Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields

Jean-François Biasse* Fang Song†

Abstract

This paper gives polynomial time quantum algorithms for computing the ideal class group (CGP) under the Generalized Riemann Hypothesis and solving the principal ideal problem (PIP) in number fields of *arbitrary* degree. These are are fundamental problems in number theory and they are connected to many unproven conjectures in both analytic and algebraic number theory. Previously the best known algorithms by Hallgren [20] only allowed to solve these problems in quantum polynomial time for number fields of *constant* degree. In a recent breakthrough, Eisenträger et al. [11] showed how to compute the unit group in arbitrary fields, thus opening the way to the resolution of CGP and PIP in the general case. For example, Biasse and Song [3] pointed out how to directly apply this result to solve PIP in classes of cyclotomic fields of arbitrary degree.

The methods we introduce in this paper run in quantum polynomial time in arbitrary classes of number fields. They can be applied to solve other problems in computational number theory as well including computing the ray class group and solving relative norm equations. They are also useful for ongoing cryptanalysis of cryptographic schemes based on ideal lattices [5, 10].

Our algorithms generalize the quantum algorithm for computing the (ordinary) unit group [11]. We first show that CGP and PIP reduce naturally to the computation of S-unit groups, which is another fundamental problem in number theory. Then we show an efficient quantum reduction from computing S-units to the continuous hidden subgroup problem introduced in [11]. This step is our main technical contribution, which involves careful analysis of the metrical properties of lattices to prove the correctness of the reduction. In addition, we show how to convert the output into an exact compact representation, which is convenient for further algebraic manipulations.

1 Introduction

Let K be a number field of degree n and $\mathcal{O}$ be an order in K with discriminant Δ. The ideal class group $\mathrm{Cl}(\mathcal{O})$ is the finite abelian group consisting of the invertible fractional ideals of $\mathcal{O}$ up to principal factors and has order $|\Delta|^{O(1)}$. Computing the ideal class group is an essential task in number theory that occurs in particular in the resolution of unproven heuristics such as the Cohen-Lenstra heuristics [9] on class groups of quadratic number field, Littlewood's bounds [25] on $L(1,\chi)$, or Bach's bound [1] on the maximum norm of the generators required to generate the class group. Besides being a fundamental problem, computing the ideal class group is also strongly connected to number theoretic problems occurring in cryptography. For example, it is at the heart of the only known unconditional classical subexponential algorithm for integer factorization [24]. Finding relations between elements in $\mathrm{Cl}(\mathcal{O})$ also occurs in curve-based cryptography. Indeed, both classical [4, 23] and quantum [6] subexponential methods for computing isogenies between elliptic curves depend on it.

Given an ideal $\mathfrak{a} \subseteq \mathcal{O}$, deciding whether or not $\mathfrak{a}$ is principal, and if so, finding $\alpha \in \mathcal{O}$ such that $\mathfrak{a} = (\alpha)$ is called the Principal Ideal Problem. It has direct applications to the computation of relative class groups and unit groups, and computing the S-class group of a number field. It is is also relevant to lattice-based cryptography, which has received a considerable attention since it allows quantum-safe cryptosystems and homomorphic encryption schemes. For efficiency reasons, there have been many proposals of schemes using lattices arising from ideals in the ring of integers of a number field, and in particular principal ideals generated by a small element (for example, see the homomorphic encryption scheme of Smart and Vercauteren [31] and the multilinear maps of Garg, Gentry and Halevi [18]). It has been recently shown that solving the principal ideal problem in polynomial time directly induces a polynomial time attack on schemes relying on the hardness of finding the short generator of a principal ideal [10].

Our method for finding the ideal class group of $\mathcal{O}$ and solving the principal ideal problem in $\mathcal{O}$ involves the computation of the S-unit group. Let S be a set of prime ideals of an order $\mathcal{O}$ of K. The set of elements

*Department of Mathematics and Statistics, University of South Florida, biasse@usf.edu.

†Department of Combinatorics & Optimization and Institute for Quantum Computing, University of Waterloo, fang.song@uwaterloo.ca. Partially supported by Canada's NSERC, CIFAR, Government of Canada and ORF.

$\alpha \in K$ such that $\exists (e_i)_{i \leq |S|} \in \mathbb{Z}^{|S|}$, $(\alpha) = \mathfrak{p}^{e_1} \cdots \mathfrak{p}^{e_{|S|}}$ is a multiplicative group called the S-unit group of K. This notion generalizes the units of $\mathcal{O}$ which are S-units for $S = \varnothing$, and computing the S-unit group is an important task in computational number theory. In particular, it is an essential ingredient of the resolution of norm equations of the form $\mathcal{N}_{L/K}(x) = \theta$ where $\theta \in K$, as shown by Simon [30] and Fieker [15, 17].

Previous work. Computing the ideal class group and the unit group is a problem that has been extensively studied in both the classical and quantum setting. Despite these efforts, there are no known polynomial time algorithms for these tasks. On the other hand, there are quantum polynomial time algorithms for several hard computational problems in number theory based on quantum algorithms for the Hidden Subgroup Problem (HSP). Shor showed that integer factorization and the discrete logarithm problem could be solved in polynomial time [29], and Hallgren described a polynomial time algorithm for solving the Pell's equation [21]. Similar methods were used to compute the class group and the unit group in polynomial time in classes of number fields of fixed degree [20, 28]. The approach of [20] relies on the resolution of the HSP in a bounded and discretized approximation of $\mathbb{R}^m$, which does not seem to apply when the degree of the fields grows to infinity. In a recent breakthrough, Eisenträger, Hallgren, Kitaev and Song [11] described a polynomial time algorithm for computing the unit group in classes of number fields of arbitrary degree. One of the main tools they developed is a continuous HSP definition on $\mathbb{R}^m$ and an efficient quantum algorithm solving it. In essence, their new HSP definition enforces stringent *continuity* properties on the function that hides the subgroup. This makes the function more amenable to quantum Fourier sampling.

Our contribution. In this paper, we present quantum algorithms to compute the ideal class group and solve the principal ideal problem in classes of number fields of arbitrary degree in polynomial time under the GRH. We follow a different framework than the previous work in constant-degree number fields due to Hallgren [20]. We show that both the ideal class group computation and PIP reduce to a more general problem of computing the S-unit group for suitable set of prime ideals S. For example, for the ideal class group computation S is chosen to be a succinct generating set of $\mathrm{Cl}(\mathcal{O})$. Then we give an efficient quantum algorithm for computing the S-unit group by extending the work by Eisenträger, Hallgren, Kitaev and Song [11]. We show an efficient quantum reduction from the S-unit group problem to HSP on $\mathbb{R}^m$ as defined in [11], which then can be solved efficiently by the quantum HSP algorithm in [11]. We also show how to get exact compact representations of the desired field elements with respect to a given integral basis for $\mathcal{O}$, while [11] only returns fixed point rational approximations of the units. Compact representations are usually easier for further algebraic processing. Our main results are summarized in the next three theorems.

THEOREM 1.1. (S-UNIT GROUP COMPUTATION) *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.*

THEOREM 1.2. (CLASS GROUP COMPUTATION) *Under the Generalized Riemann Hypothesis, there is a quantum algorithm for computing the class group of an order $\mathcal{O}$ in a number field K which runs in polynomial time in the parameters $n = \deg(K)$ and $\log(|\Delta|)$, where Δ is the discriminant of $\mathcal{O}$.*

THEOREM 1.3. (PIP RESOLUTION) *There is a quantum algorithm for deciding if an ideal $\mathfrak{a} \subseteq \mathcal{O}$ of an order $\mathcal{O}$ in a number field K is principal, and for computing $\alpha \in \mathcal{O}$ in compact representation such that $\mathfrak{a} = (\alpha)$ which runs in polynomial time in the parameters $n = \deg(K)$, $\log(\mathcal{N}(\mathfrak{a}))$ and $\log(|\Delta|)$, where Δ is the discriminant of $\mathcal{O}$.*

As an important corollary of our quantum algorithms, combining recent works in lattice cryptanalysis [5, 10], our results induce a quantum polynomial time attack on an entire family of cryptosystems relying on the hardness of finding a short generator of a principal ideal. See more in Sect. 6.

2 Preliminaries

In this section we review some useful background in number theory and introduce some definitions and notations. The notions of ideal class group and S-unit group are standard, and can be found in many books. We suggest Neukirch's book [27] for the fundamental aspects of this theory and Cohen's book [7] for the algorithmic aspects. We invite the reader who is already familiar to these topics to pay attention to the non-standard notion of E-ideal that we introduce in the following.

Number fields. A number field K is a finite extension of $\mathbb{Q}$. Its ring of integers $\mathcal{O}_K$ has the structure of a $\mathbb{Z}$-lattice of degree $n = [K : \mathbb{Q}]$, and the orders $\mathcal{O} \subseteq \mathcal{O}_K$ are the sublattices of $\mathcal{O}_K$ which

have degree n and which are equipped with a ring structure. Throughout this paper, we assume that $\mathcal{O}$ is an order in a number field K, and we denote by $\omega_1, \ldots, \omega_n$ a $\mathbb{Z}$-basis, that is $\mathcal{O} = \mathbb{Z}\omega_1 \oplus \ldots \oplus \mathbb{Z}\omega_n$. A number field has n_1 real embeddings and n_2 pairs of complex embeddings which we denote $(\sigma_j : K \to \mathbb{R})_{j \leq n_1}, ((\sigma_j, \overline{\sigma_j}) : K \to \mathbb{C})_{j \leq n_2}$ with $n_1 + n_2 = n = \deg(K)$. These embeddings define two essential maps, namely the norm and trace maps which are given by $\mathcal{T}(x) := \sum_\sigma \sigma(x) \in \mathbb{Q}$ and $\mathcal{N}(x) := \prod_\sigma \sigma(x) \in \mathbb{Q}$. The trace map is additive while the norm map is multiplicative. Note that $\mathcal{T}(\mathcal{O}) \subseteq \mathbb{Z}$ and $\mathcal{N}(\mathcal{O}) \subseteq \mathbb{Z}$. We measure the size of the ring $\mathcal{O}$ by $\log|\Delta|$ where $\Delta := (\det(\sigma_j(\omega_k)))^2$ is its discriminant, and it equals the volume of the fundamental domain of $\mathcal{O}$. Equivalently, the discriminant can be defined from the trace map by $\Delta := \det(\mathcal{T}(\omega_i\omega_j))_{i,j \leq n}$.

The ideal class group. The fractional ideals of $\mathcal{O}$ generalize the notion of ring ideals of $\mathcal{O}$. They are the subsets of K of the form $\mathfrak{a} = \frac{1}{d}I$ where $d \in \mathbb{Z}^+$ and $I \subseteq \mathcal{O}$ is an (integral) ideal of $\mathcal{O}$. A fractional ideal $\mathfrak{a}$ is invertible if $\mathfrak{a}^{-1} := \{x \in K \mid x\mathfrak{a} \subseteq \mathcal{O}\}$ is also a fractional ideal. The invertible fractional ideals have a multiplicative group structure, and the principal fractional ideals are one of its subgroups. The ideal class group is defined by

$$\mathrm{Cl}(\mathcal{O}) := \mathcal{I}/\mathcal{P},$$

where $\mathcal{I}$ is the multiplicative group of fractional invertible ideals of $\mathcal{O}$ and $\mathcal{P}$ is the subgroup of elements of $\mathcal{I}$ that are principal. This means that we identify $\mathfrak{a}$ and $\mathfrak{b}$ in $\mathrm{Cl}(\mathcal{O})$ if there is $\alpha \in K$ such that $\mathfrak{a} = (\alpha)\mathfrak{b}$. Ideals are sublattices of $\mathcal{O}$ of rank n, and we define their norm by $\mathcal{N}(I) := |\mathcal{O}/I|$. This notion naturally extends to fractional ideals using the multiplicative rule $\mathcal{N}(\mathfrak{a}/\mathfrak{b}) := \mathcal{N}(\mathfrak{a})/\mathcal{N}(\mathfrak{b})$. This notion of norm extends the norm on K in the sense that if $\mathfrak{a} = (\alpha)$, then $\mathcal{N}(\mathfrak{a}) = \mathcal{N}(\alpha)$.

The S-unit group. The S-units are a generalization of the units $\mathcal{O}^*$, which are the invertible elements of $\mathcal{O}$. The unit group can alternatively be defined as the $\alpha \in \mathcal{O}$ with $|\mathcal{N}(\alpha)| = 1$, or the $\alpha \in \mathcal{O}$ such that $(\alpha) = \mathcal{O}$. The unit group $\mathcal{O}^*$ satisfies $\mathcal{O}^* \simeq \mu \times \langle\varepsilon_1\rangle \times \ldots \times \langle\varepsilon_r\rangle$, where $r := n_1 + n_2 - 1$, μ is the set of roots of unity and the ε_i are torsion-free units. Let $S = \{\mathfrak{p}_i\}$ be a finite set of prime ideals of $\mathcal{O}$, the S-units are the elements $\alpha \in K$ such that there is $(e_i)_{i \leq |S|} \in \mathbb{Z}^{|S|}$ with $(\alpha) = \mathfrak{p}^{e_1} \cdots \mathfrak{p}^{e_{|S|}}$. Note that the S-units are elements of K. They form a multiplicative group $U(S)$ satisfying $U(S) \simeq \mu \times \langle\varepsilon_1\rangle \times \ldots \times \langle\varepsilon_{r+|S|}\rangle$, where $r := n_1 + n_2 - 1$, μ is the set of roots of unity and the ε_i are torsion-free S-units.

E-ideals. The number field K can be naturally embedded into $E := \mathbb{R}^{n_1} \times \mathbb{C}^{n_2}$ by setting $z \in \mathcal{O} \mapsto (\sigma_1(z), \ldots, \sigma_{n_1+n_2}(z))$. As in [11], we denote by $\underline{\mathcal{O}}$ the image of $\mathcal{O}$ via this embedding. The set $\underline{\mathcal{O}}$ inherits from the lattice structure of $\mathcal{O}$, i.e. it can be identified as a lattice in $\mathbb{R}^n$, as well as from the multiplication between elements (which is performed componentwise). The image of the fractional ideals of K in E are lattices $\Lambda \subseteq E$ with the property that $x\Lambda \subseteq \Lambda$ for all $x \in \underline{\mathcal{O}}$. We define the E-ideals as all the lattices in E satisfying this property. When there is no ambiguity, we identify a fractional ideal of $\mathcal{O}$ and the corresponding E-ideal.

Definition 2.1. (E-ideals) *Let $E := \mathbb{R}^{n_1} \times \mathbb{C}^{n_2}$ and $\underline{\mathcal{O}}$ the image of $\mathcal{O}$ via the embedding $K \to E$. An E-ideal is a lattice $\Lambda \subseteq E$ such that $\forall x \in \underline{\mathcal{O}}$, $x\Lambda \subseteq \Lambda$.*

Continuous HSP. We review the definition of continuous HSP proposed by Eisenträger et al. [11], for which they have shown an efficient quantum algorithm.

Definition 2.2. (Continuous HSP over $\mathbb{R}^m$) *The unknown subgroup $L \subseteq \mathbb{R}^m$ is a full-rank lattice satisfying some promise: the norm of the shortest vector is at least λ and the unit cell volume is at most d. The oracle has parameters (a, r, ε). Let $f : \mathbb{R}^m \to S$ be a function, where S is the set of unit vectors in some Hilbert space. We assume that f hides L in the following way.*

1. *f is periodic on L, i.e. $f(x) = f(x + v)$ for all $x \in \mathbb{R}^m$ and $v \in L$;*
2. *f is Lipschitz with constant a, i.e. $\big\||f(x)\rangle - |f(y)\rangle\big\| \leq a\|x - y\|$ for all $x, y \in \mathbb{R}^m$;*
3. *If the distance between the cosets ($x \bmod L$) and ($y \bmod L$) is greater or equal to r, i.e. if $\min_{v \in L} \|x - y - v\| \geq r$, then $\big|\langle f(x)|f(y)\rangle\big| \leq \varepsilon$.*

Under these conditions, the problem is to compute a basis of L by a quantum algorithm that can make oracle calls $|x\rangle \mapsto |x\rangle \otimes |f(x)\rangle$.

Actually, the definition also applies more generally to other topological groups $G = \mathbb{R}^k/\Lambda \times D$ with a proper metric on G [11, Sect.6.1]. Here G is decomposed to a continuous part, which is the quotient of $\mathbb{R}^k$ over some lattice Λ, and a discrete part that is finitely generated. It is nonetheless sufficient to consider HSP on $\mathbb{R}^m$, because the more general case can be reduced to HSP on $\mathbb{R}^m$ [11], and hence can be solved efficiently.

3 Overview of the algorithms

Our algorithms for CGP and PIP consist of reductions to the continuous hidden subgroup problem in two steps, and invoking the quantum HSP algorithm [11] at the end.

$$\mathsf{CGP} \leq_C S_{\mathsf{CGP}}\text{-units} \leq_Q \mathrm{HSP}(\mathbb{R}^{O(n)}),$$
$$\mathsf{PIP} \leq_Q S_{\mathsf{PIP}}\text{-units} \leq_Q \mathrm{HSP}(\mathbb{R}^{O(n)}).$$

Specifically, we first reduce them to S-unit problems with proper choices of S, which are almost entirely *classical* except that we apply a quantum algorithm for factoring ideals in the case of PIP[1]. We describe these reductions to S-units problems in Sect. 4. Next we show a *quantum* reduction from S-units problem for any S to $\mathrm{HSP}(\mathbb{R}^m)$, with $m = O(|S|, n)$. This is the main technical contribution of this work and it generalizes the reduction from (ordinary) unit-group problem to HSP by Eisenträger et al. [11]. The details will appear in Sect. 5, and we give an overview below.

Given $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$, we want to establish a function that hides the S-unit group according to Definition 2.2. To warm up, we review the reduction for the ordinary unit group (i.e., $S = \emptyset$) [11].

Review: reduction for unit-group [11]. Observe that the unit group can be identified as a subgroup of $G := \mathbb{R}^{n_1+n_2} \times \mathbb{Z}_2^{n_1} \times (\mathbb{R}/\mathbb{Z})^{n_2}$, and the mapping

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

translates between the so-called *log coordinates* and the conjugate vector representation. To see this, note that under canonical embeddings, any $z \in \mathcal{O}$ has the conjugate vector representation $(\ldots, \sigma_i(z), \ldots) \in \mathbb{R}^{n_1} \times \mathbb{C}^{n_2}$. If in addition z is invertible, then $\sigma_i(z) \neq 0$. Therefore, we can write $\sigma_i(z) = (-1)^{\mu_i} e^{u_i}$ with $\mu_i \in \mathbb{Z}_2$ and $u_i \in \mathbb{R}$ if σ_i is real, or $\sigma_i(z) = e^{2\pi i \theta_i} e^{u_i}$ with $\theta_i \in \mathbb{R}/\mathbb{Z}$ and $u_i \in \mathbb{R}$ if σ_i is complex.

Now one defines f in [11] as composition of two mappings:

$$f : G \xrightarrow{g} \{E\text{-ideals}\} \xrightarrow{f_q} \{\text{quantum states}\}.$$

Given $x \in G$, $g(x) := \varphi(x)\underline{\mathcal{O}} \subseteq E$ produces an E-ideal which is a transformed lattice of $\underline{\mathcal{O}}$. This is motivated by the fact that $\alpha\mathcal{O} = \mathcal{O}$ for any unit $\alpha \in \mathcal{O}^*$. Actually, one can verify easily that $g(x) = g(y)$ *iff.* $\varphi(x - y) \in \mathcal{O}^*$. Namely g is periodic on $\mathcal{O}^*$. For lacking of a canonical basis to represent real-valued lattices uniquely, which is needed to apply the quantum HSP algorithm, a quantum mapping f_q follows. It encodes a lattice L into a quantum state $|L\rangle$ that is roughly composed of quantum superposition over all lattice points, and hence provides a canonical representation for lattices. We will give more details of the quantum encoding in Sect. 5.1.

Very informally, one can show that small shift on an input to g causes small variance on the output lattice, but two inputs that are far apart modulo any unit will be mapped to lattices that have small overlap. Moreover, f_q preserves the "closeness" of lattices. Namely, quantum encodings of two lattices will have substantial inner product if and only if the lattices are very well lined up. To formalize these statements and thus proving the HSP properties, nonetheless, turn out to be highly non-trivial. It involves for example defining proper distance measures on various input and output spaces, and analyzing the continuity properties of f with respect to these metrics. This has been a great amount of efforts in [11] with further details in [12]

Other than these analytic properties, to make an efficient reduction, one needs to implement $f = f_q \circ g$ efficiently. In fact, f_q can be implemented efficiently on a quantum computer by standard techniques. Computing g, on the other hand, is much more tricky. For instance e^{u_i} will involve doubly-exponential numbers if we manipulate them naively. Instead one splits the computation into small pieces, in the spirit of repeated squaring, and carefully controls the precision. There is one key observation that guarantees that the size of any intermediate step does not blow up. That is $\mathcal{N}(z) = \pm 1$ for any unit z and hence $\prod_{i=1}^{n_1} e^{u_i} \prod_{j=1}^{n_2} e^{2u_{n_1+j}} = 1$. This indicates one redundant coordinate, and we can hence restrict f on $\mathbb{R}^{n_1+n_2-1} \times \mathbb{Z}_2^{n_1} \times (\mathbb{R}/\mathbb{Z})^{n_2}$ instead. This characterization is also essential to show a suitable bound on the volume of the unit cell of $\mathcal{O}^*$.

Reducing S-units to HSP. It is now easier to describe our generalized reduction for S-units. Let $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$. By definition, if $\alpha \in \mathcal{O}$ is an S-unit, we have

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

where $v_{\mathfrak{p}}(\alpha)$ is the coefficient of $\mathfrak{p}$ in the power of $(\alpha)\mathcal{O}$ (the valuation of α at $\mathfrak{p}$). Therefore the group of S-units $U(S)$ is the subgroup of $\hat{G} = \mathbb{R}^{n_1+n_2} \times \mathbb{Z}_2^{n_1} \times (\mathbb{R}/\mathbb{Z})^{n_2} \times \mathbb{Z}^k$. This motivates us defining the function $\hat{g} : \hat{G} \to \{E\text{-ideals}\}$ by:

$$\hat{g} : (y, v_1, \ldots, v_{|S|}) \longmapsto \phi(y) \cdot \underline{\mathcal{O}} \cdot \mathfrak{p}_1^{-v_1} \cdots \mathfrak{p}_{|S|}^{-v_{|S|}}.$$

[1] These reductions are straightforward. But classical algorithms typically compute the S-unit group by solving CGP and solving instances of PIP first. Our quantum algorithm tackles these problems in the reverse order.

We can show that (Prop. 5.1) $\hat{g}$ is periodic on $U(S)$. We then apply the same quantum encoding f_q on the output of $\hat{g}$. Namely, our oracle function behaves like:

$$\hat{f} : \hat{G} \xrightarrow{\hat{g}} \{E\text{-ideals}\} \xrightarrow{f_q} \{\text{quantum states}\}.$$

While the classical mappings g and $\hat{g}$ bear some similar motivation and we reuse f_q, to prove HSP properties of our function $\hat{f}$ is far from straightforward. We need to define new metrics tailored to the specific group structure that the S-units belong and the E-ideals (lattices in $\mathbb{R}^n$) that our $\hat{g}$ may possibly generate. Then we show quantitatively that under these metrics, small variance in inputs induces slightly perturbed lattices, whereas large variance of inputs modulo any S-units will induce with high fraction of mismatch. Finally we relate the new metrics to the analysis of [11] and conclude the HSP properties. We further extend the function $\hat{f}$ to obtain an HSP instance on $\mathbb{R}^m$ and work out the necessary bounds (λ, d) as required, which allows us to invoke the quantum HSP algorithm to recover $U(S)$.

Again, efficient implementation of $\hat{g}$ needs extra care. We need to split the computation differently due to the $\prod \mathfrak{p}_j^{-v_j}$ part. It is also important to notice, similar to the unit-group case, that the S-unit group actually forms a subgroup of $\mathbb{R}^{n_1+n_2-1} \times \mathbb{Z}_2^{n_1} \times (\mathbb{R}/\mathbb{Z})^{n_2} \times \mathbb{Z}^k$. That is, for a given S-unit α, the information given by the $|\sigma_j(\alpha)|$ for $j \leq n_1 + n_2$ and $v_{\mathfrak{p}}(\alpha)$ for $\mathfrak{p} \in S$ is redundant. Indeed, if α is an S-unit, then

$$\begin{aligned}&\mathcal{N}(\alpha) \cdot \mathcal{N}\left(\prod_{j \leq |S|} \mathfrak{p}^{-v_{\mathfrak{p}_j}(\alpha)}\right)\\ &= \prod_{j \leq n} e^{\log(\sigma_j(\alpha))} \cdot \prod_{j \leq |S|} e^{-v_{\mathfrak{p}_j}(\alpha) e_j \log(p_j)} = 1,\end{aligned}$$

where $e_j \leq n$ and p_j are such that $\mathcal{N}(\mathfrak{p}_j) = p_j^{e_j}$, and where $\log(x)$ denotes the natural logarithm of x (we us $\log_2(x)$ for the base-2 logarithm). Therefore $|\sigma_{n_1+n_2}(\alpha)|$ satisfies

$$\begin{aligned}\log(|\sigma_{n_1+n_2}(\alpha)|) = &-\frac{1}{2}\sum_{j \leq n_1} \log(|\sigma_j(\alpha)|)\\ &- \sum_{n_1 < j < n_1+n_2} \log(|\sigma_j(\alpha)|)\\ &+ \frac{1}{2}\sum_{j \leq |S|} v_{\mathfrak{p}_j}(\alpha) e_j \log(p_j).\end{aligned}$$

More details will appear in Sect. 5.1. Note that the solution of HSP is given to us as approximations of generators of the hidden subgroup. For many applications, an exact (and polynomially bounded) representation is preferable. Therefore, we process the solutions to the S-units problem classically to produce a compact representation of the generators of the S-unit group.

Definition 3.1. (Compact representation) *Let $l > 0$ be a constant, a compact representation of $\alpha \in \mathcal{O}$ with respect to the integral basis $(\omega_j)_{j \leq n}$ of $\mathcal{O}$ is a set of exact representations of polynomial size algebraic numbers γ_j satisfying $\alpha = \gamma_0 \gamma_1^l \cdots \gamma_k^{l^k}$, where k is polynomial in the size of the input.*

Recently, Biasse and Fieker [2, Sec. 5] described an efficient method based on [16, Alg. 7.53] to classically compute a compact representation of an algebraic number in polynomial time. These methods rely on the knowledge of an exact representation of the algebraic number we wish to represent (which is not the case here). A modification of [16, Alg. 7.53] using the approximation of the vector corresponding to an algebraic number yields a compact representation of that number. This extension uses well known lattice techniques and the details will be presented in the full version of this work.

4 Reducing CGP and PIP to S-units problem

As a motivating example, note that computing the (ordinary) unit-group problem reduces to S-units problem trivially by setting S to be the empty set. Next we show how to reduce CGP and PIP to computing S-units. There is an important observation about S-units that will be useful. Let $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$ be a set of prime ideals and let $U(S) = \mu_i \times \langle \varepsilon_1 \rangle \times \ldots \times \langle \varepsilon_{r+k} \rangle$. Each $\varepsilon_i \in \mathcal{O}$ can be represented by $(\mathbf{u}_i, v_{i,1}, \ldots, v_{i,k})$ such that $\mathbf{u}_i = (\sigma_1(\varepsilon_i), \ldots, \sigma_{n_1+n_2}(\varepsilon_i))$, $v_{i,j} = v_{\mathfrak{p}_j}(\varepsilon_i)$ for $j = 1, \ldots, k$, and more importantly $(\varepsilon_i) = \prod_{j=1}^k \mathfrak{p}_j^{v_{i,j}}$. We define $L(S) \subseteq \mathbb{Z}^k$ to be the lattice generated by $\{(v_{i,1}, \ldots, v_{i,k})\}_{i=1}^{r+k}$. The following statement follows almost immediately from the definition of S-units.

Lemma 4.1. *Let $U(S)$ and $L(S)$ be as defined above. Let $\mathfrak{a} := \prod_{i=1}^k \mathfrak{p}_i^{z_i}$ be an ideal with $z_i \in \mathbb{Z}, i \in [k]$. Then $\mathfrak{a} = (\alpha)$ for some $\alpha = \mu \prod_{i=1}^{r+k} \varepsilon_i^{x_i} \in U(S)$ with $x_i \in \mathbb{Z}, i \in [r+k]$ iff. $(z_1, \ldots, z_k) \in L(S)$ with $z_j = \sum_i x_i v_{i,j}$ for $j \in [k]$.*

Proof. Suppose that $\mathfrak{a} = \prod \mathfrak{p}_i^{z_i} = (\alpha)$ for some $\alpha \in U(S)$. Therefore $\alpha = \prod \varepsilon_i^{x_i}$ for some $x_i \in \mathbb{Z}, i = 1, \ldots, r+k$, and hence $(\alpha) = \prod_i (\varepsilon_i)^{x_i}$. Since $(\varepsilon_i) = \prod_j \mathfrak{p}_j^{v_{i,j}}$, we have that $(\alpha) = \prod_i (\prod_j \mathfrak{p}_j^{v_{i,j}})^{x_i} = \prod_j \mathfrak{p}_j^{\sum_i x_i v_{i,j}}$. By unique factorization of ideals, $z_i =$

$\sum_i x_i v_{i,j}$ and hence $(z_1, \ldots, z_k) \in L(S)$. Likewise, the exact same argument goes through in the reverse direction as well. □

Class group problem. To ensure an efficient reduction, we need a polynomial time generating set for the ideal class group. As pointed out in [2, Sec. 3.2], this directly derives from [1] (in the standard case where $\mathcal{O} = \mathcal{O}_K$ the maximal order of K, the factor 48 can be replaced by 12).

FACT 4.1. *Let* $\mathcal{B} := \{\mathfrak{p} \subseteq \mathcal{O} \text{ prime} : \mathcal{N}(\mathfrak{p}) \leq 48\log(|\Delta|)^2\}$ *be the set of all prime ideals of* $\mathcal{O}$ *of norm up to* $48\log(|\Delta|)^2$. *Under the Generalized Riemann Hypothesis (GRH),* $\mathcal{B}$ *generates* $\mathrm{Cl}(\mathcal{O})$, *the size of* $\mathcal{B}$ *is polynomial in* $\log(|\Delta|)$, *and can be computed in time polynomial in* $\log(|\Delta|)$.

Now let $S_{\mathsf{CGP}} = \mathcal{B} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_N\}$ as given in Fact 4.1. Consider the surjective morphism

$$\begin{array}{ccccc} \mathbb{Z}^N & \xrightarrow{\varphi} & \mathcal{I} & \xrightarrow{\pi} & \mathrm{Cl}(\mathcal{O}) \\ (e_1, \ldots, e_N) & \longrightarrow & \prod_i \mathfrak{p}_i^{e_i} & \longrightarrow & \prod_i [\mathfrak{p}_i]^{e_i} \end{array},$$

and note that the class group $\mathrm{Cl}(\mathcal{O})$ is isomorphic to $\mathbb{Z}^N / \ker(\pi \circ \varphi)$. Therefore, computing the class group boils down to computing $\ker(\pi \circ \varphi)$, which consists of all $(e_1, \ldots, e_N)$ such that $\prod \mathfrak{p}_i^{e_i}$ is a principal ideal. By Lemma 4.1, $\ker(\pi \circ \varphi)$ is exactly $L(S_{\mathsf{CGP}})$. As a result, the Smith Normal form of $L(S_{\mathsf{CGP}})$, which can be computed efficiently [19, 26], will reveal the desired decomposition of $\mathrm{Cl}(\mathcal{O})$. This is summarized in Algorithm 1.

Algorithm 1 Reducing CGP to S-units

Input: $\mathcal{O}$

1: Let $S_{\mathsf{CGP}} = \{\mathfrak{p} \subseteq \text{ prime } \mid \mathcal{N}(\mathfrak{p}) \leq 48\log(|\Delta|)^2\}$ with $|S_{\mathsf{CGP}}| = N$.
2: Compute a set of generators for the S_{CGP}-unit group $U(S_{\mathsf{CGP}})$: $\{(\mathbf{u}_i, v_{i,1}, \ldots, v_{i,N})\}_{i=1}^{r+N}$.
3: Compute $\mathrm{diag}(d_1, \ldots, d_n)$, the Smith Normal Form of $(v_{i,j})_{i \in [r+N], j \in [N]}$.
4: **return** $d_1, \ldots, d_n$.

Principal ideal problem. Given an ideal $\mathfrak{a}$ by a $\mathbb{Z}$-basis, consider its prime factorization as $\mathfrak{a} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_k^{a_k}$, which can be obtained efficiently by adapting Shor's quantum factoring algorithm [29, 14]. Let $S_{\mathsf{PIP}} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$ be the prime divisors and clearly $\mathfrak{a}$ is principal *if and only if* $\mathfrak{a} = (\alpha)$ for an S_{PIP}-unit α. By Lemma 4.1, this is equivalent to $(a_1, \ldots, a_k) \in L(S_{\mathsf{PIP}})$. Therefore, to decide if $\mathfrak{a}$ is principal, it suffices to check $(a_j) \in L(S_{\mathsf{PIP}})$ which can be done efficiently by solving a linear system. If so, and suppose $a_j = \sum_i x_i v_{i,j}$ with $x_i \in \mathbb{Z}, i \in [r+k]$, then $\alpha := \prod_{i=1}^{r+k} \varepsilon_i^{x_i}$ gives a generator of $\mathfrak{a}$. The reduction is described in Algorithm 2.

Algorithm 2 Reducing PIP to S-units

Input: $\mathcal{O}$ and an ideal $\mathfrak{a} \subseteq \mathcal{O}$.

1: Factor $\mathfrak{a} = \prod \mathfrak{p}_j^{a_j}$. Let $S_{\mathsf{PIP}} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$ be the divisors of $\mathfrak{a}$.
2: Compute the S_{PIP}-unit group $U(S_{\mathsf{PIP}}) = \mu \times \langle \varepsilon_1 \rangle \times \ldots \times \langle \varepsilon_{r+k} \rangle$. Note that $\varepsilon_i = (\ldots, v_{i,1}, \ldots, v_{i,k})$ with $\varepsilon_i = \prod_{j=1}^k \mathfrak{p}_j^{v_{i,j}}$. Let $M = (v_{i,j})$.
3: Solve for $(x_1, \ldots, x_{r+k})M = (a_1, \ldots, a_k)$ with $x_i \in \mathbb{Z}, i \in [r+k]$.
4: **return** $\prod_i \varepsilon_i^{x_i}$ or "not principal" if the system has no solution.

5 Reducing S-units problem to continuous HSP

In this section, we show a quantum reduction from computing S-units to HSP for an arbitrary S. We define a function f in Sect. 5.1, which is periodic on the S-unit group. We also show that this function can be implemented efficiently on a quantum computer. Next we show in Sect. 5.2 that the function satisfies the conditions of the continuous HSP definition. In Sect. 5.3, we complete the remaining pieces of the reduction such as proving the geometric bounds of the S-unit group.

5.1 Defining the oracle function $(\mathbf{y}, \mathbf{v}) \mapsto |\varphi(\mathbf{y})\underline{\mathcal{O}} \prod_{\mathfrak{p} \in S} \mathfrak{p}^{-v_i}\rangle$

As we informally discussed in Sect. 3, we define f as[2]

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

where $G = \mathbb{R}^{n_1+n_2} \times \mathbb{Z}_2^{n_1} \times (\mathbb{R}/\mathbb{Z})^{n_2} \times \mathbb{Z}^{|S|}$. Specifically, f_c maps $(\mathbf{y}, \mathbf{v}) \in G$ to a rational approximation of a basis for the E-ideal

$$f_c(y, v_1, \ldots . v_{|S|}) = \phi(y) \cdot \underline{\mathcal{O}} \mathfrak{p}_1^{-v_1} \cdots \mathfrak{p}_{|S|}^{-v_{|S|}}. \tag{5.1}$$

We show that f_c is periodic on $U(S)$.

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*

- $f_c(y', (v_j')) = f(y, (v_j)) \iff \phi(u) \in U(S)$.
- $v_{\mathfrak{p}_j}(\phi(u)) = w_j, \forall j = 1, \ldots, |S|$.

[2]Here we overload the notations of f, G, and rewrite $\hat{g}$ as f_c to emphasize that it is a classical function.

Proof. If $\phi(u) \in U(S)$, $f_c(u,(w_j)) = \mathcal{O}$ and $f_c(y',(v'_j)) = f_c((y,(v_j)+(u,(w_j)))$. Reciprocally, if $f_c(y',(v'_j)) = f_c((y,(v_j)+(u,(w_j)))$, then $\phi(u)\cdot\underline{\mathcal{O}}\cdot \mathfrak{p}_1^{-v_1}\cdots\mathfrak{p}_{|S|}^{-v_{|S|}} = \mathcal{O}$. In particular, there exist $\alpha \in \prod_j \mathfrak{p}_j^{-v_j} \subseteq K$ and $\beta \in \mathcal{O}$ such that $\phi(u) = \beta/\alpha \in K$. Therefore $u \in K$ and has to be an S-unit. □

Note that the naive computation of f_c involves computing $(e^{u_i})_{i\le n_1+n_2}$, where $y = (u_1,\ldots,n_{n_1+n_2},\theta)$ with a phase $\theta \in \mathbb{Z}_2^{n_1}\times(\mathbb{R}/\mathbb{Z})^{n_2}$. Any rational approximation of e^{u_i} has at least $\lceil\log_2(e^{u_i})\rceil \in O(u_i)$ bits where $\log_2$ denotes the base 2 logarithm. As this is exponential in the bit size of the entry, we need to proceed differently to evaluate f_c. The authors of [11] described a way to split up the computation ensuring that we only manipulate values of polynomial size. We adapt this method to our specific classical oracle that differs by a term of the form $\prod_{\mathfrak{p}_i\in S}\mathfrak{p}_i^{-v_i}$ from the one described in [11].

PROPOSITION 5.2. *The methods of [11] can be adapted to evaluate $e^t\underline{\mathcal{O}}\prod_{\mathfrak{p}\in S}\mathfrak{p}^{-v_i}$ in a polynomial number of multiplications between E-ideals of determinant $\sqrt{|\Delta|}$.*

The arithmetic between E-ideals is directly inspired from the arithmetic between ideals in a number field. To evaluate our classical oracle, we need an efficient implementation of the E-ideal multiplication. Let $A = \oplus_{j\le n}\mathbb{Z}a_j$ and $B = \oplus_{k\le n}\mathbb{Z}b_k$ be E-ideals generated by the $a_j, b_k \in E$. Then the E-ideal $A\cdot B$ is the lattice generated by the n^2 elements $(a_j\cdot b_k)_{j,k\le n}$. The multiplication of two E-ideals can be described by the two following steps:

1. Calculate all the cross terms $a_j\cdot b_k$ for $j,k\le n$.
2. Compute a basis $(c_j)_{j\le n}$ of $\sum_{j,k}\mathbb{Z}a_j\cdot b_k$.

The main challenge of E-ideal multiplication is that we need to deal with rational approximations of lattices. We need to estimate how much precision is needed to ensure accuracy, and how much precision is lost after each operation. Knowing how to bound the number of operation between E-ideals and the cost of each operation allows us to estimate the asymptotic complexity of the classical oracle.

THEOREM 5.1. *The E-ideal multiplication between E-ideals of determinant $\sqrt{|\Delta|}$ requires a polynomial number of bits of precision and runs in polynomial time. The complexity of the classical oracle is in*

$$\tilde{O}\left(\|(y,v)\|^2 n^{5+\varepsilon}\left(\left(n\log(|\Delta|)+n^2+\|(y,v)\|^2\right)^{1+\varepsilon}\right.\right.$$
$$\left.\left.+|S|\max_j(\log(p_j)^3)\right)\right),$$

where $\varepsilon > 0$ is arbitrarily small.

Quantum Encoding f_q. Once we have obtained a basis for an E-ideal from f_c, we use the same quantum encoding proposed in [11] to encode the ideal (lattice) in a quantum state. This gives a (quantum) canonical way of representing real-valued lattices uniquely, which is needed later to apply the quantum algorithm for solving HSP. Here we give a brief review of the quantum encoding f_q.

Let $g_s(\cdot)$ be the Gaussian function $g_s(x) := e^{-\pi\|x\|^2/s^2}, x\in\mathbb{R}^n$. For any set $S\subseteq\mathbb{R}^n$, denote $g_s(S) := \sum_{x\in S} g_s(x)$. Given a a lattice L, the quantum encoding maps L to the lattice Gaussian state via

$$f_q(L) = |L\rangle := \gamma\sum_{v\in L} g_s(v)|\mathrm{str}_{\nu,n}(v)\rangle,$$

where $\mathcal{S} = \{\text{unit vectors in a Hilbert space}\}$ and γ is a factor that normalized the state. Here $|\mathrm{str}_{\nu,n}(v)\rangle$ is the straddle encoding of a real-valued vector $v\in\mathbb{R}^n$, as defined in [11]. Intuitively, one discretizes the space $\mathbb{R}^n$ by a grid $\nu\mathbb{Z}^n$, and encodes the information about v by a superposition over all grid nodes surrounding v. Specifically, for the one-dimensional case, the straddle encoding of a real number is

$$x\in\mathbb{R}\mapsto|\mathrm{str}_\nu(x)\rangle := \cos(\frac{\pi}{2}t)|k\rangle + \sin(\frac{\pi}{2}t)|k+1\rangle,$$

where $k := \lfloor x/\nu\rfloor$ denotes the nearest grid point no bigger than x and $t := x/\nu - k$ denotes the (scaled) offset. Repeat this for each coordinate of $v = (v_1,\ldots,v_n)$ we get $|\mathrm{str}_{\nu,n}(v)\rangle := \bigotimes_{i=1}^n|\mathrm{str}_\nu(v_i)\rangle$.

FACT 5.1. ([11]) *Let L be an LLL-reduced basis. Assume that $\lambda_1(L)\ge\lambda$, $\det(L)\le d$ and $s\ge n^{n/2+1}2^n\lambda^{-n+1}d$. There is a quantum algorithm that takes L as input and produces a state that is $2^{-\Omega(n)}$-close to $|L\rangle = \gamma\sum_{v\in L}g_s(v)|\mathrm{str}_{\nu,n}(v)\rangle$ within time* $\mathrm{poly}(n,\log s,\log\frac{1}{\nu})$.

5.2 Analyzing the HSP properties of f

In this section, we discuss the properties that the function $f: G\to\mathcal{S}$ hiding $U(S)$ needs to satisfy by rephrasing Definition 2.2 for the group we are interested in.

DEFINITION 5.1. (HSP PROPERTY) *We say that $f: G\to\{\text{Quantum states}\}$ satisfies the HSP property for a discrete subgroup $H\le G$ if*

1. *f is periodic on H, that is $f(x+u) = f(x)\ \forall x\in G,\ u\in H$,*

2. *f is Lipschitz for some constant a : $\forall\ x, y \in G/H$, $\| |f(x)\rangle - |f(y)\rangle \| \leq a \cdot d_{G/H}(x, y)$,*

3. *There are $r, \varepsilon > 0$ such that $\forall\ x, y \in G/H$, if $d_{G/H}(x, y) \geq r$, then $|\langle f(x)|f(y)\rangle| \leq \varepsilon$,*

where $d_{G/H}(\cdot, \cdot)$ denotes a distance on G/H.

Because the input includes valuations v_i of a power-product of prime ideals, our classical oracle significantly differs from the one used to hide the unit group in [11]. We need to define metrics on G and the set of E-ideals arising as the images of an element in G, together with a careful analysis of the topological properties of the oracle with respect to this metric.

Definition 5.2. (Distance on $G/U(S)$) *Let $(z, (v_j)_{j \leq |S|})$ and $(z', (v'_j)_{j \leq |S|})$, we define their distance in $G/U(S)$ by*

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

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

Definition 5.3. (Distance between E-ideals) *Let $\mathcal{L}$ and $\mathcal{L}'$ be two E-ideals arising as the image of elements in G by the classical encoding f_c, and $\mathcal{L}_\Delta := \mathcal{L}'/\mathcal{L}$. We define*

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

where L_Δ runs over all the matrices of a basis of $\mathcal{L}'/\mathcal{L}$ 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 $(a_j)_{j \leq n} \in E$ satisfying $L_\Delta = e^{\operatorname{diag}(a_j)} B_\omega \operatorname{diag}(d_j/d)$.

Proposition 5.3. *Definition 5.3 defines a distances between lattices arising as the image of an element of G by the map* (5.1).

Let G and $f = f_q \circ f_c$ be as defined before, we are able to prove Theorem 5.2 and Theorem 5.3, which ensure that our oracle satisfies the HSP property.

Theorem 5.2. *There exists $a > 0$ such that for any $x, y \in G/U(S)$, $\| |f(x)\rangle - |f(y)\rangle \| \leq a \cdot \operatorname{dist}_{G/U(S)}(x, y)$.*

Theorem 5.3. *There are $r > 0$ and $\varepsilon > 0$ such that $d_{G/U(S)}(x, y) \geq r \Rightarrow |\langle f(x)|f(y)\rangle| \leq \varepsilon$.*

5.3 Completing the reduction

We have shown that the S-unit group corresponds to the periods of a function on $\mathbb{R}^{n_1+n_2-1} \times \mathbb{Z}_2^{n_1} \times (\mathbb{R}/\mathbb{Z})^{n_2} \times \mathbb{Z}^{|S|}$ satisfying the continuous HSP property. To invoke the algorithm described in [11], we need to reduce further to an instance of the continuous HSP on $\mathbb{R}^m$ for some $m > 0$. This follows similar arguments as in [11, Sect.6.1]. A formal proof is deferred to the full version.

Theorem 5.4. *Let $f : G = \mathbb{R}^{n_1+n_2-1} \times (\mathbb{R}/\mathbb{Z})^{n_2} \times \mathbb{Z}_2^{n_1} \times \mathbb{Z}^{|S|} \to \mathcal{S}$ be an (a, r, ε) oracle function that hides L with $\lambda_1(L) \geq \lambda$ and $\operatorname{Vol}(G/L) \leq d$. Then it reduces to an HSP instance $g : \mathbb{R}^m \to \mathcal{S}$ that hides $\tilde{L}$ with $m = 2(n_1+n_2)+|S|-1, \lambda_1(\tilde{L}) \geq \lambda, \operatorname{Vol}(\mathbb{R}^m/\tilde{L}) \leq d\lambda^{n_1}$ and parameters $\varepsilon = \varepsilon$,*

$$a = \sqrt{a^2 + |S|(\frac{\pi}{2\nu}(1+\nu))^2 + n_2(\frac{\pi}{2\nu\lambda}(1+\nu))^2},$$
$$r = \sqrt{(2r + 2|S|\nu)^2 + n_2(2\nu\lambda)^2}.$$

In addition g can be instantiated efficiently on a quantum computer with access to f.

According to Definition 2.2, we still need to derive bounds for the first minima and the fundamental volume of the lattice of S-units, which the complexity of the algorithm for solving the HSP depends on. We show such bounds by an analogue of Dirichlet's unit theorem.

Proposition 5.4. *The first minima of $U(S) \subseteq G$ satisfies $\lambda_1(U(S)) \geq \frac{\log(n)}{6n^4}$ where the norm on elements of G is defined by $\|(z, v_1, \ldots, v_{|S|})\| := \sqrt{\sum_j z_j^2} + \sum_j |v_j| e_j \log(p_j)$. Moreover, the volume of the lattice of S-units satisfies*

$$\operatorname{Vol}(G/U(S)) \leq \frac{1}{\log(2)^{|S|}} \left(300 \log(P) \sqrt{|\Delta|} \left(\frac{e}{2} \log(|\Delta|) \right)^{n-1} \right)^{|S|+r-\frac{n}{2}},$$

where $P = \max_j \mathcal{N}(\mathfrak{p}_j)$.

We can now invoke the efficient quantum algorithm for HSP on $\mathbb{R}^m$ proposed in [11, Theorem 6.1]. Pick a fine enough discrete grid $\delta\mathbb{Z}^m$ and a sufficiently broad and smooth window function w, we create a superposition of grid points with in the window, evaluate the function, and then measure the state in the Fourier basis. With sufficiently many samples, one obtains an approximate generating set of $\mathcal{L}^*$, from which one can compute a basis for $\mathcal{L}$ as well within the desired precision.

6 Applications and Discussion

There are a few recent cryptosystems relying on the hardness of finding a short generator of a principal ideal (short-PIP) of the cyclotomic ring $\mathbb{Z}[X]/(X^{2^n}+1)$. Typical examples of these schemes are the fully homomorphic encryption scheme of Smart and Vercauteren [31] and the multilinear maps of Garg, Gentry and Halevi [18]. Following an observation of CESG scientists Campbell et al. [5, Sec. 3], the short-PIP reduces to the PIP (a fact rigorously proved later by Cramer et al. [10]). The task of recovering an arbitrary generator of an ideal in $\mathbb{Q}(\zeta_{2^n})$ (PIP under the promise that the ideal is principal) was conjectured to be feasible in quantum polynomial time by Campbell et al. [5], but the algorithm they proposed seems to have an exponential run time [3, Sec. 5]. Biasse and Song [3] later adapted the unit group algorithm of Eisenträger et al. [11] to derive a polynomial time solution to this task. However, the algorithm proposed in [3] is limited to cyclotomic fields and assumes a priori that the ideal is principal. Our algorithm for the PIP in arbitrary fields leaves the door open for further generalizations of the attacks against cryptosystems relying on the short-PIP in $\mathbb{Q}(\zeta_{2^n})$ to other schemes using ideal lattices. In particular, there is currently a lot of attention around the possibility of reducing the NTRU problem [22] to an instance of the short-PIP in a quadratic extension of $\mathbb{Q}(\zeta_{2^n})$.

Our work also has direct applications in computational number theory. Indeed, the S-unit group is a central object that can be used in a lot of algorithms. It usually is computed together with the so-called S-class group, which is the quotient of the group of ideals in the ring of S-integers by the subgroup of principal ideals. The S-class group can easily be derived from the ideal class group and an oracle for the PIP by quotienting the class group by extra relations. A description of this method can be found in Simon's PhD thesis [30, Chap. 1].

Another consequence of our work is that it implies a polynomial time algorithm for computing the relative class group and the relative unit group of an arbitrary extension of number fields. Algorithms for these tasks are already known [8, Ch. 7], but their run time is exponential in the degree of the fields. As for the S-class group, they also consist of using a complete set of relations for the ideal class group and of enriching it with new relations that are obtained by solving instances of the PIP.

Our algorithms also directly imply a quantum algorithm for computing the ray class group of an arbitrary number field. The computation of the ray class group is an essential task in computational class field theory. A classical method due to Cohen can be found in [8, 3.2] and has an exponential run time with respect to the degree (but runs in subexponential time for classes of fixed degree number fields). A quantum algorithm was described by Eisenträger and Hallgren [13] with a polynomial run time in classes of fixed degree number fields. As for the aforementioned tasks, computing the ray class group essentially relies on subroutines for computing the ideal class group and solving the PIP, for which we provide polynomial time algorithms in arbitrary number fields. It also relies on algorithms for factoring ideals and solving the discrete logarithm, both of which are easy on a quantum computer [29, 14].

Finally, our work allows us to describe polynomial time algorithms for solving relative norm equations of the form $\mathcal{N}_{L/K}(x) = \theta$ where L/K is an arbitrary Galois extension. Norm equations are an important example of Diophantine equations which are a major topic in number theory. The resolution of the Pell's equation (for which there is a quantum algorithm [21]) can be seen as a special case where $L = \mathbb{Q}(\sqrt{\Delta})$, $K = \mathbb{Q}$ and $\theta = 1$ (when we restrict our attention to integer solutions). Solving norm equations in general is an important task in computational number theory. A classical method was described by Simon [30] (based on the work of Fieker [15] for Galois extensions) that solves general extensions in exponential time in the degree of the fields. For the Galois case, it simply uses the knowledge of the S-unit group and the relative class group, which we can provide in polynomial time for number fields of arbitrary degree. However, the general method uses the Galois closure, whose degree can be exponential in the degree of the field, thus restricting the direct application of our work to arbitrary Galois extensions.

References

[1] E. Bach. Explicit bounds for primality testing and related problems. *Mathematics of Computation*, 55(191):355–380, 1990.

[2] J.-F. Biasse and C. Fieker. Subexponential class group and unit group computation in large degree number fields. *LMS Journal of Computation and Mathematics*, 17:385–403, 1 2014.

[3] J.-F. Biasse and F. Song. On the quantum attacks against schemes relying on the hardness of finding a short generator of an ideal in $\mathbb{Q}(\zeta_{p^n})$. `http://cacr.uwaterloo.ca/techreports/2015/cacr2015-12.pdf`, 2015.

[4] R. Bröker, D. Xavier Charles, and K. Lauter. Evaluating large degree isogenies and applications to pairing based cryptography. In S. Galbraith and K. Paterson, editors, *Pairing-Based Cryptography - Pairing 2008, Second International Conference,*

Egham, UK, September 1-3, 2008. Proceedings, Lecture Notes in Computer Science, pages 100–112. Springer, 2008.

[5] P. Campbel, M. Groves, and D. Shepherd. SOLILOQUY, a cautionary tale. `http://docbox.etsi.org/Workshop/2014/201410_CRYPTO/S07_Systems_and_Attacks/S07_Groves_Annex.pdf`, 2014.

[6] A. Childs, D. Jao, and V. Soukharev. Constructing elliptic curve isogenies in quantum subexponential time. *Journal of Mathematical Cryptology*, 8(1):1 – 29, 2013.

[7] H. Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, 1991.

[8] H. Cohen. *Advanced topics in computational algebraic number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, 1999.

[9] H. Cohen and H.W. Lenstra. Heuristics on class groups of number fields. *Number Theory, Lecture notes in Math.*, 1068:33–62, 1983.

[10] R. Cramer, L. Ducas, C. Peikert, and O. Regev. Recovering short generators of principal ideals in cyclotomic rings. *IACR Cryptology ePrint Archive*, 2015:313, 2015.

[11] K. Eisenträger, S. Halgren, A. Kitaev, and F. Song. A quantum algorithm for computing the unit group of an arbitrary degree number field. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, STOC '14, pages 293–302, New York, NY, USA, 2014. ACM.

[12] K. Eisenträger, S. Halgren, A. Kitaev, and F. Song. A quantum algorithm for computing the unit group of an arbitrary degree number field (long version), 2015. In preparation.

[13] K. Eisenträger and S. Hallgren. Algorithms for ray class groups and hilbert class fields. In *Proceedings of the Twenty-first Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '10, pages 471–483, Philadelphia, PA, USA, 2010. Society for Industrial and Applied Mathematics.

[14] Kirsten Eisenträger and Sean Hallgren. Algorithms for ray class groups and hilbert class fields. In *Proceedings of the twenty-first annual ACM-SIAM symposium on Discrete Algorithms*, pages 471–483. Society for Industrial and Applied Mathematics, 2010.

[15] C. Fieker. *Relative Normgleichungen*. PhD thesis, Technische Universität Berlin, 1997.

[16] C. Fieker. Algorithmic Number Theory. Lecture notes available at http://www.mathematik.uni-kl.de/agag/mitglieder/professoren/prof-dr-claus-fieker, 2014.

[17] C. Fieker, A. Jurk, and M. Pohst. On solving relative norm equations in algebraic number fields. *Mathematics of Computation*, 66(217):399–410, 1997.

[18] S. Garg, C. Gentry, and S. Halevi. Candidate multilinear maps from ideal lattices. In T. Johansson and P. Nguyen, editors, *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, pages 1–17, 2013.

[19] M. Giesbrecht, M. Jacobson, and A. Storjohann. Algorithms for large integer matrix problems. In *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, AAECC-14, pages 297–307, London, UK, UK, 2001. Springer-Verlag.

[20] S. Hallgren. Fast quantum algorithms for computing the unit group and class group of a number field. In *Proceedings of the 37th Annual ACM Symposium on Theory of Computing*, pages 468–474, 2005.

[21] S. Hallgren. Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem. *Journal of the ACM*, 54(1):1–19, 2007.

[22] J. Hoffstein, N. Howgrave-Graham, J. Pipher, J. Silverman, and W. Whyte. NTRUSign: Digital signatures using the NTRU lattice. In *Proceedings of the 2003 RSA Conference on The Cryptographers' Track*, CT-RSA'03, pages 122–140, Berlin, Heidelberg, 2003. Springer-Verlag.

[23] D. Jao and V. Soukharev. A subexponential algorithm for evaluating large degree isogenies. In G. Hanrot, F. Morain, and E. Thomé, editors, *Algorithmic Number Theory*, volume 6197 of *Lecture Notes in Computer Science*, pages 219–233. Springer Berlin Heidelberg, 2010.

[24] H. Lenstra and C. Pomerance. A rigorous time bound for integer factoring. *Journal of the American Mathematical Society*, 5(3):483–516, 1992.

[25] J.E. Littlewood. On the class number of the corpus $p(\sqrt{-k})$. *Proc. London Math.Soc*, 27:358–372, 1928.

[26] F. Lübeck. On the computation of elementary divisors of integer matrices. *J. Symb. Comput.*, 33(1):57–65, 2002.

[27] J. Neukirch. *Algebraic number theory*. Comprehensive Studies in Mathematics. Springer-Verlag, 1999. ISBN 3-540-65399-6.

[28] A. Schmidt and U. Vollmer. Polynomial time quantum algorithm for the computation of the unit group of a number field. In *Proceedings of the 37th Annual ACM Symposium on Theory of Computing*, pages 475–480, 2005.

[29] P. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

[30] D. Simons. Solving norm equations in relative number fields using s-units. *Mathematics of Computation*, 71(239):1287–1305, 2002.

[31] N. Smart and F. Vercauteren. Fully homomorphic encryption with relatively small key and ciphertext sizes. In P. Nguyen and D. Pointcheval, editors, *Public Key Cryptography - PKC 2010*, volume 6056 of *Lecture Notes in Computer Science*, pages 420–443. Springer Berlin Heidelberg, 2010.