QUANTUM ALGORITHMS IN ALGEBRAIC NUMBER THEORY

SIMON RUBINSTEIN-SALZEDO

Abstract. In this article, we discuss some quantum algorithms for determining the group of units and the ideal class group of a number field. Assuming the generalized Riemann hypothesis, we will show furthermore that these algorithms require only quantum polynomial time.

1. Introduction

Two very important problems in computational algebraic number theory are the computations of the unit group and the ideal class group of an algebraic number field. These groups are very important objects both in algebraic number theory and in other areas of mathematics.

Ideal class groups of number fields were first studied by Gauß in 1798. They also played a major role in several early attempts at proving Fermat's Last Theorem starting with the work of Kummer. In particular, if p is an odd prime and p does not divide the class number of $\mathbb{Q}(\zeta_p)$, where ζ_p is a primitive p^{th} root of unity, then it can be shown (see [5]) without too much difficulty that

$$x^p + y^p = z^p$$

has no integer solutions in which $p \nmid xyz$. (The case of $p \mid xyz$ is also treated in [5], but it is more difficult.)

In this paper, we discuss algorithms that compute the unit group and the ideal class group of a number field in quantum polynomial time. The algorithms we study here are due to Hallgren [2]. In the classical case, these two problems are typically solved simultaneously. In the quantum case, however, we first need to compute the unit group, and then we use the result of that computation to compute the ideal class group.

2. Number Theoretic Preliminaries

Of key importance in algebraic number theory is the Galois group of a field extension; if L/K is a field extension, then $\text{Gal}(L/K)$ is the group of field automorphisms of L that fix every element of K. We frequently write elements of the Galois group multiplicatively, i.e. we write x^σ rather than $\sigma(x)$.

Definition 1. An (algebraic) number field K is a finite field extension of the field of rational numbers $\mathbb{Q}$ contained in the field of complex numbers $\mathbb{C}$. The ring of integers $\mathfrak{o} = \mathfrak{o}_K$ of K is the set of roots of monic polynomials $f(x) \in \mathbb{Z}[x]$ lying in K. The degree of K is the dimension of K considered as a vector space over $\mathbb{Q}$; we write $[K : \mathbb{Q}]$ for this number. If $[K : \mathbb{Q}] = d$, and $\mathfrak{o} = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_d$, then the discriminant of K is defined to be $\Delta = \det(\text{Tr}(\alpha_i\alpha_j))_{1\leq i,j,\leq d}$, where $\text{Tr} : F \to \mathbb{Q}$ is given by $x \mapsto \sum_{\sigma\in\text{Gal}(K/\mathbb{Q})} x^\sigma$.

It turns out (see e.g. Chapter 4 of [1]) that the structure of the group of units $\mathfrak{o}^\times$ of $\mathfrak{o}$ can be described quite explicitly.

Theorem 2. *(Dirichlet's Unit Theorem.) Suppose K is a number field. If K has r_1 distinct embeddings into $\mathbb{R}$ and r_2 complex conjugate pairs of embeddings into $\mathbb{C}$, and μ_K is the group of roots of unity of K, then*

$$\mathfrak{o}^\times \cong \mu_K \oplus \mathbb{Z}^{r_1+r_2-1}.$$

Therefore to compute the unit group of a number field, it suffices to list generators of the torsion-free part of $\mathfrak{o}^\times$.

In the case of a real quadratic field $\mathbb{Q}(\sqrt{d})$, $d > 0$ a squarefree integer, finding a generator of the torsion-free part of $\mathfrak{o}^\times$ is equivalent to finding the smallest nontrivial solution to Pell's equation $x^2 - dy^2 = 1$.

Another important group in algebraic number theory is the ideal class group. To define the ideal class group, we first need the notion of a (fractional) ideal.

Definition 3. A fractional ideal of $\mathfrak{o}$ is a finitely generated $\mathfrak{o}$-submodule of K.

It is well-known that in a Dedekind domain (such as the ring of integers of a number field), every fractional ideal is invertible. (That is, for every fractional ideal $\mathfrak{a}$, there is another fractional ideal $\mathfrak{b}$ so that $\mathfrak{a}\mathfrak{b} = \mathfrak{o}$.) Therefore the fractional ideals of $\mathfrak{o}$ form an abelian group under multiplication with identity $\mathfrak{o}$; this group is denoted by I_K. The principal fractional ideals (i.e. those of the form $a\mathfrak{o}$ for some $a \in K^\times$) form a subgroup P_K of I_K.

Definition 4. The ideal class group $\mathrm{Cl}(K)$ of K is the quotient group I_K/P_K.

The major result about ideal class groups is the following theorem:

Theorem 5. *If K is a number field, then* $\mathrm{Cl}(K)$ *is a finite group. We call its order the class number of K.*

3. The Algorithm for Computing the Unit Group

In what follows, we will assume that we are fixing a positive integer $d \geq 2$, and that the number fields considered are of degree d. We will enter the number field by inputting the discriminant Δ of K. Our algorithms will run in polynomial time in $\log|\Delta|$ and d.

The output format is slightly more problematical: in general, a generating set for the unit group will not be polynomial in $\log|\Delta|$. However, the logarithms of the elements of the generating set is polynomial in $\log|\Delta|$; therefore if α is in the generating set, we will output the vector $\mathrm{Log}(\alpha) = (\log|\alpha|_1, \ldots, \log|\alpha|_r)$, where $|\cdot|_i$ runs over some $r = r_1 + r_2 - 1$ of the $r_1 + r_2$ absolute values determined by embeddings of K into $\mathbb{C}$. (Complex conjugate pairs of embeddings into $\mathbb{C}$ determine the same absolute value.) These vectors will not be precisely units since the logarithms will be irrational; however, we can specify them to the necessary degree of precision.

Under this logarithm map, the units of $\mathfrak{o}$ (modulo the roots of unity, which can easily be computed) become a lattice in $\mathbb{R}^r$. Therefore it will be necessary to study lattices on $\mathbb{R}^r$.

The logarithm map allows us to talk about reduced ideals. We call a fractional ideal I reduced if $1 \in I$ and for any $\alpha \neq 0$ in I, at least one coordinate of $\mathrm{Log}(\alpha)$ is nonnegative. In the following, we generally implicitly assume that our ideals are reduced without mentioning it every time. More generally, we say that $\mu \in I$ is a minimal element of I if for any $\alpha \neq 0$ in I, some coordinate of $\mathrm{Log}(\alpha) - \mathrm{Log}(\mu)$ is nonnegative. Hence a fractional ideal is reduced if 1 is a minimal element.

We first state the algorithm. Later, we will explain how the difficult step can be implemented on a quantum computer.

Theorem 6. *There exists an algorithm which computes generators for the unit group of a number field K in quantum polynomial time. More precisely, if we enter a number field whose logarithmic unit group is L, the algorithm will provide a set of vectors which approximate a basis for L.*

1. *Find a basis for the dual basis $L^{\perp} = \{u \in \mathbb{R}^r \mid u \cdot v \in \mathbb{Z} \text{ for all } v \in L\}$ as follows:*
   (a) *Take a Fourier sampling of an appropriate lattice-hiding function f_N a constant number of times.*
   (b) *Use a spanning set of vectors to compute a basis B.*
2. *Compute $(B^{-1})^t$, and use this matrix to find a basis for L.*
3. *Check that the resulting vectors correspond to units of K. If they do not, try the algorithm again.*

By far the most difficult part of this algorithm (and also the only part that involves quantum computers!) is step (1). We will describe how to do step (1) in the next section. It will be done by an application of the hidden subgroup problem on $\mathbb{R}^r$ that we will be able to solve.

In order to apply the hidden subgroup algorithm in the next section, we first need a function hiding the logarithmic unit group L. We define $f : \mathbb{R}^r \to I_K \times \mathbb{R}^r$ by $x \mapsto (I_x, \delta_x)$, where $I_x = \frac{1}{\mu}\mathfrak{o}$ is an ideal with minimal element μ so that $|\,\mathrm{Log}\,\mu - x|$ is minimized, and every coordinate of $\mathrm{Log}\,\mu - x$ is nonnegative. We then set $\delta_x = x - \mathrm{Log}\,\mu$.

In quantum algorithms, we must typically work with discrete functions, so we define $f_N : \mathbb{Z}^r \to I_K \times \mathbb{Z}^r$ by $f_N(i) = (I_{i/N}, k_{i/N})$, where the j^{th} coordinate of $k_{i/N}$ is $\lfloor N(\delta_{i/N})_j \rfloor$.

4. Hidden Subgroups on $\mathbb{R}^r$

In this section, we discuss how to retrieve a hidden lattice L from a function f_N which hides it. This process can then be applied to the function f_N and the lattice L from the previous section. Our method for computing a basis of L will be to start by finding a basis matrix B of $L^{\perp}$. Once we have done that, $(B^{-1})^t$ will be a basis for L.

The first step in our quantum algorithm for finding the unit group of a number field involves solving a special case of the hidden subgroup problem over $\mathbb{R}^r$. Let $L \subseteq \mathbb{R}^r$ be an r-dimensional lattice, S a set, and $f : \mathbb{R}^r \to S$ a function with the property that $f(x) = f(y)$ if and only if $x - y \in L$. Now let N be a positive integer. A function $f_N : \mathbb{R}^r \to S$ is said to hide L if an arbitrary point $i \in \mathbb{Z}_q^r$ satisfies the following with inverse polynomial (in q) probability: for all $j \in \mathbb{Z}_q^r$, $f_N(i) = f_N(j)$ if and only if there exists a $v \in L$ such that $\left|\frac{i-j}{N} - v\right| \leq \frac{1}{N}$. (This means that there is an element of the coset $\frac{i-j}{N} + L$ of $\mathbb{R}^r$ whose absolute value is at most $\frac{1}{N}$.)

We now show how, given a function f_N hiding a lattice L, to construct a basis of the dual lattice $L^\perp$. We will also need to assume that there exists some $M \in \mathbb{R}$ such that if B is any basis matrix for L (i.e. the columns of B form a basis for L), then $\|B\| \cdot \|B^{-1}\| \leq M$, where $\|A\|$ is the absolute value of the largest entry of A.

Let $L_q = L \cap [0, q)^r$, and let $\lfloor \cdot \rceil : \mathbb{R} \to \mathbb{Z}$ be the function that sends x to the nearest integer to x; we extend $\lfloor \cdot \rceil$ componentwise to $\mathbb{R}^r$. Let us start with a quantum state

$$\frac{1}{\sqrt{q^r}} \sum_{k \in \mathbb{Z}_q^r} |k, f_N(k)\rangle.$$

We now measure the second component of our quantum state so that it collapses to

$$\frac{1}{\sqrt{|L_q|}} \sum_{\substack{v \in L \\ k_0 + v \in [0,q)^r \\ k_0 \text{ fixed}}} |\lfloor N(k_0 + v) \rceil\rangle$$

for some k_0. Since $Nk_0 \in \mathbb{Z}$, we have $\lfloor Nk_0 + Nv \rceil = Nk_0 + \lfloor Nv \rceil$. We will perform a Fourier sampling, so we may ignore Nk_0. Thus we need only concern ourselves with states of the form

$$\frac{1}{\sqrt{|L_q|}} \sum_{\substack{v \in L_q \\ k_0 + v \in [0,q)^r \\ k_0 \text{ fixed}}} |\lfloor Nv \rceil\rangle.$$

Now let M be the length of the longest basis vector of L with respect to some fixed basis. If we choose q to be sufficiently large, then the set of points within rM of the boundary of the parallelepiped decreases exponentially with q, so the state above is exponentially near to

$$\frac{1}{\sqrt{|L_q|}} \sum_{v \in L_q} |\lfloor Nv \rceil\rangle.$$

We now apply a Fourier transform over $\mathbb{Z}_{qNk}^r$ to obtain

$$\frac{1}{|L_q|} \frac{1}{\sqrt{(qNk)^r}} \sum_{i \in \mathbb{Z}_{qNk}^r} \sum_{v \in L_q} \zeta_{qNk}^{i \cdot \lfloor Nv \rceil} |i\rangle,$$

where $\zeta_{qNk} = e^{2\pi i/(qNk)}$. Now let $w \in L^\perp$ and $i = \lfloor kqw \rceil$. We now let $n = \lceil \log \Delta \rceil$. We will discard any points for which $i_j > \frac{qNk}{n}$ for some j (where i_j is the j^{th} entry of i). We then have $|w_j| \leq \frac{N}{n} + 1$ for points that we keep; hence choosing N larger will give us more samples. We can bound the inner product $i \cdot \lfloor Nv \rceil$ in the exponent:

$$i \cdot \lfloor Nv \rceil = (qkw + \delta_w) \cdot (Nv + \varepsilon_v) = qNk + qk(w \cdot \varepsilon_v) + \delta_w \cdot (Nv + \varepsilon_v),$$

where $-\frac{1}{2} \leq (\delta_w)_j, (\varepsilon_v)_j \leq \frac{1}{2}$. The first term on the right is congruent to zero modulo qNk since $w \in L^\perp$. For the second term, we have

$$\frac{qk(w \cdot \varepsilon_v)}{qNk} \leq \frac{r}{n}.$$

For the last term, if we take k to be sufficiently large, we have

$$\frac{\delta_w \cdot (Nv + \varepsilon_v)}{qNk} \leq \frac{1}{8}.$$

Hence the probability of finding an integer vector $i \in \mathbb{Z}^r$ after measurement is at least $\frac{|L_q|}{2(qNk)^r}$. Since $|L_q| \geq \frac{q^r}{2\det(L)}$ (see [3]) and $|L^\perp_{N/n}| \geq \frac{(N/n)^r}{2\det(L^\perp)}$ for sufficiently large q and N, we have

$$\frac{|L_q|}{2(qNk)^r} \geq \frac{1}{8(nk)^r|L^\perp_{N/n}}.$$

When this happens, we have

$$\frac{i}{qk} - w = \frac{kqw + \delta_w}{qk} - w = \frac{\delta_w}{qk},$$

so $\frac{i}{qk}$ is within $\frac{1}{q}$ of a point in $L^\perp$, so the probability of sampling a point within $\frac{1}{q}$ of a point in $L^\perp$ is at least $\frac{1}{8(nk)^r}$.

In particular, we have shown the following:

Lemma 7. *Let N and q be sufficiently large. Let f_N be a function hiding a lattice in $\mathbb{R}^r$. If we Fourier sample over $\mathbb{Z}^r_{qNk}$ and discard points with any coordinate greater than $\frac{qNk}{n}$ until we find one that is not discarded, then for the resulting point $i \in \mathbb{Z}^r_{qNk}$, $\frac{i}{kq}$ is within $\frac{1}{q}$ of a point in $L^\perp$.*

5. The Principal Ideal Algorithm

Before we discuss a quantum algorithm for computing the ideal class group, we must tackle another problem: Given an ideal I of $\mathfrak{o}$, determine whether I is a principal ideal, and if it is, find an $\alpha \in I$ such that $I = \alpha\mathfrak{o}$. In fact, we will always find some α in this algorithm; we can then check if $I = \alpha\mathfrak{o}$ to determine whether I is indeed a principal ideal.

Let $x = \operatorname{Log}\alpha$. If I is a principal ideal, then $I = \alpha\mathfrak{o} = I_x$. We define $g : \mathbb{Z} \times \mathbb{R}^r \to \mathcal{I} \times \mathbb{R}$ by $(a, y) \mapsto f(ax - y)$, and the discrete version of g is $g_N : \mathbb{Z} \times \mathbb{Z}^r \to I_K \times \mathbb{Z}$ given by $(a, b) \mapsto f\left(ax - \frac{b}{N}\right)$. Hence we need to compute $I_{ax-b/N}$ and $\delta_{ax-b/N}$. These can be computed in quantum polynomial time.

The function g_N hides the lattice $\Lambda = \{(a, y) \in \mathbb{Z} \times \mathbb{R}^r \mid ax - y \in L\}$, where L is the logarithmic unit group lattice. A basis of Λ is $\{(1, x), (0, v_1), \ldots, (0, v_r)\}$, where $v_1, \ldots, v_r$ form a basis for L. By the algorithm described above, we can compute a basis for Λ in quantum polynomial time. (However, the basis given by the algorithm will not necessarily be the above basis.)

Once we have some basis for Λ, we need to find x. Pick two basis vectors of Λ whose first coordinates are relatively prime and find a linear combination $(1, y)$ of these two basis vectors. Then $x - y \in L$, so $y = \operatorname{Log}(\varepsilon\alpha)$ for some $\varepsilon \in \mathfrak{o}^\times$, and $I = \alpha\mathfrak{o} = \varepsilon\alpha\mathfrak{o}$. Now reduce y modulo the basis of L. This gives us the coordinates of x and hence α.

We can carry out this algorithm regardless of whether I is a principal ideal. We then end up with some $\alpha \in I$. We can then check if $I = \alpha\mathfrak{o}$ and determine whether I is a principal ideal. Hence we have the following result:

Theorem 8. *Given an ideal $I \subseteq \mathfrak{o}$, we can determine in quantum polynomial time whether there is some $\alpha \in I$ such that $I = \alpha\mathfrak{o}$. Furthermore, if such an α exists, we can find one in quantum polynomial time.*

6. The Ideal Class Group

Finally, we are able to compute the ideal class group of a number field K. By this, we mean that we wish to determine the structure of the group. Since class groups are finite abelian groups, we can write $\mathrm{Cl}(K) \cong \mathbb{Z}_{a_1} \oplus \mathbb{Z}_{a_2} \oplus \cdots \oplus \mathbb{Z}_{a_\ell}$.

It is shown in [4] that, assuming the generalized Riemann hypothesis, we can find generators $g_1, \dots, g_m$ of $\mathrm{Cl}(K)$ in polynomial time. Having done this, we reduce the problem of determining the structure of $\mathrm{Cl}(K)$ to the hidden subgroup problem on $\mathbb{Z}^m$ as follows: Define $f : \mathbb{Z}^m \to G$ by $(e_1, \dots, e_m) \mapsto g_1^{e_1} \cdots g_m^{e_m}$. Then the hidden subgroup is $\ker(f) = \{(e_1, \dots, e_m) \mid g_1^{e_1} \cdots g_m^{e_m} = 1\}$.

In fact, we can reduce this to period finding on $\{1, 2, 3, \dots, M\}$ for some M that is "not too big" as follows: By the Minkowski bound (see Theorem 35 of [1]) for the norms of ideals in ideal classes, we need only look at those integral ideals above $\mathbb{Z}$-ideals up to

$$\left(\frac{4}{\pi}\right)^{r_2} \frac{d!}{d^d}\sqrt{|\Delta|} \le \left(\frac{4}{e\pi}\right)^{d} \sqrt{2\pi d|\Delta|}.$$

There can only be d ideals above a given $\mathbb{Z}$-ideal, so we can let M be $O(d^{3/2}\sqrt{|\Delta|})$. We can now use the ordinary period-finding algorithm on $\mathbb{Z}_M^d$, which will compute the periods in polynomial time. We now apply the following algorithm on each coordinate axis to find the coordinate periods p:

(1) Set up a superposition

$$\frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x, 0\rangle.$$

(2) Apply f to the above superposition, leaving us with

$$\frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x, f(x)\rangle \approx \frac{1}{\sqrt{M}} \sum_{y=0}^{p-1} \left(\sum_{t=0}^{M/p-1} |tp + y\rangle \right) \otimes |f(y)\rangle.$$

(3) Measure the right register above. If we end up with $F(c)$ for $0 \le c < p$, then our superposition collapses to

$$\sqrt{\frac{p}{M}} \sum_{t=0}^{M/p-1} |tp + c\rangle.$$

(4) Apply a Fourier transform over $\mathbb{Z}_M$ to get

$$\frac{\sqrt{p}}{M} \sum_{j=0}^{M-1} \zeta_M^{jc} \left(\sum_{t=0}^{M/p-1} \zeta_M^{jtp} \right) |j\rangle \approx \frac{1}{\sqrt{p}} \sum_{k=0}^{p-1} \zeta_M^{ckM/p} |kM/p\rangle.$$

(5) Take a measurement of the above superposition. With high probability, we will end up with a multiple of M/p.
(6) Apply the above steps several times.
(7) Take the greatest common divisor of the above numbers to determine M/p; this then tells us p.

At this point, we have only to solve the hidden subgroup problem on $\mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_m}$, and this can be done in polynomial time.

However, there is a slight problem in that it is not clear how to run the hidden subgroup algorithm without first finding representatives of the ideal classes. Hence, to run this algorithm, we need to create a superposition of reduced ideals in a given ideal class. To construct a superposition of reduced ideals with ideal class $g_1^{e_1} \cdots g_m^{e_m}$, we first compute the $\mathfrak{o}^\times$ and get a basis B for the logarithmic unit group. The basis vectors for $\operatorname{Log} \mathfrak{o}^\times$ form a parallelepiped. We now apply f_N from §3 and compute the superposition

$$\frac{1}{\sqrt{N^r}} \sum_{i \in \mathbb{Z}_N^r} |i, f_N(B \times i)\rangle = \frac{1}{\sqrt{N^r}} \sum_{i \in \mathbb{Z}_N^r} |i, I_{B \times i/N}, k_{B \times i/N}\rangle.$$

Then apply the principal ideal algorithm to the second register of the superposition on the right above with basis B. This process allows us to delete the first register, leaving only the superposition

$$\frac{1}{\sqrt{N^r}} \sum_{i \in \mathbb{Z}_N^r} |I_{B \times i/N}, k_{B \times i/N}\rangle.$$

We are now in a position to apply the hidden subgroup algorithm for $\mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_m}$ in quantum polynomial time, so we have the following result:

Theorem 9. *Assuming the generalized Riemann hypothesis, we can compute the structure of* $\mathrm{Cl}(K)$ *in quantum polynomial time.*

References

[1] A. Fröhlich and M. J. Taylor. *Algebraic number theory.* Cambridge Studies in Advanced Mathematics **27**, Cambridge University Press, Cambridge, England, 1991.

[2] S. Hallgren. "Fast quantum algorithms for computing the unit group and class group of a number field." *Annual ACM Symposium on Theory of Computing, Proceedings of the thirty-seventh annual ACM symposium on theory of computing*, ACM Press, Baltimore, Maryland, USA, 2005.

[3] D. Micciancio and S. Goldwasser. *Complexity of lattice problems: a cryptographic perspective.* The Kluwer International Series in Engineering and Computer Science **671**, Kluwer Academic Publishers, Boston, Massachusetts, USA, 2002.

[4] C. Thiel. *On the complexity of some problems in algorithmic algebraic number theory.* PhD thesis, Universität des Saarlandes, Saabrücken, Germany, 1995.

[5] L. C. Washington. *Introduction to cyclotomic fields*, Second Edition. Graduate Texts in Mathematics **83**, Springer-Verlag, New York, New York, USA, 1997.

Department of Mathematics, University of California, Santa Barbara, CA 93106
E-mail address: complexzeta@gmail.com