Quantum Information and Computation, Vol. 24, No. 15&16 (2024) 1313–1324

UPPER BOUNDING THE QUANTUM SPACE COMPLEXITY FOR COMPUTING CLASS GROUP AND PRINCIPAL IDEAL PROBLEM

IU-IONG NG
Graduate School of Mathematics, Nagoya University
Furo-cho, Chikusa-ku, Nagoya 464-8602, Japan

Received February 19, 2024
Revised December 30, 2024

In this paper, we calculate the upper bound on quantum space complexity of the quantum algorithms proposed by Biasse and Song (SODA'16) for solving class group computation and the principal ideal problem using the reductions to S-unit group computation. We follow the approach of Barbulescu and Poulalion (AFRICACRYPT'23) and the framework given by de Boer, Ducas, and Fehr (EUROCRYPT'20) and Eisenträger, Hallgren, Kitaev, and Song (STOC'14).

Keywords: Quantum space complexity, Principal ideal problem, S-unit group computation

1 Introduction

1.1 Number theoretical problems

The computation of number theoretical problems, or the computational number theory, is important both as a field of mathematics and in terms of applications, such as developing algorithms and cryptography. The main objects in these number theoretical problems are number fields, i.e., finite extensions of the field of rational numbers $\mathbb{Q}$, and their ring of integers. Most quantum algorithms have the running time exponentially better than the best known classical algorithms for addressing several theoretical problems or their applications. There are some problems which are believed to be hard classically but have polynomial quantum algorithms solving them, for example, integer factorisation and discrete logarithm [1], and the problems for general number fields, like the unit group computation [2, 3], the principal ideal problem [4, 5], and the ideal class group computation [2, 5] assuming the Generalised Riemann Hypothesis. These quantum algorithms can be reduced to a type of problem, the hidden subgroup problems (HSP), that find the subgroup hidden as the period of a function.

In this work, we focus on the quantum space complexity of ideal class group computation and solving the principal ideal problem. The ideal class group, or simply the class group, of a number field is the finite abelian group consisting of the equivalent classes of fractional ideals of the ring of integers. One can also define the class group for an ideal of the ring of integers as the finite abelian group consisting of invertible fractional ideals of the order. Class groups appear in many significant problems in number theory, for instance, factoring large integers and determining principal ideals in a cyclotomic field. The computation of ideal class groups is also commonly used in other number theoretical tasks such as computing other

objects of the number field like ray class group, relative class group, and unit group [6, 7], or in problems like finding Bach's bound on the maximum norm of the generators [8]. There is also a close relation to cryptography, for example, the classical subexponential classical algorithm for integer factorisation [9], and some curve-based cryptography [10] that include finding relations between elements in the class group.

An ideal is principal if it can be generated by a single element. The principal ideal problem (PIP) determines whether the input ideal is principal and finds a generator. Like the class group computation, PIP has applications in computing ray class groups, relative class groups, unit groups, and S-class groups. Problems such as lattice isomorphism and matrix similarity can be efficiently reduced to deciding whether an ideal is principal [11]. Since many cryptographic schemes use principal ideals generated by a short element, PIP is also related to lattice-based cryptography. Recently, it has been shown that solving PIP in polynomial time directly induces a polynomial time attack on schemes relying on the hardness of finding the short generator of a principal ideal [12].

1.2 Quantum algorithms for number theoretical problems

Instead of the ordinary HSP, most recent quantum algorithms for number theoretical problems are based on a framework called the continuous hidden subgroup problem (CHSP), proposed by Eisenträger, Hallgren, Kitaev, and Song [3] as a generalisation of HSP to the group $\mathbb{R}^m$ for some non-constant dimension m. As an application, [3] applied CHSP to solve the unit group problem in polynomial time by constructing an oracle that maps from a group containing the unit group to a group of ideals and then to a field of quantum states. Recently, Barbulescu and Poulalion [13] applied the complexity framework proposed by [14] on the unit group oracle to analyse the space complexity of the unit group algorithm and propose a modified algorithm for a special case in cyclotomic fields.

Theorem 1 ([13, Corollary 37]) *Let K be a number field of discriminant Δ and unit rank m. For any error bound $\tau > 0$, there exists a quantum algorithm running in time* $\mathrm{poly}(m, \log|\Delta|, \log\tau)$ *using a number of qubits $O(m^5 + m^4 \log|\Delta|) + O(m \log\tau^{-1})$ which outputs a set of generators for the unit group of K.*

Other important applications on the CHSP are given by Biasse and Song [5], which gave a polynomial time quantum algorithms for computing class groups and solving PIP in arbitrary degree number fields by reducing the problems to a problem computing the S-unit group. Notice that the previous works by Hallgren, the polynomial time algorithms for class group computation [2] and for PIP for constant degree number fields [4], utilise the HSP algorithms but not CHSP. The S-unit group problem can be viewed as a generalisation of the unit group problem with $|S|$ more parameters. Hence, [5] follows the way of defining the oracle for unit groups and extends it to the one for S-unit groups, which makes it possible to reduce the S-unit group computation to CHSP. A well-known application of the PIP algorithm is the polynomial time quantum algorithm finding the shortest vector[a] in an ideal lattice (ideal-SVP) proposed by Cramer, Ducas, and Wesolowski [15], which applies the PIP algorithm and a variant of class group computation as dominant parts. For the applications in cryptography,

[a] The length of the shortest vector is called the minimum distance or the first successive minima.

since some schemes for post-quantum cryptography rely on the hardness of PIP, [5] indeed broke some cryptography systems from a theoretical point of view. Nevertheless, a precise estimation of the quantum time or space complexity is essential in evaluating the threat raised by the quantum algorithm rather than only knowing it runs in polynomial time.

1.3 Our results

In this work, we follow the way in [13] of calculating the space complexity of the unit group algorithm, apply the framework provided by [14] on the oracle for S-unit groups, which is defined in [5], and derive the space complexity for the S-unit group algorithm.

Theorem 2 *Let K be a number field of discriminant Δ and unit rank m, and let S be a set of prime ideals such that $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$. For any error bound $\tau > 0$, the S-unit group computation algorithm from [5] (Theorem 5) uses*

$$O(m^5 + m^4 \log|\Delta| + m^4 \sum_{j=1}^{k} \log \mathcal{N}(\mathfrak{p}_j)) + O(m \log \tau^{-1})$$

qubits, where $\mathcal{N}(\cdot)$ is the ideal norm.

Since the unit rank m has the same order as the degree n, we can rewrite it in the notations as [5] with a maximum.

Corollary 1 *The S-unit group computation algorithm from [5] (Theorem 5) uses $O(n^5 + n^4 \log|\Delta| + n^4 \cdot |S| \cdot \max_{\mathfrak{p}\in S}\{\log \mathcal{N}(\mathfrak{p})\}) + O(n \log \tau^{-1})$ qubits.*

Our result can be viewed as a generalisation of the space complexity given by [13] by taking the set S to be empty. Applying our result to the PIP quantum algorithm derived by [5], which with an input ideal $\mathfrak{a}$ runs in polynomial time in the parameters $n, \log \mathcal{N}(\mathfrak{a}), \log|\Delta|$, we obtain the quantum space complexity for PIP.

Corollary 2 *The principal ideal problem algorithm ([5, Theorem 1.3]) uses $O(n^5 + n^4 \log|\Delta| + n^4 \log \mathcal{N}(\mathfrak{a}))$ qubits.*

From this result, we expect the number of qubits used for PIP or its applications, e.g., ideal-SVP, to be large with respect to the degree of the input number field. Therefore, our results indicate that, in general, implementing these algorithms may require a large-scale quantum computer.

2 Preliminaries

2.1 Number field

We follow the definitions in [5]. Let K be a number field with degree n, i.e., $n = [K : \mathbb{Q}]$. Denote by n_1 and n_2 the number of real embeddings and the number of pairs of complex embeddings, respectively. Then $n = n_1 + 2n_2$ and the unit rank of K is defined as $m =$

$n_1 + n_2 - 1$. The absolute norm of an element $x \in K$ is defined as $\mathcal{N}(x) \coloneqq \prod_\sigma \sigma(x) \in \mathbb{Q}$, where σ denotes the n embeddings.

We denote the ring of integers of K by $\mathcal{O}$. Notice that every ring of integers of a number field is a Dedekind ring, and which implies that any ideal I of $\mathcal{O}$ can be uniquely factored into a product of powers of prime ideals, i.e., $I = \prod \mathfrak{p}^{v_\mathfrak{p}(I)}$ with $v_\mathfrak{p}(I) \in \mathbb{Z}$ and only finitely many of them are non-zero. The norm of an ideal is defined by $\mathcal{N}(I) = |\mathcal{O}/I|$, and if it is a principal ideal such that $I = (\alpha)$, then $\mathcal{N}(I) = \mathcal{N}(\alpha)$. The unit group $\mathcal{O}^*$ consists of invertible elements, i.e., the units, in $\mathcal{O}$. For $\alpha \in \mathcal{O}^*$, $(\alpha) = \mathcal{O}$.

2.1.1 S-unit group

We now define the S-unit group. The definition is equivalent to the one in [5]. We refer to [16] for more details. For a Dedekind domain o, define $o(X) = \{\frac{f}{g} \mid f, g \in o, g \not\equiv 0 \mod \mathfrak{p} \text{ for } \mathfrak{p} \in X\}$, where X is a set of nonzero prime ideals of o which contains almost all prime ideals of o. Let $S = \{\mathfrak{p}_1, \dots \mathfrak{p}_k\}$ be a finite set of prime ideals of $\mathcal{O}$, and let X_S be the set of all prime ideals that do not belong to S. The ring $\mathcal{O}(X_S)$ has the units called the S-units. If $S = \emptyset$, it turns out that $\mathcal{O}(X_S) = \mathcal{O}$, which is the special case that the S-units are exactly the units.[b] Otherwise, the S-units are the elements $\alpha \in K$ such that $(\alpha) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_k^{e_k}$ for some $e_1, \dots, e_k \in \mathbb{Z}$. Then the S-units form a multiplicative group $U(S)$ and satisfy that for $\alpha \in U(S)$,

$$\alpha \cdot \mathcal{O} \cdot \mathfrak{p}_1^{-v_{\mathfrak{p}_1}(\alpha)} \cdots \mathfrak{p}_k^{-v_{\mathfrak{p}_k}(\alpha)} = \mathcal{O}. \tag{1}$$

2.1.2 E-ideals

We denote $E = \mathbb{R}^{n_1} \times \mathbb{C}^{n_2}$ to be the field for K under canonical embeddings, i.e., for $z \in K$, $(\sigma_1(z), \dots, \sigma_{n_1+n_2}(z)) \in E$, which is called the conjugate vector representation. Since $\mathcal{O}$ has the structure as a $\mathbb{Z}$-lattice, its image under the embedding $K \to E$, which we denote by $\underline{\mathcal{O}}$, inherits the lattice structure and can be identified as an $\mathbb{R}^n$-lattice. So do the fractional ideals of $\mathcal{O}$ with lattice structures correspond to fractional ideals (lattices) in E.

Definition 1 ([5, Definition 2.1]) *An E-ideal is a lattice $\Lambda \subseteq E$ such that $\forall x \in \underline{\mathcal{O}}, x\Lambda \subseteq \Lambda$.*

Here state two theorems related to E-ideals that will be used in our proofs.

Theorem 3 ([18, Theorem 2.4.13]) *Let L be a $\mathbb{Z}$-submodule of a free module $\tilde{L}$ and of the same rank. Then there exist positive integers $d_1, \dots, d_n$ satisfying the following conditions:*

1. *For every i such that $1 \leq i < n$ we have $d_{i+1} | d_i$.*
2. *$[\tilde{L} : L] = d_1 \cdots d_n$.*
3. *There exists a $\mathbb{Z}$-basis $(v_1, \dots v_n)$ of $\tilde{L}$ such that $(d_1 v_1, \dots, d_n v_n)$ is a $\mathbb{Z}$-basis of L.*

Furthermore, the d_i are uniquely determined by L and $\tilde{L}$.

[b] For the definition for S-units given by the valuations or places, it is the case that when $S = S_\infty$, the Archimedean valuations or infinite places, then the S-units are the units. See, for example, [17].

Theorem 4 ([18, Theorem 4.7.4]) *Let M be a module with denominator 1 with respec to a given R (i.e. $M \subset R$), and $W = (w_{i,j})$ its Hermite normal form (HNF) with respect to a basis $\alpha_1, \ldots, \alpha_n$ of R. Then the product of the $w_{i,i}$ (i.e. the determinant of W) is equal to the index $[R : M]$.*

2.2 The unit group computation algorithm

In this subsection, we review the ideas for the unit group algorithm from [3]. By the properties of units, one can identify $\mathcal{O}^*$ as a subgroup of $\hat{G} = \mathbb{R}^{n_1+n_2-1} \times \mathbb{Z}_2^{n_1} \times (\mathbb{R}/\mathbb{Z})^{n_2}$. To see this, we consider the mapping $\varphi : \hat{G} \to E$ translating between the log coordinates and the conjugate vector representation.

$$\begin{aligned}\varphi :&(u_1, \ldots, u_{n_1+n_2}, \mu_1, \ldots, \mu_{n_1}, \theta_1, \ldots, \theta_{n_2}) \\ &\mapsto ((-1)^{\mu_1} e^{u_1}, \ldots, (-1)^{\mu_{n_1}} e^{u_{n_1}}, e^{2\pi i\theta_1} e^{u_{n_1+1}}, \ldots, e^{2\pi i\theta_{n_2}} e^{u_{n_1+n_2}}).\end{aligned}$$

Since the units are the elements $z \in \mathcal{O}$ with $\mathcal{N}(z) = \pm 1$, for a unit written as $z = e^{\boldsymbol{u}}\boldsymbol{v}$, where $\boldsymbol{u} \in \mathbb{R}^{n_1+n_2}$, it satisfies that $\sum_{j=1}^{n_1+n_2} u_j = 0$, and hence $\mathbb{R}^{n_1+n_2-1}$ is enough for the presentation of units.

The oracle function defined in [3] is a composition of two mappings:

$$\mathcal{F} : \hat{G} \xrightarrow{f_c} \{E\text{-ideals}\} \xrightarrow{f_q} \{\text{quantum states}\},$$

where f_q encodes a lattice L into a quantum state $|L\rangle$ so that it provides a canonical representation for lattices, and f_c map an element of $\hat{G}$ to the principal ideal generated by it.

2.3 The S-unit group computation algorithm

Theorem 5 ([5, Theorem 1.1]) *There is a quantum algorithm for computing the S-unit group of a number field K in compact representation which runs in polynomial time in the parameters $n = \deg(K), \log|\Delta|, |S|$ and $\max_{\mathfrak{p}\in S}\{\log(\mathcal{N}(\mathfrak{p}))\}$, where Δ is the discriminant of the ring of integers of K.*

One of the contributions by [5] is showing how to get an exact compact representation of the desired field element, which is processed classically. Notice that similar to the unit group, the S-unit group can be identified as a subgroup of $G = \hat{G} \times \mathbb{Z}^{|S|} = \mathbb{R}^{n_1+n_2-1} \times \mathbb{Z}_2^{n_1} \times (\mathbb{R}/\mathbb{Z})^{n_2} \times \mathbb{Z}^{|S|}$, where $\mathbb{Z}^{|S|}$ corresponds the valuations (exponents) of the prime ideals in S. The algorithm for Theorem 5 applies the CHSP framework from [3] with an HSP oracle

$$\mathcal{F}' : G \xrightarrow{f_c'} \{E\text{-ideals}\} \xrightarrow{f_q} \{\text{quantum states}\},$$

where f_c' is defined as

$$f_c'(\boldsymbol{y}, v_1, \ldots, v_{|S|}) = \varphi(\boldsymbol{y}) \cdot \underline{\mathcal{O}} \cdot \mathfrak{p}_1^{-v_1} \cdots \mathfrak{p}_{|S|}^{-v_{|S|}},$$

and f_q is defined as the one in [3], which can be extended from E-integral ideals to E-fractional ideals. By the property of S-units, $\mathcal{F}'$ hides the subgroup of G, denoted by $U(S)$, identified as the S-unit group. The periodicity of f_c' on $U(S)$ is proved by Proposition 5.1 in [5]. We rephrase it as follows.

Proposition 6 ([5, Proposition 5.1]) *For any $(y,(v_j))$ and $(y',(v'_j))$, let $(u,(w_j)) = (y',(v'_j)) - (y,(v_j))$. Then the function f'_c satisfies that*

$$f'_c(y',(v'_j)) = f'_c(y,(v_j)) \Leftrightarrow \varphi(u) \in U(S).$$

In particular, $v_{\mathfrak{p}_j}(\varphi(u)) = w_j, \forall j = 1,\ldots,|S|$ if $\varphi(u) \in U(S)$.

Distances. In Section A.3 of [3], the distance between two lattices is defined as the geodesic distance on the group $\mathrm{GL}_n(\mathbb{R})$ between their bases matrices B and B'. Here, to specify the distance by lattice but not its bases, we modify the definition as stated below.

Definition 2

$$\mathrm{dist}_g(L,L') \coloneqq \inf\{\|A\|_2 : e^A B_{L'} = B_L, B_L \text{ and } B_{L'} \text{ are bases for } L \text{ and } L', \text{ respectively}\},$$

where $\|(a_{jk})\|_2 = \sqrt{\sum_{j,k} |a_{jk}|^2}$.

On the other hand, the definition of the distance for the elements in the domain in [5] and for the lattices are defined as follows.

Definition 3 ([5, Definition 5.2]) *Let $(z,(v_j)_{j\le|S|})$ and $(z',(v'_j)_{j\le|S|})$, we define their distance in $G/U(S)$, $\mathrm{dist}_{G/U(S)}((z,(v_j)),(z',(v'_j)))$, by*

$$\inf\{\|a\| + \sum_j |w_j| e_j \log(p_j) \text{ such that } (z',(v'_j)_{j\le|S|}) = (z,(v_j)_{j\le|S|}) + (a,(w_j)) + u, u \in U(S)\},$$

where $\|a\|$ is the Euclidean norm of the vector corresponding to a in $\mathbb{R}^{n_1+n_2} \times \mathbb{Z}_2^{n_1} \times (\mathbb{R}/\mathbb{Z})^{n_2}$. The p_j, e_j are defined as $\mathcal{N}(\mathfrak{p}_j) = p_j^{e_j}$.

Definition 4 ([5, Definition 5.3])

$$\mathrm{dist}(L,L') = \inf\left\{ \|a\| + \sum_j \log(d_j) + n\log(d) \text{ such that } L_\Delta = e^{\mathrm{diag}(a_j)} B_\omega \,\mathrm{diag}(d_j/d) \right\},$$

where L_Δ runs over all the matrices of a basis of L'/L such that there is a matrix B_ω of an integral basis of $\mathcal{O}$, $d_j, d \in \mathbb{Z}_{>0}$, and $\|a\|$ is the Euclidean norm of the vector $a \in \mathbb{R}^{n_1+n_2} \times \mathbb{Z}_2^{n_1} \times (\mathbb{R}/\mathbb{Z})^{n_2}$ corresponding to $(a_j)_{j\le n} \in E$ satisfying $L_\Delta = e^{\mathrm{diag}(a_j)} B_\omega \,\mathrm{diag}(d_j/d)$.

The definition for L'/L is not explicitly stated in [5], but it can be realised from the statements and proofs in the paper as $L'/L = \varphi(z'-z)\mathcal{O}\prod \mathfrak{p}_j^{-(v'_j - v_j)}$.

2.4 Complexity of the CHSP framework

The complexity of the CHSP framework from [3] is studied in [14, 13]. An HSP oracle hiding L on $\mathbb{R}^m$ for some positive integer m is defined as follows.

Definition 5 ([3, Definition 1.1]) *A function $f : \mathbb{R}^m \to H$, where H is the set of unit vectors in some Hilbert space, is said to be an (a, r, ϵ)-HSP oracle of the full-rank lattice $L \subset \mathbb{R}^m$ if*

1. *f is periodic on L;*
2. *f is a-Lipschitz;*
3. *For all $x, y \in \mathbb{R}$ such that $\mathrm{dist}_{\mathbb{R}^m/L}(x, y) \geq r$, it holds that $|\langle f(x)|f(y)\rangle| \leq \epsilon$.*

Theorem 1 from [13] calculates the space complexity for the unit group algorithm from [3]. According to [13, Lemma 21, Lemma 34 and Corollary 37], one can obtain that $O(\log(1/\lambda_1^*)) = O(m + \frac{1}{m}\log|\Delta|)$, where λ_1^* is the first successive minima of the dual lattice of L, and the following corollary on the complexity of the CHSP framework applied on an HSP oracle f.

Corollary 3 ([13]) *Given access to an HSP oracle f, the CHSP algorithm uses*

$$O(m^3 \log \mathrm{Lip}(f) + m^4 \log|\Delta|) + O(m \log \tau^{-1})$$

qubits.

In [14], the algorithm of [3] is rigorously analysed (and modified) as follows. The oracle function is considered on a restricted domain $\mathbb{D}^m := \left(\frac{1}{q}\mathbb{Z}^m\right)/\mathbb{Z}^m$ with the parameter q relating to the space complexity, and H is a subset of a Hilbert space of dimension 2^n. The input state is a Gaussian superposition over the representatives $x \in \mathbb{D}^m_{\mathrm{rep}} := \frac{1}{q}\mathbb{Z}^m \cap [-\frac{1}{2}, \frac{1}{2})^m$ of $\mathbb{D}^m$ with the parameter $s \in \mathbb{R}$. The algorithm has oracle access to f which maps $|x\rangle|0\rangle$ to $|x\rangle|f(Vx)\rangle$ with the parameter $V \in \mathbb{R}$. The first register uses $m \log q$ qubits, and the second register uses N qubits. Reference [14] denotes that $\log q =: Q$ and gives the number of qubits needed for the oracle as follows.

Theorem 7 ([14, Theorem 2]) *There exists dual lattice sampler quantum algorithm with the error parameter $\eta > 0$ and the relative distance parameter $1/2 > \delta > 0$ which uses one quantum oracle call to f, $Qm + N$ qubits, where*

$$Q = O\left(m \log\left(m \log \frac{1}{\eta}\right)\right) + O\left(\log\left(\frac{\mathrm{Lip}(f)}{\eta\delta\lambda_1^*}\right)\right). \tag{2}$$

Later in [13, Corollary 37], the number of qubits for the second register is claimed that one stores the values of f on Qm qubits.

Lipschitz constant. Consider the quantum encoding part, f_q, in the oracle functions for both the unit group algorithm and the S-unit group algorithm. The Lipschitz continuity for f_q is proven as stated below.

Theorem 8 ([3, Theorem D.4]) $\| |f_q(L)\rangle - |f_q(L')\rangle \| \leq \mathrm{Lip}(f_q) \cdot \mathrm{dist}_g(L, L')$.

From this result, [3] derived the value of $\mathrm{Lip}(\mathcal{F})$, and the order of $\log \mathrm{Lip}(\mathcal{F})$ is given in [13].

Theorem 9 ([13, Theorem 36]) $\log_2 \mathrm{Lip}(\mathcal{F}) = O(m^2 + m \log |\Delta|)$.

3 Proof for the main theorem

To prove Theorem 2, we need the Lipschitz constant for $\mathcal{F}'$. Since the Lipschitz constants depend on the distance chosen, the approach is to calculate the Lipschitz constant for f'_c with the distance $\mathrm{dist}(\cdot, \cdot)$ between the ideals (Lemma 2), and the relation between distances $\mathrm{dist}(\cdot, \cdot)$ and $\mathrm{dist}_g(\cdot, \cdot)$ (Lemma 1). Combined with Theorem 8, one can obtain an upper bound for $\log \mathrm{Lip}(\mathcal{F}')$ from the upper bound for $\log \mathrm{Lip}(\mathcal{F})$. Therefore, we will use the following two lemmas shown at the end of this section.

Lemma 1 *For any E-ideals L and L', $\mathrm{dist}_g(L, L') = O(n^{2n+2} + \prod_j \mathcal{N}(\mathfrak{p}_j)^{c_j n}) \cdot \mathrm{dist}(L, L')$ holds for some constants c_j.*

Lemma 2 *For any $x, y \in G$ and $L = f'_c(x), L' = f'_c(y)$,*

$$\mathrm{dist}(L, L') = O(n) \cdot \mathrm{dist}_{G/U(S)}(x, y)$$

holds.

Proof. (for Theorem 2) Combining Theorem 8, Lemma 1 and Lemma 2, we have that

$$\| |f_q(x)\rangle - |f_q(y)\rangle \| = O\left(n^{2n+3} + \prod_j \mathcal{N}(\mathfrak{p}_j)^{c_j n} \right) \cdot \mathrm{Lip}(f_q) \cdot \mathrm{dist}_{G/U(S)}(x, y)$$

for some constants c_j, which implies that

$$\mathrm{Lip}(\mathcal{F}') = O\left(m^{2m+3} + \prod_j \mathcal{N}(\mathfrak{p}_j)^{c_j m} \cdot \mathrm{Lip}(\mathcal{F}) \right),$$

and hence

$$\log \mathrm{Lip}(\mathcal{F}') = O\left(m^2 + m \log |\Delta| + m \sum_{j=1}^{|S|} \log \mathcal{N}(\mathfrak{p}_j) \right)$$

by Theorem 9.

Notice that in [5, Theorem 5.4], it is shown that the $(\mathrm{Lip}(\mathcal{F}'), r, \epsilon)$-HSP oracle $\mathcal{F}'$ reduces to an $(\mathrm{Lip}(\hat{\mathcal{F}}'), \hat{r}, \epsilon)$-HSP oracle $\hat{\mathcal{F}}'$ defined on $\mathbb{R}^{\hat{n}}$ with $\hat{n} = 2(n_1+n_2)+|S|-1$, and moreover, $O(\log \mathrm{Lip}(\hat{\mathcal{F}}')) = O(\log \mathrm{Lip}(\mathcal{F}'))$. In order to apply the CHSP framework ([14, Theorem 1]) on $\hat{\mathcal{F}}'$, one needs that $\epsilon < 1/4$. According to [13, Theorem 36], we can take tensor product $\otimes^c \hat{\mathcal{F}}'$ with a constant c large enough such that the resulting oracle hides the same lattice. It is a $(c\,\mathrm{Lip}(\hat{\mathcal{F}}'), \hat{r}, \epsilon^c)$-HSP oracle satisfying that $\epsilon^c < 1/4$. Hence by applying Corollary 3 with $f = \mathcal{F}'$, we obtain the number of qubits

$$O(m^5 + m^4 \log|\Delta| + m^4 \sum_{j=1}^{|S|} \log \mathcal{N}(\mathfrak{p}_j)) + O(m \log \tau^{-1})$$

as claimed. □

Below, we give the proofs of the two lemmas.

Proof. for Lemma 1 Fix $L = \varphi(z)\underline{\mathcal{O}} \prod \mathfrak{p}_j^{-v_j}$ and $L' = \varphi(z')\underline{\mathcal{O}} \prod \mathfrak{p}_j^{-v'_j}$. Let a, d_j, d be ones that satisfy $\mathrm{dist}(L, L') = \|a\| + \sum_j \log(d_j) + n\log(d)$. We first consider the special case by assuming that $d_j = d = 1$ for all j such that $L_\Delta = e^{\mathrm{diag}(a_j)} B_\omega$. Therefore, without loss of generality, we can write $L'/L = \varphi(z'-z)\underline{\mathcal{O}} \prod \mathfrak{p}_j^{-(v'_j - v_j)}$, where $-(v'_j - v_j) \geq 0$ for all j. It is implied that $1/\varphi(z)L \supseteq L'$, and that there exist the HNF-basis H for L' and a matrix A satisfying $e^A = He^{\mathrm{diag}((-z)_j)}$ such that

$$\begin{aligned}
\mathrm{dist}_g(L, L') &\leq \|A\|_2 \\
&\leq n^2 \cdot \det(H) \cdot \mathrm{dist}(L, L') \\
&\leq n^2 \prod \mathcal{N}(\mathfrak{p}_j)^{c_j} \cdot \mathrm{dist}(L, L')
\end{aligned}$$

by Theorem 4 for some constants c_j.

Now suppose that not all of d_j and d are ones, so that $\sum_j \log(d_j) + n\log(d) \geq \log 2$. Since L and L' are fractional ideals of $\mathcal{O}$, there exist $\alpha, \alpha' \in K$ such that they can be written as $L = \frac{1}{\alpha} M$ and $L' = \frac{1}{\alpha'} M'$ for some integral ideals M, M' in $\mathcal{O}$. Let $W, W' \in \mathrm{GL}_n(\mathbb{Z})$ denote the HNF-bases such that $\frac{1}{\alpha} W B_\omega$ and $\frac{1}{\alpha'} W' B_\omega$ are basis for L and L', respectively. Under the condition, we can obtain an upper bound for the matrix A satisfying that $e^A = \alpha/\alpha' W' W^{-1}$ by Theorem 4 and the inequality $\mathrm{dist}(L, L') \geq \log 2$ derived from the above.

$$\begin{aligned}
\mathrm{dist}_g(L, L') &\leq \|A\|_2 \\
&\leq \left\| \frac{\alpha}{\alpha'} \right\| \|W'\|_2 \|W^{-1}\|_2 \\
&\leq n^2 \prod_j \mathcal{N}(\mathfrak{p}_j)^{h_j} \sqrt{\sum_j j |w'_{j,j}|^2} \cdot \frac{\|W\|_2^{n-1}}{|\det W|} \\
&\leq n^2 \prod_j \mathcal{N}(\mathfrak{p}_j)^{h_j} \frac{n(n+1)}{2} \prod_j w'_{j,j} \left(\frac{n(n+1)}{2} \prod_j w_{j,j} \right)^{n-1} \\
&\leq \frac{n^2}{\log 2} \left(\frac{n(n+1)}{2} \right)^n \prod_j \mathcal{N}(\mathfrak{p}_j)^{\tilde{h}_j n} \cdot \mathrm{dist}(L, L')
\end{aligned}$$

for some constants h_j and $\tilde{h}_j$.

Hence we can obtain that $\mathrm{dist}_g(L, L') = O(n^{2n+2} + \prod_j \mathcal{N}(\mathfrak{p}_j)^{\tilde{h}_j n}) \cdot \mathrm{dist}(L, L')$ as claimed. □

Proof. for Lemma 2 Fix $L = \varphi(z)\underline{\mathcal{O}} \prod \mathfrak{p}_j^{v_j}$ and $L' = \varphi(z')\underline{\mathcal{O}} \prod \mathfrak{p}_j^{v'_j}$ that are the images of $(z, (v_j))$ and $(z', (v'_j))$ under the map f'_c, respectively. We write

$$\mathrm{dist}_{G/U(S)}((z, (v_j)), (z', (v'_j))) = \|z - z' - u\| + \sum |v_j - v'_j - w_j| e_j \log p_j$$

for some $(u, (w_j))) \in U(S)$. Notice that if $(z - z' - u, (v_j - v'_j - w_j)) = 0$, i.e., $(z, (v_j))$ and $(z', (v'_j))$ satisfy the condition in Proposition 6 that they are different by an S-unit, then $L = L'$, and moreover, $L'/L = L/L' = \underline{\mathcal{O}}$, which implies that

$$\mathrm{dist}(L, L') = \mathrm{dist}_{G/U(S)}((z, (v_j)), (z', (v'_j))) = 0.$$

Now we suppose that $(z - z' - u, (v_j - v'_j - w_j)) \neq 0$ and that z, z', v_j, v'_j satisfy the infimum, i.e., $\mathrm{dist}_{G/U(S)}((z, (v_j)), (z', (v'_j))) = \|z - z'\| + \sum |v_j - v'_j| e_j \log p_j$. From the definition of the distance $\mathrm{dist}(\cdot, \cdot)$ among E-ideals, we have that

$$\mathrm{dist}(L, L') \leq \|z - z'\| + \sum_j \log d_j + n \log d$$

for some $d_j, d \in \mathbb{Z}$ such that $\prod d_j = \prod \mathcal{N}(\mathfrak{p}_j)^{\min\{-(v'_j - v_j), 0\}}$ and $d \leq \prod \mathcal{N}(\mathfrak{p}_j)^{\max\{-(v'_j - v_j), 0\}}$ by Theorem 3. Therefore, the upper bound for the distance can be taken as

$$\mathrm{dist}(L, L') \leq \|z - z'\| + n \sum_j c_j \log \mathcal{N}(\mathfrak{p}_j)$$

for some constants c_j. Then we can derive that

$$\begin{aligned} \mathrm{dist}(L, L') &\leq \|z - z'\| + n \sum_j c_j e_j \log p_j \\ &\leq n h_j \cdot \mathrm{dist}_{G/U(S)}((z, (v_j)), (z', (v'_j))), \end{aligned}$$

where h_j are constants. Hence, it follows that

$$\mathrm{dist}(L, L') = O(n) \cdot \mathrm{dist}_{G/U(S)}((z, (v_j)), (z', (v'_j)))$$

as claimed. □

4 Reductions to S-unit computation

Reference [5] proposed two problems that can be reduced to S-unit group computation, the class group problem, and the principal ideal problem.

4.1 Class group problem

In the class group algorithm from [5], the set is taken as

$$S_{\mathrm{CGP}} = \{\mathfrak{p} : \text{ prime } \mid \mathcal{N}(\mathfrak{p}) \leq 48(\log |\Delta|)^2\},$$

and the output is the Smith normal form (SNF) of the valuations of the result of S_{CGP}-unit group computation. The computation of the SNF is classical, so for the quantum space complexity, it suffices to evaluate $|S_{\mathrm{CGP}}|$. We approximate the number of rational primes smaller than $48(\log|\Delta|)^2$ with the following theorem, which was first discovered by Gauss; see, for example, [19]. Denote by $\pi(x)$ the number of rational primes less than x.

Theorem 10 (The prime number theorem) $\pi(x) \sim \frac{x}{\log x}$ *as* $x \to \infty$.

Let $e = \left\lfloor \frac{\log x}{\log 2} \right\rfloor$ and p denotes a rational prime number. Then the number of rational prime powers that are smaller than x is

$$\sum_{p \le 1} 1 + \cdots + \sum_{p^e \le x} 1 = \frac{x}{\log x} + \frac{x^{\frac{1}{2}}}{\frac{1}{2}\log x} + \cdots + \frac{x^{\frac{1}{e}}}{\frac{1}{e}\log x}$$

and has the order $O(x/\log x)$. From Corollary 1, we can obtain the quantum space complexity of the class group algorithm.

Corollary 4 *Under the Generalised Riemann Hypothesis, the class group computation algorithm ([5, Theorem 1.2]) uses* $O(n^5 + n^4(\log|\Delta|)^4/\log\log|\Delta|) + O(n\log\tau^{-1})$ *qubits.*

4.2 Principal ideal problem

In the algorithm reducing PIP to S-units from [5], the first step, that factors the input ideal to the product of powers of prime ideals $\mathfrak{a} = \mathfrak{p}_1^{a_1}\cdots\mathfrak{p}_k^{a_k}$, is quantum. The set S is taken to be the prime ideals dividing the ideal, i.e., $S_{\mathrm{PIP}} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$. The last step following the S_{PIP}-unit group computation is to classically solve equations on the valuations.

For the ideal factorisation, we follow the algorithm from [7, Algorithm 2], which shows that factoring integers is the only computationally difficult part.

Proposition 11 ([7, Lemma 4.1]) *Factoring fractional ideals of* K *into a product of prime ideals of* $\mathcal{O}$ *reduces to factoring integers in polynomial time in* $\log|\Delta|$ *and* n.

A fractional ideal I is given as $d \in \mathcal{O}$ and A, the integer which makes dI an integral ideal and a matrix of a basis of $\mathcal{O}$, respectively.

1. Compute the norm $N = \mathcal{N}(dI)$.
2. Factor $N = \prod p^{e_p}$ with $e_p > 0$.
3. For each p dividing N, compute the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ above p.
4. For each p dividing N, and each $\mathfrak{p} \supset p\mathcal{O}$ from Step (3), compute $v_{\mathfrak{p}}(dI)$, giving the exponent of $\mathfrak{p}$ in the factorization of dI.
5. For each $\mathfrak{p}$ found with nonzero valuation, output $\mathfrak{p}$, $v_{\mathfrak{p}}(dI)$. We have $dI = \prod \mathfrak{p}^{v_{\mathfrak{p}}(dI)}$.

6. Repeat steps (1)-(5) for the integral ideal $d\mathcal{O}$, then subtract the exponents of $d\mathcal{O}$ from the exponents computed above for the ideal dI for each prime, giving the primes $\mathfrak{p}$ and the exponents $v_{\mathfrak{p}}$ such that $I = \prod \mathfrak{p}^{v_{\mathfrak{p}}}$.

By the multiplicative rule of the ideal norms, for $\mathfrak{a} = \prod \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})}$, we can factor its norm into $\mathcal{N}(\mathfrak{a}) = \prod \mathcal{N}(\mathfrak{p})^{v_{\mathfrak{p}}(\mathfrak{a})}$. Therefore the norms of $d\mathfrak{a}$ and d will be $\mathcal{N}(d\mathfrak{a}) = \prod \mathcal{N}(\mathfrak{p})^{\max\{0, v_{\mathfrak{p}}(\mathfrak{a})\}}$ and $\mathcal{N}(d) = \mathcal{N}(d\mathcal{O}) = \prod \mathcal{N}(\mathfrak{p})^{-\min\{0, v_{\mathfrak{p}}(\mathfrak{a})\}}$, respectively. Hence, if we only do Step 2 in quantum, which factors positive integers $\mathcal{N}(d\mathfrak{a})$ and $\mathcal{N}(d\mathcal{O})$, then by [1], the number of qubits used for ideal factorization will be $O\left(\log\left(\mathcal{N}(d) \cdot (\mathcal{N}(\mathfrak{a}) + 1)\right)\right) = O(\log \mathcal{N}(\mathfrak{a}))$. By Theorem 2, to compute the S_{PIP}-unit group costs $O(n^5 + n^4 \log|\Delta| + n^4 \log \mathcal{N}(\mathfrak{a})) + O(n \log \tau^{-1})$ qubits, and hence it turns out to be the quantum space complexity for PIP as claimed in Corollary 2.

Acknowledgements

The author would like to thank Professor François Le Gall for his supports, Professor Katsuyuki Takashima for his comments, and Yuichiro Toma for his advice. The author is supported by MEXT Q-LEAP grant No. JPMXS0120319794.

References

[1] Peter W. Shor. "Algorithms for quantum computation: discrete logarithms and factoring". *35th Annual Symposium on Foundations of Computer Science (Santa Fe, NM, 1994)*. 1994, pp. 124–134.

[2] Sean Hallgren. "Fast quantum algorithms for computing the unit group and class group of a number field". *STOC'05: Proceedings of the 37th Annual ACM Symposium on Theory of Computing*. 2005, pp. 468–474.

[3] Kirsten Eisenträger et al. "A quantum algorithm for computing the unit group of an arbitrary degree number field". *STOC'14—Proceedings of the 2014 ACM Symposium on Theory of Computing*. 2014, pp. 293–302.

[4] Sean Hallgren. "Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem". *J. ACM* 54.1 (2007), Art. 4, 19.

[5] Jean-François Biasse and Fang Song. "Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields". *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms*. 2016, pp. 893–902.

[6] Jean-François Biasse and Claus Fieker. "Subexponential class group and unit group computation in large degree number fields". *LMS J. Comput. Math.* 17 (2014), pp. 385–403.

[7] Kirsten Eisenträger and Sean Hallgren. "Algorithms for ray class groups and Hilbert class fields". *Proceedings of the Twenty-First Annual ACM-SIAM Symposium on Discrete Algorithms*. 2010, pp. 471–483.

[8] Eric Bach. "Explicit bounds for primality testing and related problems". *Math. Comp.* 55.191 (1990), pp. 355–380.

[9] H. W. Lenstra Jr. and Carl Pomerance. "A rigorous time bound for factoring integers". *J. Amer. Math. Soc.* 5.3 (1992), pp. 483–516.

[10] Reinier Bröker, Denis Charles, and Kristin Lauter. "Evaluating large degree isogenies and applications to pairing based cryptography". *Pairing-based cryptography—Pairing 2008*. Vol. 5209. Lecture Notes in Comput. Sci. 2008, pp. 100–112.

[11] Werner Bley, Tommy Hofmann, and Henri Johnston. "Computation of lattice isomorphisms and the integral matrix similarity problem". *Forum Math. Sigma* 10 (2022), pp. 1–36.

[12] Ronald Cramer et al. "Recovering short generators of principal ideals in cyclotomic rings". *Advances in cryptology—EUROCRYPT 2016. Part II*. Vol. 9666. Lecture Notes in Comput. Sci. 2016, pp. 559–585.

[13] Razvan Barbulescu and Adrien Poulalion. "The special case of cyclotomic fields in quantum algorithms for unit groups". *Progress in cryptology—AFRICACRYPT 2023*. Vol. 14064. Lecture Notes in Comput. Sci. 2023, pp. 229–251.

[14] Koen de Boer, Léo Ducas, and Serge Fehr. "On the quantum complexity of the continuous hidden subgroup problem". *Advances in cryptology—EUROCRYPT 2020. Part II*. Vol. 12106. Lecture Notes in Comput. Sci. 2020, pp. 341–370.

[15] Ronald Cramer, Léo Ducas, and Benjamin Wesolowski. "Mildly Short Vectors in Cyclotomic Ideal Lattices in Quantum Polynomial Time". *J. ACM* 68.2 (2021).

[16] Jürgen Neukirch. *Algebraic number theory*. Vol. 322. Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. 1999.

[17] Władysław Narkiewicz. *Elementary and analytic theory of algebraic numbers*. Third. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2004.

[18] Henri Cohen. *A course in computational algebraic number theory*. Vol. 138. Graduate Texts in Mathematics. Springer-Verlag, Berlin, 1993.

[19] Tom M. Apostol. *Introduction to analytic number theory*. Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg, 1976.