkim, E., Ducas, L., Pöppelmann, T., Schwabe, P.: Newhope without reconciliation. IACR Cryptography ePrint Archive 2016, 1157 (2016).
7. Bos, J.W., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Schwabe, P., Seiler, G., Stehlé, D.: CRYSTALS - kyber: A CCA-secure module lattice-based KEM. In: Proceedings of 2018 IEEE EUropean Symposium on Security and Privacy, EuroS&P 2018. pp. 353-367 (2018).
8. Fouque, P.A., Hoffstein, J., Kirchner, P., Lyubashevsky, V., Pornin, T., Prest, T., Ricosset, T., Seiler, G., Whyte, W., Zhang, Z.: Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU. In: Submission to the NIST's post-quantum cryptography standardization process (2018).
9. Micciancio, D.: Generalized compact knapsacks, cyclic lattices, and efficient oneway functions from worst-case complexity assumptions. In: Proceedings of 43rd Symposium on Foundations of Computer Science (FOCS 2002). pp. 356–365 (2002).
10. Pan, Y., Xu, J., Wadleigh, N., Cheng, Q.: On the ideal shortest vector problem over random rational primes. In: IACR-EUROCRYPT-2021 (2021). `https://eprint.iacr.org/2021/245`
11. Bernstein, D.J.: A subfield-logarithm attack against ideal lattices: Computing algebraic number theory tackles lattice-based cryptography. The cr.yp.to blog (2014), `http://blog.cr.yp.to/20140213-ideal.html`
12. Albrecht, M., Bai, S., Ducas, L.: A subfield lattice attack on overstretched NTRU assumptions. In: Proceedings of Advances in Cryptology – CRYPTO 2016. pp. 153–178 (2016).
13. Stehlé, D., Steinfeld, R.: Making NTRU as secure as worst-case problems over ideal lattices. In: Advances in Cryptology - EUROCRYPT 2011, Talinn, Estonia, ser. Lecture Notes in Computer Science, K.G. Paterson Ed., vol. 6632, pp. 27-47, Springer (2011).
14. Biasse, J., Espitau, T., Fouque, P., Gélin, A., Kirchner, P.: Computing generator in cyclotomic integer rings. In: Proceedings of Advances in Cryptology – EUROCRYPT 2017. pp. 60–88 (2017).
15. Lenstra, A.K., Lenstra, H.W., Lovász, L.: Factoring polynomials with rational coefficients. Mathematische Annalen **261**(4), pp. 515-534 (1982).
16. Kim, T., Lee, C.: Lattice reductions over Euclidean rings with applications to cryptanalysis. In: Cryptography and Coding - 16th IMA International Conference, IMACC 2017, vol. 10655, pp. 371-391, Springer (2017).
17. Napias, H.: A generalization of the LLL-algorithm over Euclidean rings or orders. In: Journal de Théorie des Nombres de Bordeaux, vol. 8, no. 2, pp. 387-396 (1996).
18. Lyu, S., Porter, C., Ling, C.: Lattice Reduction over Imaginary Quadratic Fields. In: IEEE Transactions on Signal Processing, vol. 68, pp. 6380-6393 (2020).
19. Fieker, C., Pohst, M.: On lattices over number fields. In: Algorithmic Number Theory, Second International Symposium, ANTS-II, Talence, France, vol. 1122, pp. 133-139, Springer (1996).
20. Fieker, C., Stéhle, D.: Short bases of lattices over number fields. In: Algorithmic Number Theory, 9th International Symposium, ANTS-IX, Nancy, France, vol. 6197, pp. 157-173, Springer (2010).
21. Cramer, R., Ducas, L., Peikert, C., Regev, O.: Recovering short generators of principal ideals in cyclotomic rings. In: Proceedings of Advances in Cryptology – EUROCRYPT 2016. pp. 559–585 (2016).
22. Cramer, R., Ducas, L., Wesolowski, B.: Short stickelberger class relations and application to ideal-SVP. In: Proceedings of Advances in Cryptology – EUROCRYPT 2017. pp. 324–348 (2017).

23. Schnorr, C., Euchner, M.: Lattice basis reduction: Improved practical algorithms and solving subset sum problems. In: Math. Program., vol. 66, pp. 181–199 (1994).
24. Lidl, R., Niederreiter, H.: Finite Fields, Encyclopedia of Mathematics and Its Applications, vol. 20. Cambridge University Press, 2nd edn. (1997).
25. Meyn, H.: Factorization of the cyclotomic polynomials $x^{2^n} + 1$ over finite fields. Finite Fields Appl. **2**, 439–442 (1996).
26. Wang L., Wang Q.: On explicit factors of cyclotomic polynomials over finite fields. In: Des. Codes Cryptogr. **63**, pp. 87–104 (2011).
27. Wu, H., Zhu, L., Rongquan, F., Yang, S.: Explicit factorizations of cyclotomic polynomials over finite fields. In: Designs, Codes and Cryptography, **83**, pp. 197-217 (2017).
28. Lekkerkerker, C.G., Gruber, P.: Geometry of Numbers. Elsevier Science (1987).
29. Washington L.C.: Introduction to Cyclotomic Fields. Springer, New York (1982).
30. Neukirch, J.: Algebraic Number Theory. Grundlehren der mathematischen Wissenschaften, vol. 322. Springer, 1st edn. (1999).
31. Nathanson, M.B.: Elementary Methods in Number Theory. Springer-Verlag, New York (2000).

A Supplementary Material

A.1 Proof of Theorem 8

Proof. Let $f(x)$ be any irreducible factor of $\Phi_{p^A s}(x)$. We take t in Lemma 2 to be p^{n-A+1} and check the conditions of Lemma 2 term by term. By Lemmas 1 and 3, $f(x)$ has order $p^A s$ and degree m, where m is the least positive integer such that $q^m \equiv 1 \mod sp^A$. We claim that the prime divisor p of t divides $e = sp^A$ but not $\frac{q^m-1}{e}$. Clearly p divides sp^A, so we only need to show the latter. We proceed via induction, and assume first that $A = 1$. Note that $q^{\phi(s)} = 1 \mod s$ (a consequence of Euler's theorem), and so $q^{\phi(s)m'} \equiv 1 \mod sp$, where m' is the smallest integer so that $q^{\phi(s)m'} \equiv 1 \mod p$, and so $m \mid \phi(s)m'$. If a contradiction to our claim were to hold, then we would have

$$q^{\phi(s)m'} - 1 \equiv 0 \mod p^2.$$

The above may be represented in terms of its decomposition into cyclotomic polynomials:

$$q^{\phi(s)m'} - 1 \equiv \prod_{d|m'} \Phi_d(q^{\phi(s)}) \mod p^2.$$

By Lemma 1, each cyclotomic polynomial factors into distinct irreducible factors mod p. Since $q^{\phi(s)} \equiv a \mod p$, the above can only be zero if the factor $(q^{\phi(s)} - a)$ occurs in the factorisation of two distinct cyclotomic polynomials, which implies that there is at least one polynomial $\Phi_k(x)$ containing the factor $(x - a)$ such that $k < m'$. Then we must have

$$q^{\phi(s)k} - 1 \equiv \prod_{d|k} \Phi_d(q^{\phi(s)}) \mod p \equiv 0 \mod p,$$

which is a contradiction since m' was defined to be the minimum integer such that $q^{\phi(s)m'} \equiv 1 \mod p$. Then we must have $p \nmid \frac{q^{m'\phi(s)}-1}{p}$ and since $m \mid m'\phi(s)$, $p \nmid \frac{q^m-1}{e}$. Now, assume that $p \nmid \frac{q^{m'\phi(s)p^{A-1}}-1}{p^A}$ for some $A \geq 1$, and as before we let m' be the minimum integer such that $q^{\phi(s)m'} \equiv 1 \mod p$, so we must have that $m \mid m'\phi(s)p^{A-1}$. By Lemma 4, since $p^A \mid q^{\phi(s)m'p^{A-1}} - 1$ and $p \nmid \frac{q^{\phi(s)m'p^{A-1}}-1}{p^A}$, we must have $p^{A+1} \mid q^{\phi(s)m'p^A} - 1$ and $p \nmid \frac{q^{\phi(s)m'p^A}-1}{p^{A+1}}$, and since $m \mid \phi(s)m'p^A$, it holds that $p \nmid \frac{q^{\phi(s)m}-1}{e}$ as required. Moreover, p is an odd prime so $4 \nmid t$, hence all the requirements in Lemma 2 have been fulfilled. Therefore it follows that $f(x^{p^{n-A+1}})$ is also irreducible over $\mathbb{F}_q$. By this method we can get $\frac{\phi(p^A s)}{m}$ irreducible factors of $\Phi_{p^{n+1}s}(x)$. Now, suppose that $\Phi_{p^{n+1}s}(x)$ factors into $\frac{\phi(p^{n+1}s)}{M} = \frac{(p-1)p^n\phi(s)}{M}$ distinct factors, where M is the least integer such that $q^M \equiv 1 \mod p^{n+1}s$. By Lemma 4, we must have $M = mp^{n-A+1}$ and hence

$$\frac{\phi(p^{n+1}s)}{M} = \frac{(p-1)p^n\phi(s)}{mp^{n-A+1}} = \frac{(p-1)p^{A-1}\phi(s)}{m}.$$

Hence in this way we may obtain all the irreducible factors of $\Phi_{p^{n+1}s}(x)$. □