

On the ideal shortest vector problem over random rational primes

Yanbin Pan¹, Jun Xu², Nick Wadleigh³, and Qi Cheng³

¹ Key Laboratory of Mathematics Mechanization, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China.

`panyanbin@amss.ac.cn`

² State Key Laboratory of Information Security, Institute of Information Engineering Chinese Academy of Sciences, Beijing 100093, China

`xujun@iie.ac.cn`

³ School of Computer Science, University of Oklahoma, Norman, OK 73019, USA.

`ndwadleigh@gmail.com, qcheng@ou.edu`

Abstract. Any non-zero ideal in a number field can be factored into a product of prime ideals. In this paper we report a surprising connection between the complexity of the shortest vector problem (SVP) of prime ideals in number fields and their decomposition groups. When applying the result to number fields popular in lattice based cryptosystems, such as power-of-two cyclotomic fields, we show that a majority of rational primes lie under prime ideals admitting a polynomial time algorithm for SVP. Although the shortest vector problem of ideal lattices underpins the security of the Ring-LWE cryptosystem, this work does not break Ring-LWE, since the security reduction is from the worst case ideal SVP to the average case Ring-LWE, and it is one-way.

Keywords: Ring-LWE · Ideal lattice · Average case computational complexity

1 Introduction

Due to their conjectured ability to resist quantum computer attacks, lattice-based cryptosystems have drawn considerable attention. In 1996, Ajtai [1] pioneered the research on worst-case to average-case reduction for the Short Integer Solution problem (SIS). In 2005, Regev [33] presented a worst-case to average-case (quantum) reduction for the Learning With Errors problem (LWE). SIS and LWE became two important cryptographic assumptions, and a large number of cryptographic schemes based on these two problems have been designed. However, the common drawback of such schemes is their limited efficiency.

To improve the efficiency of lattice-based schemes, some special algebraic structures are employed. The first lattice-based scheme with some algebraic structure was the NTRU public key cryptosystem [15], which was introduced by Hoffstein, Pipher and Silverman in 1996. It works in the convolution ring $\mathbb{Z}[x]/(x^p - 1)$ where p is a prime. The cyclic nature of the ring $\mathbb{Z}[x]/(x^p - 1)$

contributes to NTRU’s efficiency, and makes NTRU one of the most popular schemes. Later the ring was employed in many other cryptographic primitives, such as [25, 21, 31, 26, 36, 5].

In 2009, Stehlé *et al.* [37] introduced a structured and more efficient variant of LWE involving the ring $\mathbb{F}_p[x]/(x^N + 1)$ where N is a power of 2 and p is a prime satisfying $p \equiv 3 \pmod{8}$. In 2010, Lyubashevsky, Peikert and Regev [22] presented a ring-based variant of LWE, called Ring-LWE. The hardness of problems in [37, 22] is based on worst-case assumptions on ideal lattices. Recently, Peikert, Regev and Stephens-Davidowitz [30] presented a polynomial time quantum reduction from (worst-case) ideal lattice problems to Ring-LWE for any modulus and any number field. Lots of schemes employ the ring $\mathbb{Z}[x]/(x^N + 1)$ where N is a power of 2, for example, NewHope [3], Crystals-Kyber [8], and LAC [20] submitted to NIST’s post-quantum cryptography standardization. Although solving the ideal SVP does not necessarily break Ring-LWE, understanding the hardness of ideal SVP is no doubt a very important first step to understand the hardness of Ring-LWE.

1.1 Previous works

Principal ideal lattices are a class of important ideal lattices which can be generated by a single ring element. There is a line of work focusing on the principal ideal SVP. Based on [9, 4], solving approx-SVP problems on principal ideal lattices can be divided into the following two steps: Step 1 is finding an ideal generator by using class group computations. In this step, a quantum polynomial time algorithm is presented by Biasse and Song [7], which is based on the work [14]; a classical subexponential time algorithm was given by Biasse, Espitau, Fouque, Gélín and Kirchner [6]. Step 2 is shortening the ideal generator in Step 1 with the log-unit lattice. This step was analyzed by Cramer, Ducas, Peikert and Regev [11]. Then a quantum polynomial time algorithm for approx-SVP, with a $2^{\tilde{O}(\sqrt{N})}$ approximation factor, on principal ideal lattices in cyclotomic number fields was presented in [11].

In 2017, Cramer, Ducas and Wesolowski [12] extended the case of principal ideal lattices in [11] to the case of a general ideal lattice in a cyclotomic ring of prime-power conductor. For approx-SVP on ideal lattices, the result in [12] is better than the BKZ algorithm [34] when the approximation factor is larger than $2^{\tilde{O}(\sqrt{N})}$. Ducas, Plancon and Wesolowski [13] analyzed the approximation factor $2^{\tilde{O}(\sqrt{N})}$ in [11, 12] to determine the specific dimension N so that the corresponding algorithms outperform BKZ for an ideal lattice in cyclotomic number fields. Recently, Pellet-Mary, Hanrot and Stehlé [32], inspired by the algorithms in [11, 12], proposed an algorithm to solve approx-SVP with the approximation factor $2^{\tilde{O}(\sqrt{N})}$ in ideal lattices for all number fields, aiming to provide trade-offs between the approximation factor and the running time. However, there is an exponential pre-processing phase.

Inspired by Bernstein’s logarithm-subfield attack [4], Albrecht, Bai and Ducas [2] and Cheon, Jeong and Lee [10] independently proposed two similar subfield

attacks in 2016 against overstretched NTRU that has much larger modulus than in the NTRUEncrypt standard. Later, Kirchner and Fouque [16] proposed a variant of the subfield attacks to improve these two attacks in practice. A typical subfield attack consists of three steps: mapping the lattice to some subfield, solving the lattice problem in the subfield and finally lifting the solution to the full field.

1.2 Our results

In this paper, we investigate the SVP for lattices corresponding to prime ideals in number fields normal over \mathbb{Q} . Every nonzero ideal in a Dedekind Domain can be factored uniquely into a product of prime ideals, so short vectors in prime ideals may help us to find short vectors in general ideals. If, in a general prime ideal \mathfrak{p} , we are able to efficiently find a vector with length within the Minkowski bound for \mathfrak{p} , then for an ideal \mathfrak{a} with few prime ideal factors, we will be able to approximate the shortest vector in \mathfrak{a} to within a factor much better than what is achieved by the LLL [17] or BKZ [35] algorithms. The most difficult step in factoring an ideal is actually factorization of an integer (the norm of the ideal), which can be done in polynomial time by quantum computers, or in subexponential time by classical computers.

Consider a finite Galois extension $\mathbb{L} \cong \mathbb{Q}[x]/(f(x))$ of \mathbb{Q} , and let \mathfrak{P} be a prime ideal in the ring of integers $O_{\mathbb{L}}$ of \mathbb{L} . The subgroup of $Gal(\mathbb{L}/\mathbb{Q})$ that stabilizes \mathfrak{P} set-wise is known as the *decomposition group* of \mathfrak{P} . Let $\mathbb{K} \subset \mathbb{L}$ be the subfield fixed by the decomposition group of \mathfrak{P} . \mathbb{K} is called the *decomposition field* of \mathfrak{P} . To find a short vector in \mathfrak{P} , we can search for a short vector in the lattice $\mathfrak{P} \cap \mathbb{K}$, which may have smaller rank. More precisely, for a rational prime p , if $pO_{\mathbb{L}}$ is factored into a product of g prime ideals in $O_{\mathbb{L}}$, we can reduce the problem of finding a short vector in any of these prime ideals to a problem of finding a short vector in a rank- g lattice, provided that a basis of $O_{\mathbb{K}}$ can be found efficiently. Equivalently, the fewer the number of irreducible factors of $f(x)$ over \mathbb{F}_p , the more efficiently we may solve SVP for prime ideals lying above p . One argues from general facts of algebraic number theory that the determinant of the sublattice is not too large compared to the original lattice in order to relate Minkowski type λ_1 bounds for the two lattices.

We go on to apply the foregoing idea to the rings $\mathbb{Z}[x]/(x^{2^n} + 1)$, which are quite popular in cryptography. We show that there is a hierarchy for the hardness of SVP for these prime ideal lattices. This arises from the observation that the decomposition groups (or their index-two subgroups) form a chain in the subgroup lattice (See Appendices A and B). Roughly speaking, we can classify such prime ideal lattices into n distinct classes, and for a prime ideal lattice in the r -th class, we can find its shortest vector by solving SVP in a dimension- 2^r lattice. This suggests that the difficulty of prime ideal SVP can change dramatically from ideal to ideal, an interesting phenomenon that has, to our knowledge, not been pointed out in the literature. By considering some of these classes, we prove that a nontrivial fraction of prime ideals admit an efficient SVP algorithm.

Theorem 1. *Let $N = 2^n$, where n is a positive integer. Let \mathfrak{p} be a prime ideal in the ring $\mathbb{Z}[x]/(x^N + 1)$, and suppose \mathfrak{p} contains a prime number $p \equiv \pm 3 \pmod{8}$. Then under the coefficient embedding, the shortest vector in \mathfrak{p} can be found in time $\text{poly}(N, \log p)$, and the length of the shortest vector is exactly \sqrt{p} .*

Can we conclude from the above result that the *average case* prime ideal SVP is easy? It depends how we define an average prime ideal lattice. As prime ideals are rigid structures, changing distributions gives us totally different complexity results. If prime ideals are selected uniformly at random from the set of those prime ideals whose norms are bounded, then easy cases are rare. Nevertheless our result does show that an average case of the prime ideal SVP in power-of-two cyclotomic fields is not hard, if the prime ideals are selected uniformly at random from the set of all prime ideals whose rational primes are less than some fixed bound. See Subsection 4.2 for details.

For general (non prime) ideals in $\mathbb{Z}[x]/(x^{2^n} + 1)$, we present an algorithm to confirm that the hierarchy for the hardness of SVP also exists; that is, we can solve SVP for a general ideal lattice by solving SVP in a 2^r -dimensional sublattice, for some positive integer r related to the factorization of the ideal (see Theorem 6). Following Theorem 1, we show how to solve the SVP for ideals all of whose prime factors lie in a certain class. This is a special case of Theorem 6.

Proposition 1. *Let $N = 2^n$, where n is a positive integer. Let \mathcal{I} be an ideal in the ring $\mathbb{Z}[x]/(x^N + 1)$ with prime factorization*

$$\mathcal{I} = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_k.$$

If each \mathfrak{p}_i contains a prime integer $\equiv \pm 3 \pmod{8}$, the shortest vector in \mathcal{I} can be found in time $\text{poly}(N, \log(\mathcal{N}(\mathcal{I})))$.

We would like to stress that the algorithm works by exploiting the multiplicative structure of ideals in the ring of integers of a number field, without factoring the ideal. We regard this as the second contribution of this work, in addition to the algorithm for prime ideals.

Note that a decomposition field is a subfield of the number field. Our algorithm can also be seen as a kind of subfield attack to solve the ideal Hermite-SVP problem. Compared with the previous subfield attacks [4, 2, 10, 16], the main differences are: the previous subfield attacks use relative norm (or trace) to map a lattice into some subfield, while we use the intersection with the decomposition field; The approximation factor in the previous attacks, such as [2], will suffer during the lifting process, while our lifting costs not so much; The previous attacks [2, 10, 16] work for NTRU with much big modulus, while the instances amenable to our attack must satisfy the condition that the decomposition field is a proper subfield of the number field.

We have to point out that it is still unknown how our result impacts the security of cryptographic schemes. It does not break Ring-LWE, since the security reduction is from the worst case ideal SVP to the average case Ring-LWE,

and it is one-way. As pointed out by [4], Smart and Vercauteren [29] proposed an ideal lattice-based fully homomorphic encryption scheme, which generated a prime ideal lattice as the public key. It is enough to break the scheme by finding a short vector in the lattice. To improve the efficiency, they chose ideals of prime determinants, which are not weak instances revealed by our algorithm. Our paper provides a security justification for using such ideal lattices. We should no doubt avoid the weak instances when we construct cryptographic schemes. In addition, our result is a beneficial attempt to solve ideal SVP by exploiting the algebraic structure, and it helps us understand better the hardness of ideal SVP.

1.3 Paper organization

The remainder of the paper is organized as follows. In Section 2, we give some mathematical preliminaries. In Section 3 we prove a reduction of approx-SVP in the finite Galois extension of \mathbb{Q} . Then in section 4 we present a reduction of SVP for prime ideal lattices and then general ideal lattices in $\mathbb{Z}[\zeta_{2^n+1}]$. Finally, a conclusion and some open problems are given in Section 5.

2 Mathematical preliminaries

2.1 Lattices and some computational problems

Lattices are discrete additive subgroups of \mathbb{R}^N . Any finite set of linearly independent vectors $b_1, b_2, \dots, b_m \in \mathbb{R}^N$ generates a lattice:

$$\mathcal{L} = \left\{ \sum_{i=1}^m z_i b_i \mid z_i \in \mathbb{Z} \right\}.$$

Denote by B the matrix whose column vectors are the b_i 's. We say B is a basis (in matrix form) for \mathcal{L} ; m and N are the rank and dimension of \mathcal{L} , respectively. Denote by $\det(\mathcal{L})$ the determinant of lattice \mathcal{L} , which is defined as the (co)volume of \mathcal{L} in the real subspace spanned by \mathcal{L} . Note that if $m = N$, the determinant of \mathcal{L} is exactly $|\det(B)|$.

The shortest vector problem (SVP), which refers to the problem of finding a shortest nonzero lattice vector in a given lattice, is one of the most famous hard problems in lattice theory. There are some variants of SVP that are very important for applications.

- Approx-SVP: Given a lattice \mathcal{L} and an approximation factor $\gamma \geq 1$, find a non-zero lattice vector of norm $\leq \gamma \cdot \lambda_1(\mathcal{L})$, where $\lambda_1(\mathcal{L})$ is the length of a shortest non-zero vector in \mathcal{L} .
- Hermite-SVP: Given a rank- N lattice \mathcal{L} and an approximation factor $\gamma \geq 1$, find a non-zero lattice vector of norm $\leq \gamma \cdot \det(\mathcal{L})^{\frac{1}{N}}$. Note that Minkowski's theorem [27] tells us that

$$\lambda_1(\mathcal{L}) \leq \frac{2}{\mathcal{V}_N^{1/N}} \cdot \det(\mathcal{L})^{\frac{1}{N}} \leq \sqrt{N} \cdot \det(\mathcal{L})^{\frac{1}{N}},$$

where \mathcal{V}_N is the volume of the N -dimensional ball with radius 1. Thus for any $\gamma \geq \sqrt{N}$, Hermite-SVP is well-defined for all rank- N lattices.

Since $\lambda_1(\mathcal{L})$ is usually hard to determine given a basis of \mathcal{L} , it might be very hard to verify a solution returned by an algorithm for Approx-SVP with some approximation factor. However, the solution to Hermite-SVP can be verified efficiently. Hence, many algorithms, such as LLL [17] and BKZ [35], are designed as polynomial-time Hermite-SVP algorithms for some exponential approximation factor.

It is obvious that any algorithm that solves Approx-SVP with factor γ can also solve Hermite-SVP with factor $\gamma\sqrt{N}$ by Minkowski's theorem. Furthermore, based on an idea of Lenstra and Schnorr, Lovász showed that any algorithm solving Hermite-SVP with factor γ can be used to solve Approx-SVP with factor γ^2 in polynomial time [19].

Moreover, a solution to Hermite-SVP with factor \sqrt{N} , that is, satisfying the Minkowski bound, is usually taken as a good enough approximation of some shortest vector in a "random" lattice. In addition, when choosing parameters for lattice-based cryptosystems in practice, such as in NewHope[3], Crystals-Kyber [8], and LAC [20], the time complexity of solving Hermite-SVP with some particular factor usually determines the concrete security of these cryptosystems. Therefore, the algorithm for Hermite-SVP is key to both solving Approx-SVP and analyzing the security of lattice-based cryptosystems.

The closest vector problem (CVP) is another famous hard problem in lattice theory. This refers to the problem of finding a lattice vector that is closest to a given vector.

2.2 Some basic algebraic number theory

We will review some basic algebraic number theory in this section. More details can be found in [23] or [28]

Number fields An algebraic number $\zeta \in \mathbb{C}$ is any root of a nonzero polynomial $f(x) \in \mathbb{Q}[x]$ and its minimal polynomial is the unique monic irreducible $f(x) \in \mathbb{Q}[x]$ of minimal degree that has ζ as a root. An algebraic number is called an algebraic integer if its minimal polynomial lies in $\mathbb{Z}[x]$.

An algebraic number field is a finite field extension \mathbb{K} of \mathbb{Q} . Such a field can be obtained by adjoining a single algebraic integer ζ to \mathbb{Q} . That is, $\mathbb{K} = \mathbb{Q}(\zeta)$ for some algebraic integer ζ . The degree N of the minimal polynomial $f(x)$ of ζ is also the degree of \mathbb{K} over \mathbb{Q} .

Denote by $O_{\mathbb{K}}$ the ring of algebraic integers in \mathbb{K} . It is an integral domain and also a free \mathbb{Z} -module with rank N .

For example, let $\zeta_{2^{n+1}}$ be a complex primitive 2^{n+1} -th root of unity, whose minimal polynomial is $f = x^{2^n} + 1$. Then, $\mathbb{K} = \mathbb{Q}(\zeta_{2^{n+1}})$ is the cyclotomic number field of order 2^{n+1} with degree 2^n . Its ring of integers is well known to be $\mathbb{Z}[\zeta_{2^{n+1}}]$.

Embeddings A number field \mathbb{K} of degree N over \mathbb{Q} has exactly N embeddings into \mathbb{C} . Let $\sigma_1, \sigma_2, \dots, \sigma_{s_1}$ be the real embeddings from \mathbb{K} to \mathbb{R} , and let

$$\sigma_{s_1+1}, \sigma_{s_1+2}, \dots, \sigma_{s_1+s_2},$$

$$\sigma_{s_1+s_2+1} = \overline{\sigma_{s_1+1}}, \quad \sigma_{s_1+s_2+2} = \overline{\sigma_{s_1+2}}, \quad \dots, \quad \sigma_{s_1+2s_2} = \overline{\sigma_{s_1+s_2}}$$

be the non-real embeddings from \mathbb{K} to \mathbb{C} , where $\bar{\cdot}$ denotes complex conjugation.

From these σ_i 's we can define the *canonical embedding* $\Sigma_{\mathbb{K}}$ from \mathbb{K} to \mathbb{C}^N :

$$\Sigma_{\mathbb{K}} : \mathbb{K} \rightarrow \mathbb{C}^N, \quad a \mapsto (\sigma_1(a), \sigma_2(a), \dots, \sigma_N(a)).$$

It is known that the image of $\Sigma_{\mathbb{K}}$ falls into a subspace in \mathbb{C}^N , which is isomorphic to \mathbb{R}^N as an inner product space (see [22]).

Another important embedding from \mathbb{K} to \mathbb{R}^N is the *coefficient embedding*, which is most commonly used in cryptographic constructions. This embedding depends on a choice of generator α for \mathbb{K} : write $\mathbb{K} = \mathbb{Q}(\alpha)$ and map $\beta = a_0 + a_1\alpha + \dots + a_{N-1}\alpha^{N-1}$ to its coefficient vector, $C(\beta) := (a_0, a_1, \dots, a_{N-1})$.

If α may be chosen so that

$$O_{\mathbb{K}} = \mathbb{Z} + \alpha\mathbb{Z} + \alpha^2\mathbb{Z} + \dots + \alpha^{N-1}\mathbb{Z}$$

we say $O_{\mathbb{K}}$ is *monogenic*. In this case the coefficient embedding maps $O_{\mathbb{K}}$ to \mathbb{Z}^N . Alternatively, via $O_{\mathbb{K}} \cong \mathbb{Z}[x]/(f(x))$, where $f(x)$ is the minimal polynomial of α , we may think of C mapping a polynomial in $\mathbb{Z}[x]/(f(x))$ to its coefficient vector:

$$C(a_0 + a_1x + \dots + a_{N-1}x^{N-1}) = (a_0, a_1, \dots, a_{N-1}).$$

Discriminants If $\mathbb{K} \subset \mathbb{L}$ are number fields, the (relative) discriminant of a \mathbb{K} -basis b_1, b_2, \dots, b_N for \mathbb{L} is defined by

$$d_{\mathbb{L}/\mathbb{K}}(b_1, b_2, \dots, b_N) = |\det(\sigma_i b_j)|^2,$$

where σ_i varies over the $[\mathbb{L} : \mathbb{K}]$ embeddings $\mathbb{L} \rightarrow \mathbb{C}$ which fix all elements of \mathbb{K} . The discriminant $\text{disc}(O_{\mathbb{L}}/O_{\mathbb{K}})$, also denoted by $\text{disc}(\mathbb{L}/\mathbb{K})$, is then the ideal of $O_{\mathbb{K}}$ which is generated by the discriminants $d_{\mathbb{L}/\mathbb{K}}(b_1, b_2, \dots, b_N)$ of all the \mathbb{K} -bases b_1, b_2, \dots, b_N of \mathbb{L} which are contained in $O_{\mathbb{L}}$.

For any number field \mathbb{K} , the (absolute) discriminant $\text{disc}(\mathbb{K}/\mathbb{Q})$ becomes the principal ideal generated by $d(b_1, b_2, \dots, b_N)$ for any basis b_1, b_2, \dots, b_N of the free \mathbb{Z} -module $O_{\mathbb{K}}$. In this case we just write $\text{disc}(\mathbb{K})$ to refer to this ideal or the unique positive integer that generates it. In a sense made precise by the embeddings defined above, the discriminant gives a notion of the co-volume of a ring of integers in its fraction field. Specifically, the discriminant is just the square of this co-volume.

2.3 Ideal lattices

The ring of integers $O_{\mathbb{K}}$ of \mathbb{K} is a free \mathbb{Z} -module, and any ideal \mathcal{I} in $O_{\mathbb{K}}$ is a free \mathbb{Z} -submodule since \mathbb{Z} is a principal ideal domain. Under the canonical embedding or the coefficient embedding, any such \mathcal{I} is sent to a lattice in \mathbb{R}^N . We call this image the *ideal lattice* associated with \mathcal{I} , and we denote it also by \mathcal{I} .

Under the canonical embedding $\Sigma_{\mathbb{K}}$ from \mathbb{K} to \mathbb{C}^N , the co-volume (i.e. the volume of a fundamental domain) of an ideal lattice \mathcal{I} is given by $N_{\mathbb{K}}(\mathcal{I})\sqrt{|\text{disc}(\mathbb{K})|}$, where $N_{\mathbb{K}}(\mathcal{I})$ is the *norm* of \mathcal{I} , defined as the cardinality of $O_{\mathbb{K}}/\mathcal{I}$. Note that when we say the norm of a vector, it refers to the Euclidean norm rather than the algebra norm of an ideal.

Usually it is easier to use the canonical embedding in mathematical analysis, and to use the coefficient embedding in cryptography. For example, under the coefficient embedding of $\mathbb{Z}[\zeta_{2^{n+1}}]$, the lattice associated with the prime ideal $\mathfrak{p}_i = (p, f_i(\zeta_{2^{n+1}}))$ is generated by the coefficient vectors of the following polynomials (modulo $x^N + 1$)

$$f_i, xf_i, \dots, x^{N-1}f_i \quad \text{and} \quad p, px, \dots, px^{N-1},$$

where p is some rational prime, and f_i is some irreducible factor of $x^{2^n} + 1$ modulo p . The minimum generating set should have only N vectors, which can be found by computing the Hermite Normal Form.

Ideals in $\mathbb{Z}[\zeta_{2^{n+1}}]$ The cyclotomic field of order $2N = 2^{n+1}$ is widely used in cryptography. Its ring of integers is $\mathbb{Z}[\zeta_{2^{n+1}}]$, which is isomorphic to $\mathbb{Z}[x]/(x^N + 1)$. Its discriminant is 2^{n2^n} .

Let p be a rational prime, and let

$$x^N + 1 = (f_1 f_2 \cdots f_g)^e$$

be the prime factorization of $x^N + 1$ in the polynomial ring $\mathbb{F}_p[x]$. Then we have

$$(p) = (\mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_g)^e,$$

where $\mathfrak{p}_i = (p, f_i(\zeta_{2^{n+1}}))$ (here f_i is any integer polynomial which projects to the f_i in the above factorization). We say the prime ideal \mathfrak{p}_i *lies over* the prime p . If e is greater than 1, we say the prime p is *ramified* (in $\mathbb{Z}[\zeta_{2^{n+1}}]$); otherwise we say p is *unramified*. One can verify that 2 is the only ramified rational prime in the cyclotomic field of order $2N$, and that the prime ideal $(2, \zeta_{2^{n+1}} + 1) = (\zeta_{2^{n+1}} + 1)$ lies above the ideal (2).

We are therefore interested in the explicit factorization of the 2^{n+1} -th cyclotomic polynomials, $x^{2^n} + 1$, over $\mathbb{F}_p[x]$. This is computed in [18, Thm. 2.47 and Thm. 3.75] when $p \equiv 1 \pmod{4}$ and in [24] when $p \equiv 3 \pmod{4}$.

Theorem 2. *Let $p \equiv 1 \pmod{4}$, i.e. $p = 2^A \cdot m + 1$, $A \geq 2$, m odd. Denote by U_k the set of all primitive 2^k -th roots of unity modulo p . We have*

– If $n < A$, then $x^{2^n} + 1$ is the product of 2^n irreducible linear factors over \mathbb{F}_p :

$$x^{2^n} + 1 = \prod_{u \in U_{n+1}} (x + u).$$

– If $n \geq A$, then $x^{2^n} + 1$ is the product of 2^{A-1} irreducible binomials over \mathbb{F}_p of degree 2^{n-A+1} :

$$x^{2^n} + 1 = \prod_{u \in U_A} (x^{2^{n-A+1}} + u).$$

Theorem 3. Let $p \equiv 3 \pmod{4}$, i.e. $p = 2^A \cdot m - 1$, $A \geq 2$, m odd. Denote by $D_s(x, a)$ the Dickson polynomials

$$\sum_{i=0}^{\lfloor \frac{s}{2} \rfloor} \frac{s}{s-i} \binom{s-i}{i} (-a)^i x^{s-2i}$$

over \mathbb{F}_p . For $n \geq 2$, we have

– If $n < A$, then $x^{2^n} + 1$ is the product of 2^{n-1} irreducible trinomials over \mathbb{F}_p :

$$x^{2^n} + 1 = \prod_{\gamma \in \Gamma} (x^2 + \gamma x + 1),$$

where Γ is the set of all roots of $D_{2^{n-1}}(x, 1)$.

– If $n \geq A$, then $x^{2^n} + 1$ is the product of 2^{A-1} irreducible trinomials over \mathbb{F}_p of degree 2^{n-A+1} :

$$x^{2^n} + 1 = \prod_{\delta \in \Delta} (x^{2^{n-A+1}} + \delta x^{2^{n-A}} - 1),$$

where Δ is the set of all roots of $D_{2^{A-1}}(x, -1)$.

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

In the following, we will consider solving Hermite-SVP for prime ideals of $O_{\mathbb{L}}$ when \mathbb{L} is a finite Galois extension of \mathbb{Q} .

A prime ideal \mathfrak{p} in $O_{\mathbb{L}}$ contains a rational prime p , and therefore occurs as one of the prime ideals in the factorization

$$pO_{\mathbb{L}} = (\mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_g)^e.$$

Without loss of generality, we assume $\mathfrak{p}_1 = \mathfrak{p}$.

To find a short vector of \mathfrak{p}_1 , we try to find a short vector in the sublattice given by the intersection of \mathfrak{p}_1 with some intermediate field between \mathbb{Q} and \mathbb{L} . Since this sublattice has smaller rank, this may lead to a more efficient algorithm than working in \mathbb{L} directly.

More precisely, let G be the Galois group of \mathbb{L} over \mathbb{Q} . Recall the decomposition group, D , and decomposition field, \mathbb{K} , for \mathfrak{p}_1 :

$$D := \{\sigma \in G : \sigma(\mathfrak{p}_1) = \mathfrak{p}_1\},$$

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

Let $O_{\mathbb{K}}$ be the algebraic integer ring of \mathbb{K} . It is well known that the degree of \mathbb{K} over \mathbb{Q} is g (see [23, Thm. 28]). This is our desired intermediate field, and we have the following theorem.

Theorem 4. *Suppose \mathbb{L}/\mathbb{Q} is a finite Galois extension with degree N , and suppose \mathfrak{p} is a prime ideal of $O_{\mathbb{L}}$ lying over an unramified rational prime p such that $pO_{\mathbb{L}}$ has g distinct prime ideal factors in $O_{\mathbb{L}}$. If \mathbb{K} is the decomposition field of \mathfrak{p} , then a solution to Hermite-SVP with factor γ in the sublattice $\mathfrak{c} = \mathfrak{p} \cap O_{\mathbb{K}}$ under the canonical embedding of \mathbb{K} will also be a solution to Hermite-SVP in \mathfrak{p} with factor $\frac{\sqrt{N/g}}{N_{\mathbb{K}}(\text{disc}(\mathbb{L}/\mathbb{K}))^{1/(2N)}} \cdot \gamma$ ($\leq \sqrt{\frac{N}{g}} \cdot \gamma$) under the canonical embedding of \mathbb{L} .*

In particular, when $\gamma = \sqrt{g}$, a vector in the sublattice \mathfrak{c} satisfying the Minkowski bound will produce a vector in the lattice \mathfrak{p} satisfying the Minkowski bound.

Proof. Consider the following diagram

$$\begin{array}{ccccccc} \mathfrak{p} & \subset & O_{\mathbb{L}} & \subset & \mathbb{L} & \xrightarrow{\Sigma_{\mathbb{L}}} & \mathbb{C}^N \\ | & & | & & | & & \beta \uparrow \\ \mathfrak{c} & \subset & O_{\mathbb{K}} & \subset & \mathbb{K} & \xrightarrow{\Sigma_{\mathbb{K}}} & \mathbb{C}^g \\ | & & | & & | & & \uparrow \\ (p) & \subset & \mathbb{Z} & \subset & \mathbb{Q} & \subset & \mathbb{C} \end{array}$$

Here β is chosen to be the linear map making the diagram commute.

Note that every embedding of \mathbb{K} in \mathbb{C} can be extended to exactly $\frac{N}{g}$ embeddings of \mathbb{L} in \mathbb{C} [23, Thm. 50]; thus β is (up to permutation) just the linear embedding given by repeating each coordinate N/g times. Thus for any $v \in \mathbb{C}^g$ we have

$$\|\beta(v)\| = \sqrt{\frac{N}{g}} \cdot \|v\|. \quad (1)$$

Note that the norm of \mathfrak{c} is exactly p [23, Thm. 29], so that the determinant of \mathfrak{c} is $p\sqrt{|\text{disc}(\mathbb{K})|}$. Thus, under the canonical embedding of $O_{\mathbb{K}}$ into \mathbb{C}^g , any solution $v_0 \in \mathfrak{c}$ to Hermite-SVP with factor γ satisfies

$$\|v_0\| \leq \gamma \cdot p^{\frac{1}{g}} |\text{disc}(\mathbb{K})|^{\frac{1}{2g}}.$$

By Equation (1) above and the fact that $\text{disc}(\mathbb{L}) = \text{disc}(\mathbb{K})^{N/g} N_{\mathbb{K}}(\text{disc}(\mathbb{L}/\mathbb{K}))$ [28, Corollary (2.10), pp. 202], we therefore have

$$\begin{aligned} \|\beta(v_0)\| &\leq \gamma \cdot \sqrt{\frac{N}{g}} p^{\frac{1}{g}} |\text{disc}(\mathbb{K})|^{\frac{1}{2g}} \\ &= \gamma \cdot \frac{\sqrt{N/g}}{N_{\mathbb{K}}(\text{disc}(\mathbb{L}/\mathbb{K}))^{1/(2N)}} p^{\frac{1}{g}} |\text{disc}(\mathbb{L})|^{\frac{1}{2N}} \\ &= \gamma \cdot \frac{\sqrt{N/g}}{N_{\mathbb{K}}(\text{disc}(\mathbb{L}/\mathbb{K}))^{1/(2N)}} (p^{\frac{N}{g}} \sqrt{|\text{disc}(\mathbb{L})|})^{\frac{1}{N}} \end{aligned}$$

Note that the norm of \mathfrak{p} is $p^{\frac{N}{g}}$, and thus $p^{\frac{N}{g}} \sqrt{|\text{disc}(\mathbb{L})|}$ is exactly the determinant of the ideal lattice \mathfrak{p} under the canonical embedding of \mathbb{L} . Hence v_0 is also a solution to Hermite-SVP with factor $\frac{\sqrt{N/g}}{N_{\mathbb{K}}(\text{disc}(\mathbb{L}/\mathbb{K}))^{1/(2N)}} \cdot \gamma$.

Note that $N_{\mathbb{K}}(\text{disc}(\mathbb{L}/\mathbb{K}))$ is a positive integer. Thus

$$\frac{\sqrt{N/g}}{N_{\mathbb{K}}(\text{disc}(\mathbb{L}/\mathbb{K}))^{1/(2N)}} \leq \sqrt{\frac{N}{g}}.$$

In particular, when $\gamma = \sqrt{g}$, $\frac{\sqrt{N/g}}{N_{\mathbb{K}}(\text{disc}(\mathbb{L}/\mathbb{K}))^{1/(2N)}} \cdot \gamma \leq \sqrt{N}$ still holds. The theorem follows. \square

Remark 1. To design an algorithm from the theorem, we need to calculate the decomposition field from a prime ideal. In general this is not an easy problem. Fortunately, for power-of-two or prime order cyclotomic fields, the subfield structures have been worked out in the literature. Another technical problem is to compute a basis for $\mathfrak{c} = \mathfrak{p} \cap O_{\mathbb{K}}$. This can be solved if we know a \mathbb{Q} -basis of \mathbb{K} .

Remark 2. How many prime ideals are vulnerable to this attack? In other words, given an irreducible polynomial over \mathbb{Z} , how does its factoring pattern change over \mathbb{F}_p as p varies? This is a central topic of class field theory when the Galois group is solvable. In the general case, it has been studied in the famous Langlands program, where many challenging problems remain. The answer is well known for number fields popular in lattice based cryptography. There exists a set of rational primes, of positive density with non-trivial decomposition group, such that for any p in this set, the decomposition fields of the prime ideals lying above p are never the whole field \mathbb{L} . In this case, $\mathfrak{p} \cap O_{\mathbb{K}}$ has rank no more than half that of \mathfrak{p} , resulting in a much easier SVP problem.

4 Solving SVP for ideal lattices in $\mathbb{Z}[\zeta_{2^{n+1}}]$

In the following, we use the above idea to solve SVP for ideal lattices in $\mathbb{Z}[\zeta_{2^{n+1}}]$, the ring of integers in the cyclotomic field $\mathbb{Q}(\zeta_{2^{n+1}})$, a field which is widely used in

lattice-based cryptography. The decomposition field of any prime ideal is either equal to, or a degree-2 subfield of, one of the following

$$\mathbb{Q}[i] \subset \mathbb{Q}[\zeta_8] \subset \cdots \subset \mathbb{Q}[\zeta_{2^n}] \subset \mathbb{Q}[\zeta_{2^{n+1}}].$$

The subfields in this chain are convenient because they are monogenic and their integer rings have \mathbb{Z} -bases (powers of $\zeta_{2^{n+1}}$) that are mutually compatible and orthogonal under the canonical embedding. This results in a hierarchy of complexity of prime ideal SVP problems. Furthermore, for a non-prime ideal \mathcal{I} , we can approximate the shortest vectors of \mathcal{I} by finding short vectors in $\mathcal{I} \cap O_{\mathbb{K}}$, where \mathbb{K} is the smallest field in the above chain containing all the decomposition fields of the prime factors of \mathcal{I} . This allows us to find short vectors for many non-prime ideals. In contrast to the approximation result we achieved in the general setting of Theorem 4, an *exact* SVP solution is possible in power-of-two cyclotomic fields. We will first prove a reduction for SVP for *prime* ideal lattices in $\mathbb{Z}[\zeta_{2^{n+1}}]$, and then we will prove a reduction for general ideals. We would like to point out that in the case of a general ideal lattice \mathcal{I} , we do not need to know the prime factorization of \mathcal{I} to run our algorithm.

4.1 Solving SVP for prime ideal lattices in $\mathbb{Z}[\zeta_{2^{n+1}}]$

For simplicity we let $\zeta = \zeta_{2^{n+1}}$. In the sequel we say goodbye to the canonical embedding and adopt the coefficient embedding C :

$$\mathbb{Q}(\zeta) \rightarrow \mathbb{R}^{2^n}, \quad \sum_{i=0}^{2^n-1} a_i \zeta^i \mapsto (a_0, a_1, \dots, a_{2^n-1}).$$

The coefficient embedding is widely used in cryptographic constructions. For power-of-two cyclotomic fields, the two embeddings are related by scaled-rotations, since for any $v \in \mathbb{Z}[\zeta_{2^{n+1}}]$ it is easy to see that

$$\|\Sigma_{\mathbb{L}}(v)\| = \sqrt{2^n} \|C(v)\|.$$

Hence, the shortest vector under the coefficient embedding of $\mathbb{Q}(\zeta)$ must be the shortest under the canonical embedding.

The prime 2 is the unique ramified prime in $\mathbb{Q}(\zeta)$, and the prime ideal lying over (2) is $(2, \zeta + 1) = (\zeta + 1)$. Hence it is easy to find the shortest vector in the ideal lattice $(\zeta + 1)$, and its length is $\sqrt{2}$.

Below we consider a prime ideal lying over an odd prime and show that there is a hierarchy for the hardness of solving SVP for prime ideal lattices in $\mathbb{Z}[\zeta]$. Roughly speaking, we can classify all the prime ideal lattices into n classes labeled with $1, 2, \dots, n$, depending on the congruence class of $p \pmod{2^{n+1}}$, and for a prime ideal lattice in the r -th class, we can always find its shortest vector by solving SVP in a 2^r -dimensional lattice. More precisely, we have:

Theorem 5. For any prime ideal $\mathfrak{p} = (p, f(\zeta))$ in $\mathbb{Z}[\zeta]$, where p is an odd prime and $f(x)$ is some irreducible factor of $x^{2^n} + 1$ in $\mathbb{F}_p[x]$. Write

$$p = \begin{cases} 2^A \cdot m + 1, & \text{if } p \equiv 1 \pmod{4}; \\ 2^A \cdot m - 1, & \text{if } p \equiv 3 \pmod{4}, \end{cases}$$

for some odd m and $A \geq 2$, and let

$$r = \begin{cases} \min\{A - 1, n\}, & \text{if } p \equiv 1 \pmod{4}; \\ \min\{A, n\}, & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

Then given an oracle that can solve SVP for 2^r -dimensional lattices, a shortest nonzero vector in \mathfrak{p} can be found in $\text{poly}(2^n, \log_2 p)$ time with the coefficient embedding.

Proof. It is well known that the Galois group G of $\mathbb{Q}(\zeta)$ over \mathbb{Q} is isomorphic to the multiplicative group $(\mathbb{Z}/2^{n+1}\mathbb{Z})^*$. Let $G = \{\sigma_1, \sigma_3, \dots, \sigma_{2^{n+1}-1}\}$ where

$$\begin{aligned} \sigma_i : \mathbb{Q}(\zeta) &\rightarrow \mathbb{Q}(\zeta); \\ \zeta &\mapsto \zeta^i. \end{aligned}$$

We proceed by considering two separate cases.

Case 1: First we deal with the case when $p \equiv 1 \pmod{4}$. The theorem is vacuously true for $n < A$.

If $n \geq A$, we have $r = A - 1$. By Theorem 2, we know that

$$f(x) = x^{2^{n-A+1}} + u = x^{2^{n-r}} + u$$

for some $u \in U_A$. Then the prime ideal lattice \mathfrak{p} can be generated by p and $f(\zeta) = \zeta^{2^{n-r}} + u$. Consider the subgroup $H = \langle \sigma_{2^{r+1}+1} \rangle$ of G generated by $\sigma_{2^{r+1}+1}$. H is a subgroup of the decomposition group of the ideal \mathfrak{p} since

$$\sigma_{2^{r+1}+1}(p) = p, \quad \sigma_{2^{r+1}+1}(f(\zeta)) = f(\zeta).$$

Note that $\mathbb{K} = \mathbb{Q}(\zeta^{2^{n-r}})$ is the fixed field of H and its integer ring $O_{\mathbb{K}}$ has a \mathbb{Z} -basis $(1, \zeta^{2^{n-r}}, \zeta^{2 \cdot 2^{n-r}}, \dots, \zeta^{(2^r-1) \cdot 2^{n-r}})$.

Let $\mathfrak{c} = \mathfrak{p} \cap O_{\mathbb{K}}$. We claim that \mathfrak{p} is a direct sum:

$$\mathfrak{p} = \bigoplus_{k=0}^{2^{n-r}-1} \zeta^k \mathfrak{c}. \quad (2)$$

Indeed for any $a \in \mathfrak{p}$, there exist integers z_i 's and w_i 's such that

$$\begin{aligned} a &= \sum_{i=0}^{2^n-1} z_i \zeta^i f(\zeta) + \sum_{i=0}^{2^n-1} w_i p \zeta^i \\ &= \sum_{k=0}^{2^{n-r}-1} \zeta^k \sum_{j=0}^{2^r-1} (z_{k+j \cdot 2^{n-r}} \zeta^{j \cdot 2^{n-r}} f(\zeta) + w_{k+j \cdot 2^{n-r}} p \zeta^{j \cdot 2^{n-r}}) \\ &= \sum_{k=0}^{2^{n-r}-1} \zeta^k \left(\left(\sum_{j=0}^{2^r-1} z_{k+j \cdot 2^{n-r}} \zeta^{j \cdot 2^{n-r}} \right) f(\zeta) + \left(\sum_{j=0}^{2^r-1} w_{k+j \cdot 2^{n-r}} \zeta^{j \cdot 2^{n-r}} \right) p \right). \end{aligned}$$

Let $a^{(k)} = (\sum_{j=0}^{2^r-1} z_{k+j \cdot 2^{n-r}} \zeta^{j \cdot 2^{n-r}}) f(\zeta) + (\sum_{j=0}^{2^r-1} w_{k+j \cdot 2^{n-r}} \zeta^{j \cdot 2^{n-r}}) p$ for any k . Since $p \in \mathfrak{c}$ and $f(\zeta) \in \mathfrak{c}$, $a^{(k)} \in \mathfrak{c}$. We have established (2).

Since multiplication by ζ is an isometry and for $x \in \mathfrak{c}$, the coefficients of $\zeta^i x$ and $\zeta^j x$ are disjoint for $i \neq j \pmod{2^{n-r}}$, Equation (2) implies

$$\lambda_1(\mathfrak{p}) = \lambda_1(\mathfrak{c}),$$

and that to find the shortest vector in the ideal lattice \mathfrak{p} , it is enough to find the shortest vector v in the ideal lattice \mathfrak{c} , a lattice with dimension 2^r . Indeed $\zeta^k v$ for any $0 \leq k \leq 2^{n-r} - 1$ will be a shortest vector in the ideal lattice \mathfrak{p} .

Case 2: For the case when $p \equiv 3 \pmod{4}$, everything is similar except that $r = A$.

Algorithm: We can summarize the algorithm to solve SVP in a prime ideal lattice as Algorithm 1.

Algorithm 1 Solve SVP in prime ideal lattice

Input: a prime ideal $\mathfrak{p} = (p, f(\zeta))$ in $\mathbb{Z}[\zeta]$, where p is odd.

Output: a shortest vector in the corresponding prime ideal lattice.

- 1: Compute the ideal \mathfrak{c} generated by p and $f(\zeta)$ in $O_{\mathbb{K}}$ where $\mathbb{K} = \mathbb{Q}(\zeta^{2^{n-r}})$.
 - 2: Find a shortest vector v in the 2^r -dimensional lattice \mathfrak{c} .
 - 3: Output v .
-

The most time-consuming step in Algorithm 1 is Step 2 and the other steps can be done in $\text{poly}(2^n, \log_2 p)$ time. \square

Remark 3. By the decomposition (2) above, a similar result will hold for a prime ideal \mathfrak{p} in $O_{\mathbb{L}}$ other than $\mathbb{Q}(\zeta)$, whenever $O_{\mathbb{L}}$ is a free $O_{\mathbb{K}}$ -module where \mathbb{K} is the decomposition field of \mathfrak{p} , and some \mathbb{Z} -basis of $O_{\mathbb{K}}$ can be extended to the \mathbb{Z} -basis of $O_{\mathbb{L}}$ that determines the coefficient embedding. If we disregard the last condition that a basis of $O_{\mathbb{K}}$ extends to a basis of $O_{\mathbb{L}}$, there may be a distortion of length, depending on the basis of $O_{\mathbb{K}}$, when we lift the solution from \mathfrak{c} to \mathfrak{p} . That is, an approximation factor, which may be much larger than 1, will be involved.

Remark 4. By the remark above, solving the closest vector problem (CVP) for a prime ideal lattice can be also reduced to solving CVP in some 2^r -dimensional sublattice.

SVP of some special prime ideals in $\mathbb{Z}[\zeta_{2^{n+1}}]$ Using Theorem 5, we can prove Theorem 1, which shows that the SVP for prime ideals lying above some special rational primes is very easy.

Proof of Theorem 1

If $p \equiv -3 \pmod{8}$, we may write $p = 4m + 1$ with odd m . By Theorem 2, $x^{2^n} + 1$ is the product of 2 irreducible binomials over \mathbb{F}_p of degree 2^{n-1} : $x^{2^n} + 1 = (x^{2^{n-1}} + u_1) \cdot (x^{2^{n-1}} + u_2)$, where u_i satisfies $u_i^2 \equiv -1 \pmod{p}$.

For any prime ideal $(p, \zeta^{2^{n-1}} + u_i)$ over (p) , by the proof of Theorem 5, the shortest vector can be found by solving the 2-dimensional lattice \mathcal{L}_i generated by $\begin{pmatrix} u_i & 1 \\ -1 & u_i \\ p & 0 \\ 0 & p \end{pmatrix}$. Note that $(-1, u_i) \equiv u_i \cdot (u_i, 1) \pmod{p}$ and $(0, p) = p \cdot (u_i, 1) -$

$u_i \cdot (p, 0)$. The generator matrix can be reduced to the basis of \mathcal{L}_i as $\begin{pmatrix} u_i & 1 \\ p & 0 \end{pmatrix}$, which is exactly the Hermite Normal Form of the lattice basis.

For any vector $v \in \mathcal{L}_i$, there exists an integer vector (z_1, z_2) such that $v = (z_1, z_2) \begin{pmatrix} u_i & 1 \\ p & 0 \end{pmatrix} = (z_1 u_i + z_2 p, z_1)$. Note that

$$\|v\|^2 = (z_1 u_i + z_2 p)^2 + z_1^2 = z_1^2(u_i^2 + 1) + z_2^2 p^2 + 2p z_1 z_2 u_i \equiv 0 \pmod{p}.$$

Then for the nonzero shortest vector v , we have $0 < \|v\|^2 < \frac{4}{\pi} \cdot p < 2p$ (by Minkowski's Theorem [27]) and $\|v\|^2 \equiv 0 \pmod{p}$, which implies that $\|v\|^2 = p$.

In case $p \equiv 3 \pmod{8}$, we may write $p = 4m - 1$ with odd m . By Theorem 3, then $x^{2^n} + 1$ is the product of 2 irreducible binomials over \mathbb{F}_p of degree 2^{n-1} : $x^{2^n} + 1 = (x^{2^{n-1}} + \delta_1 x^{2^{n-2}} - 1) \cdot (x^{2^{n-1}} + \delta_2 x^{2^{n-2}} - 1)$, where δ_i satisfies $\delta_i^2 \equiv -2 \pmod{p}$ since the Dickson polynomial is $D_2(x, -1) = X^2 + 2$.

For any prime ideal $(p, \zeta^{2^{n-1}} + \delta_i \zeta^{2^{n-2}} - 1)$ over (p) , we similarly consider the shortest vector in \mathcal{L}_i generated by

$$\begin{pmatrix} -1 & \delta_i & 1 & 0 \\ 0 & -1 & \delta_i & 1 \\ -1 & 0 & -1 & \delta_i \\ -\delta_i & -1 & 0 & -1 \\ p & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ 0 & 0 & p & 0 \\ 0 & 0 & 0 & p \end{pmatrix}.$$

Similarly, we can easily get the basis for \mathcal{L}_i in the Hermite Normal Form

$$\begin{pmatrix} 0 & -1 & \delta_i & 1 \\ -1 & \delta_i & 1 & 0 \\ 0 & p & 0 & 0 \\ p & 0 & 0 & 0 \end{pmatrix},$$

and prove that for any vector $v \in \mathcal{L}$,

$$\|v\|^2 \equiv 0 \pmod{p}.$$

For the shortest vector v , by Minkowski's Theorem, we know $0 < \|v\|^2 \leq \frac{4\sqrt{2}}{\pi} < 2p$, which implies that $\|v\|^2 = p$. By Theorem 5, the proposition follows. \square

4.2 SVP average-case hardness for prime ideals in $\mathbb{Z}[\zeta]$

Precisely defining the average-case hardness of SVP for a prime ideal lattice in $\mathbb{Z}[\zeta]$ requires specifying a distribution. We consider the following three distributions.

The first distribution. To select a random prime ideal, one fixes a large M , uniformly randomly selects a prime number in the set

$$\{p \text{ is a prime} : p < M\},$$

and then uniformly randomly selects a prime ideal lying over p . This process provides a reasonable distribution among prime ideals, since every prime ideal in the ring of integers of $\mathbb{Q}[x]/(f(x))$ is of the form $(p, g(x))$, where p is a prime number and $g(x)$ is an irreducible factor of $f(x)$ over $\mathbb{F}_p[x]$. Since roughly half of all primes $p \leq M$ satisfy $p \equiv \pm 3 \pmod{8}$, according to Dirichlet's theorem on arithmetic progressions, at least half of all such p have the property that the ideals lying over p admit an efficient algorithm for SVP.

The second distribution. Again fixing a large M , we might alternatively select a prime ideal uniformly at random from the set

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

In this case, a non-negligible fraction of prime ideals admit efficient SVP algorithm. More precisely, we have

Proposition 2. *Under the distribution above, a random prime ideal of $\mathbb{Z}[\zeta]$ admits an efficient SVP algorithm with probability at least $\frac{1}{1+2^{n-1}}$.*

Proof. For simplicity, we disregard the single prime ideal lying over 2. Note that for $p = 8k \pm 3$, there are exactly two prime ideals over p , and, by Theorem 1, the SVP for the corresponding ideal lattices is easy. For $p = 8k \pm 1$, there are at most 2^n prime ideals lying over p , by Theorems 2 and 3. Then by Dirichlet's prime number theorem, even if we only count the prime ideals lying over $p = 8k \pm 3$, the fraction of easy instances is at least $\frac{1}{1+2^{n-1}}$. \square

The third distribution. The third distribution is more common in mathematics. Namely, after fixing a large M , we select uniformly at random a prime ideal from the set

$$\{\mathfrak{p} \text{ prime ideal} : \mathcal{N}(\mathfrak{p}) < M\},$$

where $\mathcal{N}(\mathfrak{p})$ is the norm of the ideal \mathfrak{p} .

By Theorem 5, SVP for a prime ideal lattice \mathfrak{p} reduces to SVP for a 2^r -dimensional sub-lattice \mathfrak{c} , where r is as defined in the statement of Theorem 5. Note that our algorithm will not improve matters if $r = n$, that is, if p splits completely in $\mathbb{Q}(\zeta)$, or equivalently if $\mathcal{N}(\mathfrak{p}) = p$. By Chebotarev's density theorem

[38], there are about $\frac{M}{2^n \log M}$ rational primes which split in $\mathbb{Q}(\zeta)$ and hence $\frac{M}{\log M}$ prime ideals lying above those primes, for which our algorithm cannot provide a reduction for SVP.

If our algorithm is to provide a reduction, the prime ideal under study must lie over a rational prime p with $p \leq \sqrt{M}$, since $\mathcal{N}(\mathfrak{p}) = p^f < M$ where f is some integer greater than 1. Hence there are at most \sqrt{M} such primes and hence at most $2^{n-1} \sqrt{M}$ prime ideals for which our algorithm provides a reduction.

Under such a distribution, therefore, the density of the easy instances for our algorithm is at most $\frac{2^{n-1} \log M}{\sqrt{M}}$, which goes to zero when M tends to infinity.

Remark 5. From a cryptographic perspective, there seems to be no construction relying on the average hardness of ideal SVP in ideals following one of the two first distributions above. However, our algorithm reveals the concrete reason why we should avoid such distributions in the cryptographic constructions although it seems very easy to sample according to the two distributions.

4.3 Solving SVP for a general ideal lattice in $\mathbb{Z}[\zeta_{2^{n+1}}]$

For simplicity, we let $\zeta = \zeta_{2^{n+1}}$. We will show that even for a general ideal lattice $\mathcal{I} \subset \mathbb{Z}[\zeta]$, there is a similar hierarchy for the hardness of SVP. We would like to stress that although the following theorem refers to the prime factorization of \mathcal{I} , the resulting algorithm does not require it.

Theorem 6. *Let \mathcal{I} be a nonzero ideal of $\mathbb{Z}[\zeta]$ with prime factorization*

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

where $\mathfrak{p}_i = (f_i(\zeta), p_i)$ for rational primes p_i , and where the \mathfrak{p}_i are not necessarily distinct. Write $p_i = 2^{A_i} \cdot m_i + 1$ when $p_i \equiv 1 \pmod{4}$ and $p_i = 2^{A_i} \cdot m_i - 1$ when $p_i \equiv 3 \pmod{4}$ with odd m_i , and let $r = \max\{r_i\}$, where

$$r_i = \begin{cases} \min\{A_i - 1, n\}, & \text{if } p_i \equiv 1 \pmod{4}; \\ \min\{A_i, n\}, & \text{if } p_i \equiv 3 \pmod{4}; \\ n, & \text{if } p_i = 2. \end{cases}$$

Then the shortest vector in the ideal lattice \mathcal{L} corresponding to \mathcal{I} can be solved via solving SVP in a 2^r -dimensional lattice.

Proof. If $r = n$, then the theorem follows simply.

If $r < n$, W.L.O.G., we assume $r = r_1$. Following the proof of Theorem 5, denote the Galois group $G = \{\sigma_1, \sigma_3, \dots, \sigma_{2^{n+1}-1}\}$ of $\mathbb{Q}(\zeta)$ over \mathbb{Q} , where $\sigma_i(\zeta) = \zeta^i$. Consider the subgroup $H = \langle \sigma_{2^{r+1}+1} \rangle$ of G generated by $\sigma_{2^{r+1}+1}$. For any $\tau \in H$ and every prime ideal $\mathfrak{p}_i = (p_i, f_i(\zeta))$, we have $\tau(\mathfrak{p}_i) = \mathfrak{p}_i$ since $\sigma_{2^{r+1}+1}(p_i) = p_i$, $\sigma_{2^{r+1}+1}(f_i(\zeta)) = f_i(\zeta)$. Note that $\mathbb{K} = \mathbb{Q}(\zeta^{2^{n-r}})$ is the fixed field of H and its integer ring $O_{\mathbb{K}}$ has a \mathbb{Z} -basis $(1, \zeta^{2^{n-r}}, \zeta^{2 \cdot 2^{n-r}}, \dots, \zeta^{(2^r-1) \cdot 2^{n-r}})$.

Let $\mathfrak{c} = \mathcal{I} \cap O_{\mathbb{K}}$. We claim that for any $a \in \mathcal{I}$, there exist $a^{(k)} \in \mathfrak{c}$ for $0 \leq k < 2^{n-r}$, such that

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

We proceed by induction. When $t = 1$ the above claim holds by Theorem 5. Suppose the claim holds for $t - 1$. Then setting $\mathcal{I} = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdots \mathfrak{p}_t$, and $\bar{\mathcal{I}} = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdots \mathfrak{p}_{t-1}$, we have $\mathcal{I} = \bar{\mathcal{I}} \cdot \mathfrak{p}_t$. For any $a \in \mathcal{I}$, we can write $a = \sum x_i y_i$ where $x_i \in \bar{\mathcal{I}}$ and $y_i \in \mathfrak{p}_t$. It suffices to show that for any xy , where $x \in \bar{\mathcal{I}}$ and $y \in \mathfrak{p}_t$, there exist $b^{(k)} \in \mathcal{I} \cap O_{\mathbb{K}}$ for $0 \leq k < 2^{n-r}$, such that $xy = \sum_{k=0}^{2^{n-r}-1} \zeta^k b^{(k)}$.

By the induction assumption, there exist $x^{(i)} \in \bar{\mathcal{I}} \cap O_{\mathbb{K}}$ for $0 \leq i < 2^{n-r}$ such that $x = \sum_{i=0}^{2^{n-r}-1} \zeta^i x^{(i)}$, and there exist $y^{(j)} \in \mathfrak{p}_t \cap O_{\mathbb{K}}$ for $0 \leq j < 2^{n-r}$ such that $y = \sum_{j=0}^{2^{n-r}-1} \zeta^j y^{(j)}$. Hence, we have

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

Let $b^{(k)} = \sum_{i+j=k} x^{(i)} y^{(j)} + \sum_{i+j=k+2^{n-r}} \zeta^{2^{n-r}} x^{(i)} y^{(j)}$ for any $0 \leq k \leq 2^{n-r} - 2$ and $b^{(2^{n-r}-1)} = \sum_{i+j=2^{n-r}-1} x^{(i)} y^{(j)}$. We have that $b^{(k)} \in \mathcal{I} \cap O_{\mathbb{K}}$ for $0 \leq k < 2^{n-r}$. Hence, for any $a \in \mathcal{I}$, there exist $a^{(k)} \in \mathfrak{c}$ for $0 \leq k < 2^{n-r}$, such that $a = \sum_{k=0}^{2^{n-r}-1} \zeta^k a^{(k)}$.

As in the proof of Theorem 5, we can show that $\lambda_1(\mathcal{I}) = \lambda_1(\mathfrak{c})$ and any nonzero shortest vector in \mathfrak{c} will yield 2^{n-r} nonzero shortest vectors in \mathcal{I} . \square

We would like to point out that in some cases, the r in Theorem 6 can be improved. Consider the case when $n \geq 3$ and $\mathcal{I} = (2, \zeta - 1)^2 = (2, \zeta^2 + 1)$. We need to solve SVP in a 2^n -dimensional lattice by Theorem 6. However, using the intermediate field $\mathbb{Q}(\zeta^2)$ as in the proof of Theorem 6, we can find a shortest vector by solving SVP in a 2^{n-1} -dimensional lattice.

Furthermore, since for any $a \in \mathcal{I}$, there exist $a^{(k)} \in \mathfrak{c}$ for $0 \leq k < 2^{n-r}$, such that $a = \sum_{k=0}^{2^{n-r}-1} \zeta^k a^{(k)}$, we conclude that if $(b^{(i)})_{0 \leq i < 2^r}$ is a basis of the ideal lattice \mathfrak{c} , then $(\zeta^j b^{(i)})_{0 \leq i < 2^r, 0 \leq j < 2^{n-r}}$ is a basis of the ideal lattice \mathcal{I} . Denote by \mathcal{L}_j the lattice generated by $(\zeta^j b^{(i)})_{0 \leq i < 2^r}$. Then we have that the ideal lattice \mathcal{I} has an orthogonal decomposition: $\mathcal{L}_0 \oplus \mathcal{L}_1 \oplus \cdots \oplus \mathcal{L}_{2^{n-r}-1}$.

In fact, for any \bar{r} , let $\mathfrak{c} = \mathcal{I} \cap O_{\mathbb{K}}$ where $\mathbb{K} = \mathbb{Q}(\zeta^{2^{n-\bar{r}}})$. For any basis $(b^{(i)})_{0 \leq i < 2^{\bar{r}}}$ of the ideal lattice \mathfrak{c} , if $(\zeta^j b^{(i)})_{0 \leq i < 2^{\bar{r}}, 0 \leq j < 2^{n-\bar{r}}}$ is a basis of the ideal lattice \mathcal{I} (meaning that the ideal lattice \mathcal{I} has an orthogonal decomposition), then the shortest vector in \mathfrak{c} is also a shortest vector in \mathcal{I} . Hence we have the following algorithm to solve SVP for a general ideal in $\mathbb{Z}[\zeta]$ without knowing the prime factorization of the ideal.

Algorithm 2 Solve SVP in general ideal lattice

Input: an ideal \mathcal{I} ;

Output: a shortest vector in the corresponding ideal lattice \mathcal{L} .

- 1: **for** $\bar{r} = 1$ to n **do**
 - 2: Compute a basis $(b^{(i)})_{0 \leq i < 2^{\bar{r}}}$ of the ideal lattice $\mathfrak{c} = \mathcal{I} \cap O_{\mathbb{K}}$, where $\mathbb{K} = \mathbb{Q}(\zeta^{2^{n-\bar{r}}})$.
 - 3: **if** $(\zeta^j b^{(i)})_{0 \leq i < 2^{\bar{r}}, 0 \leq j < 2^{n-\bar{r}}}$ is exactly a basis of ideal lattice \mathcal{I} **then**
 - 4: Find a shortest vector v in the $2^{\bar{r}}$ -dimensional lattice \mathfrak{c} ;
 - 5: Output v .
 - 6: **end if**
 - 7: **end for**
-

Note that Step 2 can be done efficiently by computing the intersection of the lattices \mathcal{I} and $O_{\mathbb{K}}$ under the coefficient embedding.

Remark 6. By the proof of Theorem 6, solving the closest vector problem (CVP) for a general ideal lattice can also be reduced to solving CVP in some 2^r -dimensional lattice.

5 Conclusion and open problems

We have investigated the SVP of prime ideal lattices in the finite Galois extension of \mathbb{Q} , and designed an algorithm exploiting the subfield structure of such fields to solve Hermite-SVP for prime ideal lattices. For the power-of-two cyclotomic fields, we obtained an efficient algorithm for solving SVP in many ideal lattices, either prime or non-prime ideals. We also determined the length of the shortest vector of those prime ideals lying over rational primes congruent to $\pm 3 \pmod{8}$. It is an interesting problem to study the length of the shortest vectors in other prime ideals. The worst case hardness of prime ideal lattice SVP for power-of-two cyclotomic fields is also left open.

Acknowledgements. We thank the anonymous referees for their valuable suggestions on how to improve this paper. This work is supported by National Key Research and Development Program of China (No. 2020YFA0712300, 2018YFA0704705), National Natural Science Foundation of China (No. 62032009, 61732021, 61572490) for Y. Pan and J. Xu, and National Science Foundation of USA (CCF-1900820) for N. Wadleigh and Q. Cheng.

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). <https://doi.org/10.1145/237814.237838>
2. 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). https://doi.org/10.1007/978-3-662-53018-4_6
3. Alkim, E., Ducas, L., Pöppelmann, T., Schwabe, P.: Newhope without reconciliation. IACR Cryptology ePrint Archive **2016**, 1157 (2016), <http://eprint.iacr.org/2016/1157>
4. Bernstein, D.J.: A subfield-logarithm attack against ideal lattices: Computing algebraic number theory tackles lattice-based cryptography. The cr.yt.to blog (2014), <https://blog.cr.yt.to/20140213-ideal.html>
5. Bernstein, D.J., Chuengsatiansup, C., Lange, T., van Vredendaal, C.: NTRU prime: Reducing attack surface at low cost. In: Proceedings of Selected Areas in Cryptography - SAC 2017. pp. 235–260 (2017). https://doi.org/10.1007/978-3-319-72565-9_12
6. Biasse, J., Espitau, T., Fouque, P., Gélín, A., Kirchner, P.: Computing generator in cyclotomic integer rings. In: Proceedings of Advances in Cryptology – EURO-CRYPT 2017. pp. 60–88 (2017). https://doi.org/10.1007/978-3-319-56620-7_3
7. Biasse, J., Song, F.: Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. In: Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2016. pp. 893–902 (2016). <https://doi.org/10.1137/1.9781611974331.ch64>
8. 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). <https://doi.org/10.1109/EuroSP.2018.00032>
9. Campbell, P., Groves, M., Shepherd, D.: Soliloquy: A cautionary tale. In: Proceedings of 2nd ETSI Quantum-Safe Crypto Workshop, Vol. 3, No. 9. pp. 1–9 (2014)
10. Cheon, J.H., Jeong, J., Changmin, L.: An algorithm for ntru problems and cryptanalysis of the ggh multilinear map without a low-level encoding of zero. LMS Journal of Computation and Mathematics **19**(A), 255–266 (2016). <https://doi.org/10.1112/S1461157016000371>
11. Cramer, R., Ducas, L., Peikert, C., Regev, O.: Recovering short generators of principal ideals in cyclotomic rings. In: Proceedings of Advances in Cryptology – EURO-CRYPT 2016. pp. 559–585 (2016). https://doi.org/10.1007/978-3-662-49896-5_20
12. 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). https://doi.org/10.1007/978-3-319-56620-7_12
13. Ducas, L., Plançon, M., Wesolowski, B.: On the shortness of vectors to be found by the ideal-SVP quantum algorithm. In: Proceedings of Advances in Cryptology – CRYPTO 2019. pp. 322–351 (2019). https://doi.org/10.1007/978-3-030-26948-7_12
14. Eisenträger, K., Hallgren, S., Kitaev, A.Y., Song, F.: A quantum algorithm for computing the unit group of an arbitrary degree number field. In: Proceedings of Symposium on Theory of Computing, STOC 2014. pp. 293–302 (2014). <https://doi.org/10.1145/2591796.2591860>

15. Hoffstein, J., Pipher, J., Silverman, J.H.: NTRU: A ring-based public key cryptosystem. In: Proceedings of Algorithmic Number Theory, Third International Symposium, ANTS-III. pp. 267–288 (1998). <https://doi.org/10.1007/BFb0054868>
16. Kirchner, P., Fouque, P.: Revisiting lattice attacks on overstretched ntru parameters. In: Proceedings of Advances in Cryptology – EUROCRYPT 2017. pp. 3–26 (2017). https://doi.org/10.1007/978-3-319-56620-7_1
17. Lenstra, A.K., Lenstra, H.W., Lovász, L.: Factoring polynomials with rational coefficients. *Mathematische Annalen* **261**(4), 515–534 (1982). <https://doi.org/10.1007/BF01457454>
18. Lidl, R., Niederreiter, H.: Finite Fields, *Encyclopedia of Mathematics and Its Applications*, vol. 20. Cambridge University Press, 2nd edn. (1997). [https://doi.org/10.1016/s0898-1221\(97\)84597-x](https://doi.org/10.1016/s0898-1221(97)84597-x)
19. Lovasz, L.: An algorithmic theory of numbers, graphs, and convexity, CBMS-NSF regional conference series in applied mathematics, vol. 50. Society for Industrial and Applied Mathematics (1986). <https://doi.org/10.1137/1.9781611970203>
20. Lu, X., Liu, Y., Zhang, Z., Jia, D., Xue, H., He, J., Li, B.: LAC: practical Ring-LWE based public-key encryption with byte-level modulus. *IACR Cryptology ePrint Archive* **2018**, 1009 (2018), <https://eprint.iacr.org/2018/1009>
21. Lyubashevsky, V., Micciancio, D.: Generalized compact knapsacks are collision resistant. In: Proceedings of Automata, Languages and Programming, 33rd International Colloquium, ICALP 2006. pp. 144–155 (2006). https://doi.org/10.1007/11787006_13
22. 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). https://doi.org/10.1007/978-3-642-13190-5_1
23. Marcus, D.A.: *Number Fields*. Universitext, Springer, 2nd edn. (2018). <https://doi.org/10.1007/978-1-4684-9356-6>
24. Meyn, H.: Factorization of the cyclotomic polynomials $x^{2^n} + 1$ over finite fields. *Finite Fields Appl.* **2**, 439–442 (1996). <https://doi.org/10.1017/CBO9780511525926>
25. Micciancio, D.: Generalized compact knapsacks, cyclic lattices, and efficient one-way functions from worst-case complexity assumptions. In: Proceedings of 43rd Symposium on Foundations of Computer Science (FOCS 2002). pp. 356–365 (2002). <https://doi.org/10.1109/SFCS.2002.1181960>
26. Micciancio, D.: Generalized compact knapsacks, cyclic lattices, and efficient one-way functions. *Computational Complexity* **16**(4), 365–411 (2007). <https://doi.org/10.1007/s00037-007-0234-9>
27. Micciancio, D., Goldwasser, S.: *Complexity of Lattice Problems: a cryptographic perspective*, The Kluwer International Series in Engineering and Computer Science, vol. 671. Kluwer Academic Publishers (2002). <https://doi.org/10.1007/978-1-4615-0897-7>
28. Neukirch, J.: *Algebraic Number Theory*, *Grundlehren der mathematischen Wissenschaften*, vol. 322. Springer, 1st edn. (1999). <https://doi.org/10.1007/978-3-662-03983-0>
29. P, S.N., Vercauteren, F.: Fully homomorphic encryption with relatively small key and ciphertext sizes. In: Proceedings of International Workshop on Public Key Cryptography - PKC 2010. pp. 420–443 (2010). https://doi.org/10.1007/978-3-642-13013-7_25
30. 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). <https://doi.org/10.1145/3055399.3055489>
31. Peikert, C., Rosen, A.: Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. In: Proceedings of Theory of Cryptography, Third Theory of Cryptography Conference, TCC 2006. pp. 145–166 (2006). https://doi.org/10.1007/11681878_8
 32. Pellet-Mary, A., Hanrot, G., Stehlé, D.: Approx-SVP in ideal lattices with pre-processing. In: Proceedings of Advances in Cryptology – EUROCRYPT 2019. pp. 685–716 (2019). https://doi.org/10.1007/978-3-030-17656-3_24
 33. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM* **56**(6), 1–40 (2009). <https://doi.org/10.1145/1568318.1568324>, preliminary version in STOC’05
 34. Schnorr, C., Euchner, M.: Lattice basis reduction: Improved practical algorithms and solving subset sum problems. *Math. Program.* **66**, 181–199 (1994). <https://doi.org/10.1007/BF01581144>
 35. Schnorr, C.P., Euchner, M.: Lattice basis reduction: Improved practical algorithms and solving subset sum problems. *Mathematical programming* **66**(1-3), 181–199 (1994). <https://doi.org/10.1007/BF01581144>
 36. Stehlé, D., Steinfeld, R.: Making NTRU as secure as worst-case problems over ideal lattices. In: Proceedings of Advances in Cryptology – EUROCRYPT 2011. pp. 27–47 (2011). https://doi.org/10.1007/978-3-642-20465-4_4
 37. Stehlé, D., Steinfeld, R., Tanaka, K., Xagawa, K.: Efficient public key encryption based on ideal lattices. In: Proceedings of Advances in Cryptology – ASIACRYPT 2009. pp. 617–635 (2009). https://doi.org/10.1007/978-3-642-10366-7_36
 38. Tschebotareff, N.: Die bestimmung der dichtigkeit einer menge von primzahlen, welche zu einer gegebenen substitutionsklasse gehören. *Mathematische Annalen* **95**(1), 191–228 (1926). <https://doi.org/10.1007/BF01206606>

A The subfields of $\mathbb{Q}(\zeta_{2^n})$

Now we sketch the subfield lattice of $\mathbb{Q}(\zeta_{2^{n+1}})$. Consider the three subfields

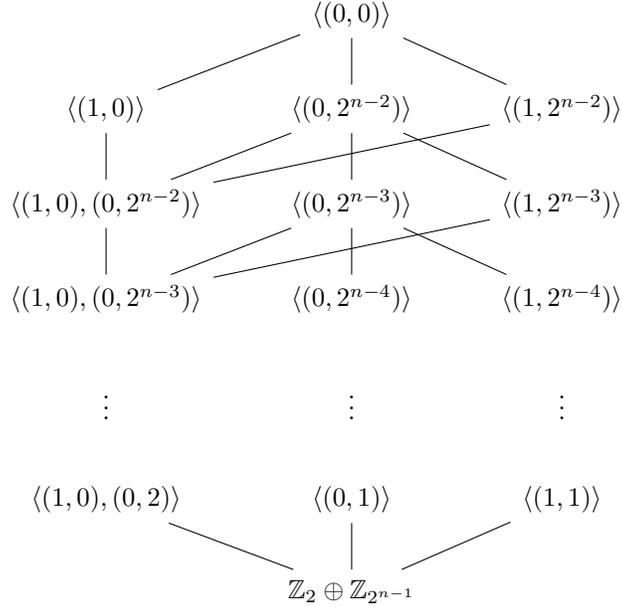
$$\mathbb{Q}(\zeta_{2^{n+1}} + \zeta_{2^{n+1}}^{-1}), \mathbb{Q}(\zeta_{2^n}), \mathbb{Q}(\zeta_{2^{n+1}} - \zeta_{2^{n+1}}^{-1}).$$

First we claim $\mathbb{Q}(\zeta_{2^{n+1}})$ is degree two over each. On the one hand, all are proper subfields since $\mathbb{Q}(\zeta_{2^{n+1}} + \zeta_{2^{n+1}}^{-1})$ is contained in the fixed field of the automorphism $\zeta_{2^{n+1}} \mapsto \zeta_{2^{n+1}}^{-1}$, and $\mathbb{Q}(\zeta_{2^{n+1}} - \zeta_{2^{n+1}}^{-1})$ is in the fixed field of the automorphism $\zeta_{2^{n+1}} \mapsto -\zeta_{2^{n+1}}^{-1}$. On the other hand, $\zeta_{2^{n+1}}$ is a root of the quadratic polynomials $x^2 - (\zeta_{2^{n+1}} + \zeta_{2^{n+1}}^{-1})x + 1 \in \mathbb{Q}(\zeta_{2^n} + \zeta_{2^{n+1}}^{-1})[x]$ and $x^2 - (\zeta_{2^{n+1}} - \zeta_{2^{n+1}}^{-1})x - 1 \in \mathbb{Q}(\zeta_{2^{n+1}} - \zeta_{2^{n+1}}^{-1})[x]$.

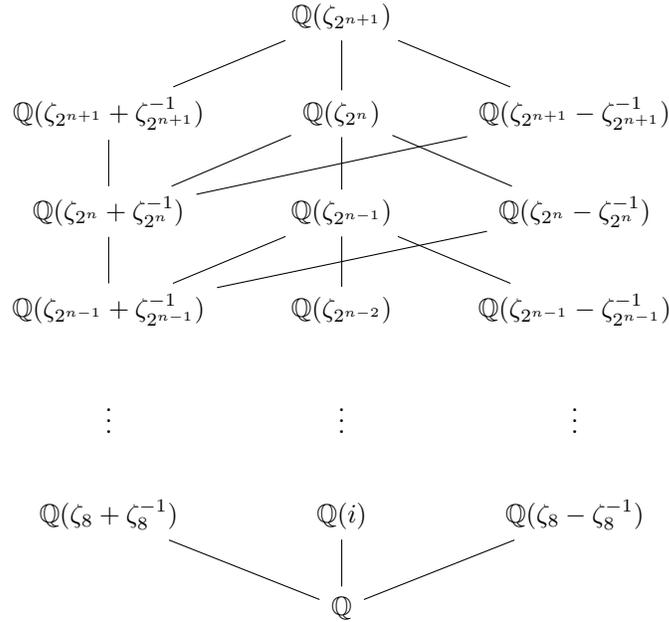
Moreover, since the involutions

$$\zeta_{2^{n+1}} \mapsto \zeta_{2^{n+1}}^{-1}, \zeta_{2^{n+1}} \mapsto \zeta_{2^{n+1}}^{2^{n-1}+1}, \zeta_{2^{n+1}} \mapsto -\zeta_{2^{n+1}}^{-1}$$

are distinct, these three subfields are distinct. Finally it is routine to sketch the subgroup lattice of $\mathbb{Z}_2 \oplus \mathbb{Z}_{2^{n-1}} \cong (\mathbb{Z}/2^{n+1}\mathbb{Z})^* \cong \text{Gal}(\mathbb{Q}(\zeta_{2^{n+1}})/\mathbb{Q})$:



Here all lines indicate extensions of index two. Combining these facts we have the subfield lattice for $\mathbb{Q}(\zeta_{2^n})$:



where all lines indicate extensions of order two.

B Decomposition groups and fixed fields

Let $\zeta = \zeta_{2^{n+1}}$, p a rational prime with $p \equiv 3 \pmod{4}$, A the natural number with $2^A \parallel p+1$, and let \mathfrak{p} be a prime ideal in $\mathbb{Z}[\zeta]$ containing p . Then

$$\mathfrak{p} = (p, \zeta^{2^{n-A+1}} + \delta\zeta^{2^{n-A}} - 1)$$

for some $\delta \in \mathbb{Z}$. Let $\sigma \in \text{Aut}(\mathbb{Q}(\zeta)/\mathbb{Q})$ be the automorphism of $\mathbb{Q}(\zeta)$ with $\zeta \mapsto \zeta^{-2^A-1}$. Then we have

$$\begin{aligned} \sigma\mathfrak{p} &= (p, \sigma(\zeta)^{2^{n-A+1}} + \delta\sigma(\zeta)^{2^{n-A}} - 1) \\ &= (p, \zeta^{2^{n-A+1}(-2^A-1)} + \delta\zeta^{2^{n-A}(-2^A-1)} - 1) \\ &= (p, \zeta^{-2^{n+1}}\zeta^{-2^{n-A+1}} + \delta\zeta^{-2^n}\zeta^{-2^{n-A}} - 1) \\ &= (p, \zeta^{-2^{n-A+1}} - \delta\zeta^{-2^{n-A}} - 1) \\ &= (p, -\zeta^{-2^{n-A+1}} \cdot (\zeta^{2^{n-A+1}} + \delta\zeta^{2^{n-A}} - 1)) \\ &= \mathfrak{p}. \end{aligned}$$

We have used the fact that ζ is a unit in $\mathbb{Z}[\zeta]$.

Since $\zeta \mapsto \zeta^{-1}$ is an involution, the order of σ is the order of $\zeta \mapsto \zeta^{2^A+1}$ (denoted by σ') which is the multiplicative order of $2^A + 1$ in $(\mathbb{Z}/2^{n+1}\mathbb{Z})^*$. We claim that, for $A \geq 2$, this order is 2^{n+1-A} : First note that for $k \equiv 1 \pmod{4}$,

$$\text{ord}_{(\mathbb{Z}/2^{n+1}\mathbb{Z})^*}(k) = 2^m$$

if and only if $2^{n+1} \parallel k^{2^m} - 1$. This fact follows easily from the identity

$$k^{2^{g+1}} - 1 = (k^{2^g} - 1)(k^{2^g} + 1)$$

and the fact that for $k = 2^A + 1$, we have $2 \parallel (k^{2^g} + 1)$. Now, that the multiplicative order of $2^A + 1$ is 2^{n+1-A} follows from an induction argument using the above identity.

The preceding two paragraphs prove that σ lies in the decomposition group of \mathfrak{p} and that σ has order 2^{n+1-A} . It follows from a standard result in the theory of number fields that the decomposition group of \mathfrak{p} has order 2^{n+1-A} . Thus $\langle \sigma \rangle$ is precisely the decomposition group of \mathfrak{p} . Now recall the subfield/subgroup lattice for $\mathbb{Q}(\zeta)/\mathbb{Q}$ and its Galois group $\mathbb{Z}_{2^{n+1}}^*$. A simple computation shows that σ fixes $\zeta^{2^{n-A}} - \zeta^{-2^{n-A}}$. But from the subfield lattice we can see that

$$[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta^{2^{n-A}} - \zeta^{-2^{n-A}})] = 2^{n+1-A} = |\langle \sigma \rangle|.$$

Thus $\mathbb{Q}(\zeta^{2^{n-A}} - \zeta^{-2^{n-A}})$ is precisely this fixed field.

A similar, in fact easier, analysis can be carried out for $p \equiv 1 \pmod{4}$. In this case

$$\mathfrak{p} = (p, \zeta^{2^{n-A+1}} - u)$$

for some $u \in \mathbb{Z}$ and $2^A \parallel p - 1$. Then it is seen that σ' fixes \mathfrak{p} . As in the 3 (mod 4) case, we know from a general result of algebraic number theory that the decomposition group of \mathfrak{p} has order 2^{n+1-A} , which matches the order of σ' (computed above). We see that $\mathbb{Q}(\zeta^{2^{n+1-A}})$ is contained in the fixed field of σ' , and again, by looking at the subfield lattice to find $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta^{2^{n+1-A}})] = 2^{n+1-A}$, we see that $\mathbb{Q}(\zeta^{2^{n+1-A}})$ is precisely the fixed field of the decomposition group of \mathfrak{p} .