Polynomial Time Quantum Algorithm for the Computation of the Unit Group of a Number Field

Arthur Schmidt*, Ulrich Vollmer

Technische Universität Darmstadt, Fachbereich Informatik
Fachgebiet Kryptographie und Computeralgebra
Hochschulstr. 10, 64289 Darmstadt

Abstract. We present a quantum algorithm for the computation of the irrational period lattice of a function on $\mathbb{Z}^n$ which is periodic in a relaxed sense. This algorithm is applied to compute the unit group of finite extensions of $\mathbb{Q}$. Execution time for fixed field degree over $\mathbb{Q}$ is polynomial in the discriminant of the field. Our algorithms generalize and improve upon Hallgren's work [Hal02] for the one-dimensional case corresponding to real-quadratic fields.

1 Introduction

In [Hal02] Sean Hallgren has extended the notion of periodicity of a function to include a class of functions on $\mathbb{Z}$ with irrational periods. He showed extending earlier work of Shor [Sho97] and others how an approximation to the period can be computed via Quantum Fourier Transform (QFT). His algorithm executes in polynomial time provided function values can be computed within time polynomial in the period and the size of the arguments. Hallgren then applied the proposed technique to compute the regulator of a real-quadratic field.

We extend Hallgren's work to functions on $\mathbb{Z}^n$. Unlike the work of Simon in [Sim94] or of Boneh and Lipton [BL95], we do not assume the periods to have rational co-ordinates. Moreover, we relax the requirement of periodicity of the function: we allow the period lattice to be disturbed, and periodicity to hold for only a constant fraction of starting values.

This generalized frame-work is then applied to a classical number-theoretic problem, the computation of the unit group of an algebraic number field which is a finite extension of $\mathbb{Q}$. The resulting algorithm represents an exponential speed-up over the best classical deterministic algorithm presented by Buchmann [Buc87b] which builds on ideas going back to Lagrange. There is only heuristic proof of a sub-exponential run-time bound for the best probabilistic algorithms for a classical computer, also by Buchmann [Buc90], [BJP94].

In the course of this generalization we also close a gap left open by Hallgren in the above cited paper: The periodic function defined and used by Hallgren cannot—at least as far as

* research supported by the DFG

we know today—computed in polynomial time. Desrosier [Des02] attempted to remedy this problem by substituting Hallgren's function with an arbitrary other one that approximates it and bounding the errors introduced thereby. He did not show, however, how to construct one such function that still is periodic with the same period, *and* computable in polynomial time.

In this paper, we remedy this problem and present a generalized variant of Hallgren's function that combines both properties: computability in polynomial time for all arguments, and periodicity. For this, we draw on work by Buchmann [Buc87a], [Buc87b] and Thiel [Thi95].

Theorem 1. *There is an algorithm that given an order $\mathcal{O}$ in a finite extension field of $\mathbb{Q}$ runs in polynomial time and computes a set of units in this order which generate a subgroup of finite index in the unit group of $\mathcal{O}$ in such manner that, with pre-determined probability, this sub-group equals the full unit group.*

Like in Hallgren's original work, the algorithms presented here can be adapted to compute generators of principal ideals of an order in the given field. Thus they can be used to attack number field crypto-systems as they were proposed, e.g., in [BMM00] in quantum polynomial time.

For purposes of determining the run-time asymptotics of the algorithms given in this paper we will only consider the dependance on the determinant of the period lattice of the examined periodic function, and keep the dimension fixed.

In the context of our arithmetic application this means that we study dependence on the growth of the discriminant of the field, keeping its degree n over $\mathbb{Q}$ and its unit rank fixed. A quantity is considered to grow linearly, polynomially, or exponentially if it is in $O(\log \Delta)$, $O((\log \Delta)^c)$ for some $c \in \mathbb{R}$, or $O(\Delta^{c'})$ for some $c' \in \mathbb{R}$, respectively, where the O-constants might depend exponentially on n.

The paper is structured as follows. In the second section we define loose periodicity, give the algorithm for computing the period lattices of loosely periodic functions, and prove its properties. In the third section we give the necessary background for the number-theoretic application, fixing notation and citing the results by Buchmann and Thiel we rely on. In the fourth section we introduce the notion of distinguished binary representation of a minimum of a reduced ideal in a number field. This represents a technical tool necessary to achieve a polynomial run-time bound for the periodic function introduced in section five. We conclude with an out-look to further work in this area.

2 Multi-Dimensional Quantum Fourier Transform

In this section we define the concept of a loosely periodic function, and show how the period lattice of a loosely periodic function can be computed via QFT. As in Kitaev's work

[Kit96], our quantum algorithm actually computes the lattice which is dual to the period lattice. The computation of the period lattice itself is left to a classical post-computation.

We follow here, as does Hallgren [Hal02], Shor's QFT approach. It should be noted, however, that it seems equally possible to solve the given task via Kitaev's Eigenvalue Estimation technique [Kit96], see also Mosca and Ekert's work [ME99], and Jozsa's comparison [Joz98] of both approaches.

Definition 1. *Let $r \in \mathbb{N}$, and $\mathcal{S}$ be some set. A function $f : \mathbb{Z}^r \longrightarrow \mathcal{S}$ is called* loosely periodic *with period lattice $\mathit{\Lambda} \subset \mathbb{R}^r$ if a non-zero fraction of all $\mathbf{v} \in \mathbb{Z}^r$ with coordinates bounded by some B in $O(\log \mathit{\Delta})$ has the property that for all $\lambda \in \mathit{\Lambda}$ there exists some $\mathbf{w} \in \mathbb{R}^r$ such that*

1. $\|\mathbf{w}\|_\infty < 2$,
2. $\mathbf{v} + \lambda + \mathbf{w} \in \mathbb{Z}^r$,
3. $f(\mathbf{v}) = f(\mathbf{v} + \lambda + \mathbf{w})$.

Moreover, we require that for $\mathbf{v}$ with this property $f(\mathbf{v}) = f(\mathbf{v}')$ for some $\mathbf{v} \in \mathbb{Z}^r$ implies that there exist $\lambda \in \mathit{\Lambda}$ and $\mathbf{w} \in \mathbb{R}^r$ with the aforementioned properties such that $\mathbf{v} - \mathbf{v}' = \lambda + \mathbf{w}$.

Note that the latter condition which could also be formulated as local injectivity was missing from Hallgren's definition of periodicity, although the number-theoretic function defined by him is, indeed, locally injective (if computed precisely). The condition is required for the plain Quantum Fourier Transform used here to work. It seems likely, however, that using the technique from [HH00] it is possible to do without.

We will now describe an algorithm that computes the period lattice of loosely periodic functions in the following sense. It computes a set of vectors $\tilde{\mathbf{v}}_1, \ldots, \tilde{\mathbf{v}}_r$ in $\mathbb{R}^r$ which with constant pre-determined probability have the property that there exists a basis $\{\mathbf{v}_1, \ldots, \mathbf{v}_r\}$ of the period lattice $\mathit{\Lambda}$ of f with $\|\tilde{\mathbf{v}}_i - \mathbf{v}_i\|_2 < c$ with *a priori* chosen c.

The run-time of the algorithm on input of function f can be bounded by a product of the following factors:

1. a polynomial in the determinant of the period lattice of f;
2. the time needed to compute f on input of size $O(\det(\mathit{\Lambda})/\lambda_1(\mathit{\Lambda}))$, where $\lambda_1(\mathit{\Lambda})$ is the first successive minimum of $\mathit{\Lambda}$.
3. the inverse of the density of $\mathbf{v}$ for which periodicity can be guaranteed;
4. the inverse of the first successive minimum of the period lattice.

We denote by $\cdot$ the dot product of two vectors and by $\mathit{\Lambda}^*$ the lattice which is dual to $\mathit{\Lambda}$, i.e. $\mathit{\Lambda}^* = \{\mathbf{v} \in \operatorname{span}(\mathit{\Lambda}) \mid \forall \mathbf{u} \in \mathit{\Lambda} : \mathbf{v} \cdot \mathbf{u} \in \mathbb{Z}\}$

We shortly describe our algorithm. The idea is to generalize Shor's algorithm to multiple dimensions. First we create in first n registers a superposition of $\mathbf{v}$ and compute

$f(\mathbf{v})$ in the last register. After measuring a random $f(\mathbf{v}')$ we get in the first r registers a superposition of $\mathbf{v}$ with $f(\mathbf{v}) = f(\mathbf{v}')$. These $\mathbf{v}$ build a lattice disturbed by an error term. Next we apply the quantum Fourier transform to each of the first r registers. Then, the resulting state is a superposition of points in Λ^*, the dual lattice, which are also disturbed by an error term. Finally, we measure one of those points.

We repeat the above procedure $O(\operatorname{poly}\log(\det(\Lambda)))$ times. Then, with probability exponentially close to one, we get a basis of Λ^*. Now, classically, we compute the dual lattice of Λ^*, which is the original Λ.

Let $q \gg \det(\Lambda)$ be a power of two. For our algorithm, we use r registers of the length $\operatorname{size}(2rq)$ and one register which is big enough to store $f(\mathbf{v})$.

The quantum part of our algorithm proceeds as follows. We begin with a superposition of $\mathbf{v}$ from 0 to $q-2$ and compute $f(\mathbf{v})$. Note that the maximum value of $\mathbf{v}$ is $q-2$ and not $2qr-1$. This constraint helps us to confine the errors caused by the factor $\mathbf{w}(\lambda)$ in the function f. We get the state

$$\frac{1}{(q-1)^{r/2}} \sum_{v_1=0}^{q-2} \cdots \sum_{v_r=0}^{q-2} |v_1\rangle \ldots |v_r\rangle |f(\mathbf{v})\rangle$$

After measuring the last register we get

$$\frac{1}{\sqrt{p}} \sum_{\lambda \in \mathcal{L}} |\mathbf{v}' + \lambda + \mathbf{w}(\lambda)\rangle |f(\mathbf{v}')\rangle$$

where $\mathbf{v}'$ is random and $\mathcal{L} \subset \Lambda$ such that $\mathbf{v}' + \lambda + \mathbf{w}(\lambda) \in \{\mathbf{v} \in \mathbb{R}^r \mid 0 \le v_j < q-2,\ j = 1 \ldots r\}$. Since we have chosen $q \gg \det(\Lambda)$, we have

$$p = \operatorname{card}\,\{\lambda \in \mathcal{L}\} \approx \frac{\text{volume of } \{\mathbf{u} \in \mathbb{R}^r | 0 \le u_i < q,\ i = 1 \ldots r\}}{\text{volume of a fundamental parallelepiped of } \Lambda} = \frac{q^r}{\det(\Lambda)}$$

Now, we classically test whether $f(\mathbf{v}')$ lies in the set for which periodicity can be guaranteed. If not, we restart the algorithm.

We apply the quantum Fourier transform to the first r registers and obtain the state

$$\frac{1}{\sqrt{(2rq)^r p}} \sum_{\lambda \in \mathcal{L}} \sum_{z_1,\ldots,z_r=0}^{2rq-1} \exp(2\pi i \frac{(\mathbf{v}' + \lambda + \mathbf{w}(\lambda)) \cdot \mathbf{z}}{2rq}) |z_1\rangle \ldots |z_r\rangle |f(\mathbf{v}')\rangle$$

The Fourier transform is shift invariant. So for probability estimation we can assume $\mathbf{v}' = 0$ and $\|\lambda\|_\infty < q$.

We want to estimate the probability to measure an approximation of a vector $\lambda^* \in \Lambda^*$, i.e. the probability to measure $\mathbf{z}$ with $\|\frac{1}{2rq}\mathbf{z} - \lambda^*\|_\infty \le \frac{1}{4rq}$. To keep the influence of the disturbing term $\mathbf{w}(\lambda)$ small, we consider only “small“ $\mathbf{z}$'s and restart the algorithm if $\mathbf{z}$ is too big. Let $\frac{1}{2rq}\mathbf{z} = \lambda^* + \delta(\mathbf{z})$, where $\|\mathbf{z}\|_\infty \le \frac{q}{32}$ and $\|\delta(\mathbf{z})\|_\infty \le \frac{1}{4rq}$. Then, we have

$$\begin{aligned}&\frac{1}{2qr}(\lambda + \mathbf{w}(\lambda)) \cdot \mathbf{z} = (\lambda + \mathbf{w}(\lambda)) \cdot (\lambda^* + \delta(\mathbf{z})) = \\ &\underbrace{\lambda \cdot \lambda^*}_{\in \mathbb{Z}} + \lambda \cdot \delta(\mathbf{z}) + \mathbf{w}(\lambda) \cdot (\lambda^* + \delta(\mathbf{z})) \equiv \lambda \cdot \delta(\mathbf{z}) + h(\lambda, \mathbf{z}) \mod 1\end{aligned}$$

where $|h(\lambda, \mathbf{z})| = |\mathbf{w}(\lambda) \cdot (\lambda^* + \delta(\mathbf{z}))| \le 2\frac{1}{2rq}\mathbf{z} \le \frac{1}{32}$.

Lemma 1. *Let $\Lambda \subset \mathbb{R}^r$ be a lattice and $\mathcal{L}$ a subset of Λ as defined above. Let $q \in \mathbb{Z}$ with $q \gg \det(\Lambda)$ and $q \gg \lambda_r(\Lambda^*)$,where $\lambda_r(\Lambda)$ is the rth successive minima of Λ^*, and $h(\lambda, \mathbf{z})$ a function with $|h(\lambda, \mathbf{z})| < \frac{1}{32}$. Assume $\mathbf{z} = 2rq(\lambda^* + \delta(\mathbf{z})) \in \mathbb{Z}^r$ with $\lambda^* \in \Lambda^*$, $\|\mathbf{z}\|_\infty \le \frac{q}{32}$ and $\|\delta(\mathbf{z})\|_\infty < \frac{1}{4rq}$. Set $p = \operatorname{card} \mathcal{L}$. Then the probability to measure such a $\mathbf{z}$ is*

$$\frac{1}{2^{r+1} r^r \det(\Lambda)} \lessapprox \frac{1}{(2qr)^r p} \left| \sum_{\lambda \in \mathcal{L}} \exp(2\pi i(\lambda \cdot \delta(\mathbf{z}) + h(\lambda, \mathbf{z}))) \right|^2 \lessapprox \frac{1}{2^r r^r \det(\Lambda)} \qquad (1)$$

The number of such $\mathbf{z}$'s is $\gtrapprox \frac{\det(\Lambda)}{(64r)^r}$ so that the probability to measure a “good” $\mathbf{z}$ is $\gtrapprox \frac{1}{2 \cdot 128^r r^{2r}}$ which is constant for fix r.

Proof. We prove the first statement. Since $\|\delta(\mathbf{z})\|_\infty \le \frac{1}{4rq}$ and $\|\lambda\|_\infty < q$ there exists some a with $-\frac{1}{4} \le a \le 0$ such that $a \le \lambda \cdot \delta(\mathbf{z}) \le a + \frac{1}{4}$ for all $\lambda \in \mathcal{L}$. Therefore, the angle between the vectors $\exp(2\pi i(\lambda \cdot \delta(\mathbf{z})))$ is at most $\frac{\pi}{2}$. We assume the worst case where the disturbing term $h(\lambda)$ is equal $-\frac{1}{32}$ for the first half of the vectors and $\frac{1}{32}$ for the second half of the vectors. It follows that the angle between the vectors $\exp(2\pi i(\lambda \cdot \delta(\mathbf{z}) + h(\lambda, \mathbf{z})))$ in the sum (1) is at most $\frac{3\pi}{4}$. If we turn each vector such that the y axis becomes the bisector between the extremal (outermost) vectors, the absolute value of the sum doesn't change and is at most $p \sin \frac{3\pi}{4} = \frac{\sqrt{2}p}{2}$. The upper bound of the sum can be achieved if all the vectors have the same direction. In this case the sum is equal to p. Since $p \sim \frac{q^r}{\det(\Lambda)}$, the first statement of the lemma holds.

We prove the second statement. Since $\det(\Lambda^*) = \frac{1}{\det(\Lambda)}$ and $\lambda_r(\Lambda^*) \ll q$, it follows

$$\operatorname{card} \{\mathbf{z} \in \mathbb{Z}^r \mid \frac{1}{2qr}\mathbf{z} - \delta(\mathbf{z}) \in \Lambda^* \text{ and } 0 \le \frac{z_j}{2qr} \le \frac{1}{64r},\ j = 1 \ldots r\} \approx \frac{\det(\Lambda)}{(64r)^r}. \qquad \square$$

From [Ban93], we have $1 \le \lambda_1(\Lambda)\lambda_r(\Lambda^*) \le Cr$ where C is constant. Since we have chosen $q \gg \lambda_1(L)$, we have $q \gg \lambda_r(\Lambda^*)$. Thus we see that if we measure the first r registers, we get a $\mathbf{z}$ from the “good” set with pre-determinable probability, and these $\mathbf{z}$ are chosen almost uniformly.

Finally, we have to prove that we need only a polynomial number of repetitions of the above procedure to get a generating set for Λ^*.

Lemma 2. *Let $\mathit{\Lambda}$ be a lattice of a fixed rank r. Then for $B_1 \in \mathbb{R}$, $B_1 > 10\sqrt{r}\lambda_r(\mathit{\Lambda})$, there is an algorithm which does the following. It samples at most $O(\operatorname{poly}\log(\det(\mathit{\Lambda})))$ random vectors λ from $\mathit{\Lambda} \cap \{\mathbf{x} \in \mathbb{R}^r \mid 0 \leq x_i < B,\ i = 0, \ldots, r\}$ and outputs with probability exponentially close to one a set of vectors from $\mathit{\Lambda}$ which generate $\mathit{\Lambda}$.*

Proof (of Lemma 2). We sketch a proof of Lemma 2.

Let λ_r be the rth successive minima of $\mathit{\Lambda}$, $B_1 = j\sqrt{r}\lambda_r$, where $j \in \mathbb{R}$ will be specified later, and $B_2 = B_1 - \lambda_r$. Set $\mathcal{A}_1 = \{\mathbf{v} \in \mathit{\Lambda} \mid 0 \leq v_i < B_1,\ i = 0, \ldots, r\}$ and $\mathcal{A}_2 = \{\mathbf{v} \in \mathit{\Lambda} \mid 0 \leq v_i < B_2,\ i = 0, \ldots, r\}$. Then, we have $\operatorname{card}\mathcal{A}_1 < \frac{(B_1+\sqrt{r}\lambda_r)^r}{\det(\mathit{\Lambda})}$ and $\operatorname{card}\mathcal{A}_2 > \frac{(B_2-\sqrt{r}\lambda_r)^r}{\det(\mathit{\Lambda})}$. It follows $\frac{\operatorname{card}\mathcal{A}_2}{\operatorname{card}\mathcal{A}_1} > \frac{1}{2^r}$ for $j > 10$ which is constant for a fixed r.

Now we describe the generating procedure of $\mathit{\Lambda}$. We denote by $\mathit{\Lambda}_i$ the lattice generated in step i. We begin with $\mathit{\Lambda}_0 = 0\mathbb{Z}$. While $\mathit{\Lambda}_i \neq \mathit{\Lambda}$ we do the following. In ith iteration we have two cases

1. $\operatorname{card}\mathit{\Lambda}_i \cap \mathcal{A}_2 \leq \frac{\operatorname{card}\mathcal{A}_2}{2}$. In this case there are at least $\frac{\operatorname{card}\mathcal{A}_2}{2}$ points which are not in $\mathit{\Lambda}_i$. The probability to sample such a point is at least $\frac{\operatorname{card}\mathcal{A}_2}{2\operatorname{card}\mathcal{A}_1} > \frac{1}{2^{r+1}}$.
2. $\operatorname{card}\mathit{\Lambda}_i \cap \mathcal{A}_2 > \frac{\operatorname{card}\mathcal{A}_2}{2}$. Since $\mathit{\Lambda}_i \neq \mathit{\Lambda}$, there is at least one vector $\lambda' \in \mathit{\Lambda}$ such that $\lambda' \notin \mathit{\Lambda}_i$ and $\|\lambda'\|_\infty \leq \lambda_r$. It follows that $\mathit{\Lambda}_i + \lambda' \cap \mathit{\Lambda}_i = \emptyset$ and $\mathit{\Lambda}_i \cap \mathcal{A}_2 + \lambda' \subset \mathcal{A}_1$. Therefore, the probability to sample a vector from $\mathit{\Lambda}_i + \lambda'$ is at least $\frac{\operatorname{card}\mathcal{A}_2}{2\operatorname{card}\mathcal{A}_1} > \frac{1}{2^{r+1}}$.

So in each step we get with constant probability (for fixed r) a vector λ' such that $\mathit{\Lambda}_i \subsetneq \mathit{\Lambda}_i + \lambda'\mathbb{Z}$. We set $\mathit{\Lambda}_{i+1} = \mathit{\Lambda} + \lambda'\mathbb{Z}$ and repeat the procedure.

We know that if $k > r + \log_2(B_1^r/\det(\mathit{\Lambda}))$, then we have $\mathit{\Lambda}_k = \mathit{\Lambda}$ (see [HV00] Theorem 3.1). Therefore the lemma holds. □

Collecting the results of this section, and using standard methods for the classical post-processing we obtain the following theorem.

Theorem 2. *Let f be a loosely periodic function with period lattic $\mathit{\Lambda} \subset \mathbb{R}^r$ as defined in Definition 1. Then for a fixed r, there is a quantum algorithm which computes a set of vectors $\tilde{\mathbf{v}}_1, \ldots, \tilde{\mathbf{v}}_r$ for which there exists with probability which can be bounded away from 0 independently from f a basis $\mathbf{v}_1 \ldots, \mathbf{v}_r$ of $\mathit{\Lambda}$ with $\|\tilde{\mathbf{v}}_i - \mathbf{v}_i\|_\infty < 1$. Its execution time is $O((\log(\det(\mathit{\Lambda}))/\lambda_1(\mathit{\Lambda}))^3)$ multiplied by the execution time of f for arguments in $O(\log(\det(\mathit{\Lambda}))/\lambda_1(\mathit{\Lambda}))$.*

3 Number theoretic background

In this section we recollect the relevant facts from number theory.

Let K be an algebraic number field of degree $n = s + 2t$ over $\mathbb{Q}$, where s is the number of real and t is the number of complex embeddings of K into $\mathbb{C}$. Let $m = s + t$, and $r = m - 1$. Let $|\ |_1, \ldots, |\ |_{s+t}$ be the normalized archimedean valuations on K. The height of a number α is the maximum $H(\alpha) = \max(\,|\alpha|_i \mid 1 \leq i \leq m\,)$.

Let $\mathcal{O}$ be an order in K. We denote the absolute value of the discriminant of $\mathcal{O}$ by Δ, the group of units of $\mathcal{O}$ by U, and the regulator of $\mathcal{O}$ by $R_{\mathcal{O}}$. A fractional $\mathcal{O}$-ideal is a free $\mathbb{Z}$-submodule of K of rank n with ring of multipliers $\mathcal{O}$.

Definition 2. *A number $\mu \neq 0$ in the fractional ideal $\mathfrak{a}$ is called a minimum of $\mathfrak{a}$ if there is no element $\alpha \neq 0$ in $\mathfrak{a}$ such that $|\alpha|_i < |\mu|_i$ for $1 \leq i \leq m$.*

For example, every number $\alpha \in \mathfrak{a}$ with minimal nonzero norm is a minimum of $\mathfrak{a}$. In particular, every unit is a minimum of $\mathcal{O}$. The set of all minima of the ideal $\mathfrak{a}$ will be denoted by $M_{\mathfrak{a}}$.

Definition 3. *A fractional $\mathcal{O}$-ideal is called reduced if* 1 *is one of its minima.*

The set of all principal reduced ideals $\mathcal{R}_{\mathcal{O}}$ is precisely the set of ideals $(\frac{1}{\mu})$ where μ runs through all minima of $\mathcal{O}$. Reduced ideals can be represented by a matrix of size linear in $\log \Delta$ (see [Buc87b]).

The group U operates multiplicatively on $M_{\mathfrak{a}}$, for any ideal $\mathfrak{a}$: If ξ is a unit, and μ is a minimum of $\mathfrak{a}$, then so is $\xi\mu$. We can identify the set of all orbits under this action with $\mathcal{R}_{\mathcal{O}}$.

Define the map

$$\mathbf{Log} \,:\, K^* \longrightarrow \mathbb{R}^r \,:\, \alpha \longmapsto (\log|\alpha|_1, \ldots, \log|\alpha|_r)$$

By the Dirichlet unit theorem, the image Λ of U under $\mathbf{Log}$ is a lattice of rank r in $\mathbb{R}^r$. The determinant of this lattice is called the regulator of $\mathcal{O}$ and is in $O(\Delta^{1/2+\epsilon})$. Its first successive minimum is bounded away from 0 by an expression depending solely on n and r.

The kernel of $\mathbf{Log}$ consists of the cyclotomic units in K. Each element of $\mathcal{R}_{\mathcal{O}}$ corresponds to a unique point in $\mathbb{R}^r/\Lambda$.

By assigning to each point $\mathbf{v}$ in $\mathbb{Q}^r$ the element of $\mathcal{R}_{\mathcal{O}}$ which is closest to $\mathbf{v}$ mod Λ we obtain a periodic function with period lattice Λ. In order to achieve local injectivity as required for the Quantum Fourier Transform, we will assign to $\mathbf{v}$ (following Hallgren) not only the closest minimum μ, but also a discrete measure of the distance of $\mathbf{v}$ to $\mathbf{Log}\,\mu$.

In order to compute this measure we need to compute an approximation to $\mathbf{Log}\,\mu$ starting from some representation of μ. It is generally not feasible to represent a minimum of $\mathcal{O}$ as a linear combination of elements of an integral basis of $\mathcal{O}$. We will make use of the so-called binary multiplicative representation by Thiel [Thi95].

A *multiplicative representation* of an algebraic number α is a pair $((\beta_1, \ldots, \beta_l), (e_1, \ldots, e_l))$ with $\beta_i \in K$, and $e_i \in \mathbb{N}$ for $1 \leq i \leq l$ such that $\alpha = \prod_{i=1}^{l} \beta_i^{e_i}$. If $e_i = 2^{k-i}$, then we speak of a binary multiplicative representation (BMR) of α. For minima of reduced ideals, there exist BMRs with entries of height bounded by $O(\Delta^{3/4\cdot(m+1)})$.

Note that the BMR of a minimum is not unique. We will show in Section 4 how to consistently single out one from among all BMRs of a given minimum.

Proposition 1. *For any fix $\delta > 0$, there is an algorithm that on input of a BMR $(\beta_1, \ldots, \beta_l)$ of a minimum μ of a reduced ideal computes $\mathbf{L} = (L_1, \ldots, L_r) \in \mathbb{Q}^r$ satisfying*

$$0 \leq L_i - \log|\mu|_i < \delta \tag{2}$$

in time $O((l \log \mathit{\Delta})^{2+\epsilon}(-\log \delta)^{1+\epsilon})$ with small $\epsilon > 0$.

Note that for different BMRs of one and the same minimum the value of $\mathbf{L}$ might vary.

A crucial result of Buchmann states that it is possible to enumerate all minima in the vicinity of a given point $\mathbf{v}$. For $\mathbf{v} \in \mathbb{R}^r$ and $s \in \mathbb{R}_{>0}$ define the set

$$\mathcal{B}(\mathbf{v}, s) = \{\, \mu \in M_{\mathcal{O}} \mid \|\mathbf{v} - \mathbf{Log}\,\mu\|_\infty < s \,\}$$

Proposition 2. *There exists a polynomial time algorithm that on input of $\mathbf{v} \in \mathbb{Q}^r$ computes a set M of minima with*

$$\mathcal{B}(\mathbf{v}, \frac{3 + \log \mathit{\Delta}}{4}) \subset M \subset \mathcal{B}(\mathbf{v}, \frac{4 + \log \mathit{\Delta}}{4}).$$

The minima are given in binary multiplicative representation $(\beta_1, \ldots, \beta_l)$ with $l \leq \log\|\mathbf{v}\|_\infty + 2$, and $H(\beta_i) \leq (4\mathit{\Delta})^{2(m+1)}$.

For a detailed proof, see [Thi95], Chapter 6. Given a minimum of $\mathcal{O}$ in BMR, Lemma 6.2.15 of the same work states, that we can also compute the reduced ideal $(1/\mu)$ in polynomial time.

Our algorithm needs to decide which of the enumerated minima lies closest to $\mathbf{v}$. This requires the computation of $\mathbf{Log}\,\mu$ for all $\mu \in M$. We cannot do this exactly. Moreover, to the best of our knowledge, the computation $\mathbf{Log}\,\mu$ to any *a priori* fixed precision does not allow to correctly make the decision. If, however, we successively increase the precision to break a tie, we might spend an amount of time on this single computation that exceeds any *a priori* given polynomial bound for the run-time of the total algorithm.

This is exactly the point where there remains a gap in Hallgren's proof of polynomial run-time of his algorithm for the quadratic case.

4 Distinguished BMRs of minima

In this section we will show how to assign to each minimum of a reduced ideal $\mathfrak{a}$ a single binary multiplicative representation. The choice will not be canonical as it depends on several parameters: two precision parameters $\delta > 0$, and $N \in \mathbb{N}$ with $\delta < 1/(2N)$ which we will specify later; and the choice of algorithms with properties as given by Proposition 1, and Proposition 2.

Therefore we fix some δ and some N; let $\mathbf{L}$ denote the function the first algorithm defines on BMRs of minima of $\mathcal{O}$; and let $\mathcal{M}$ denote the function on $\mathbb{Z}_N^r = (1/N)\mathbb{Z}^r$ with values in the power set of $M_{\mathcal{O}}$ given by the second.

Given a minimum μ, and a subset $\mathcal{N}$ of $\{\, \mathbf{v} \in \mathbb{Z}_N^r \mid \mu \in \mathcal{B}(\mathbf{v}, \frac{3+\log\varDelta}{4}) \,\}$ we can assign to any $\mathbf{w} \in \mathcal{N}$ the BMR of μ contained in $\mathcal{M}(\mathbf{w})$. We will denote this BMR by $\boldsymbol{\beta}(\mathbf{w})$, and $\mathbf{L}(\boldsymbol{\beta}(\mathbf{w}))$ by $\mathbf{L}_{\mathbf{w}}(\mu)$.

A member $\mathbf{w}$ of $\mathcal{N}$ is said to be closest to μ in $\mathcal{N}$ if for any $\mathbf{w}' \in \mathcal{N}$ we have

$$\begin{array}{ll} \text{either} & \|\mathbf{w} - \mathbf{L}_{\mathbf{w}}(\mu)\|_\infty < \|\mathbf{w}' - \mathbf{L}_{\mathbf{w}'}(\mu)\|_\infty \\ \text{or} & \|\mathbf{w} - \mathbf{L}_{\mathbf{w}}(\mu)\|_\infty = \|\mathbf{w}' - \mathbf{L}_{\mathbf{w}'}(\mu)\|_\infty \quad \text{and} \quad \mathbf{w} <_{\text{lex}} \mathbf{w}', \end{array}$$

where $<_{\text{lex}}$ stands for lexicographic comparison.

Let μ be a minimum of $\mathcal{O}$. Define for any $\mathbf{v} = (v_1, \ldots, v_r)$ with

$$v_i - \delta < \log|\mu|_i \le v_i, \quad \text{for all } 1 \le i \le r \tag{$*$}$$

the set $\mathcal{N}(\mathbf{v}) = \{\, \mathbf{w} \in \mathbb{Z}_N^r \mid v_i - \delta - 1/N < w_i < v_i + 2/N \,\}$.

Lemma 3. *For any two* $\mathbf{v}, \mathbf{v}'$ *satisfying* $(*)$*, the points closest to* μ *in* $\mathcal{N}(\mathbf{v})$ *and* $\mathcal{N}(\mathbf{v}')$ *coincide.*

Proof. There exists a point $\mathbf{w}_0 = (w_1, \ldots, w_r) \in \mathbb{Z}_N^r$ such that $0 \le w_i - \log|\mu|_i < 1/N$ for all $1 \le i \le r$. Since $\mathbf{w}_0$ necessarily lies in both $\mathcal{N}(\mathbf{v})$ and in $\mathcal{N}(\mathbf{v}')$ and $\|\mathbf{w} - \mathbf{L}_{\mathbf{w}}(\mu)\|_\infty < 1/N + \delta$, we know that the closest point to μ in both these sets is contained in

$$\mathcal{N} = \{\, \mathbf{w} \in \mathbb{Z}_N^r \mid \|\mathbf{w} - \mathbf{L}_{\mathbf{w}}(\mu)\|_\infty < 1/N + \delta \,\}$$

Since $\mathcal{N} \subset \mathcal{N}(\mathbf{v}) \cap \mathcal{N}(\mathbf{v}')$, the claim of the lemma follows. □

Given any BMR $\boldsymbol{\beta}$ of a minimum μ of $\mathcal{O}$ we can compute in polynomial time the point $\mathbf{v}$ which is closest to μ in $\mathcal{N}(\mathbf{L}(\boldsymbol{\beta}))$, and Lemma 3 assures us that the result will be independent of the BMR initially given. Thus we may take the BMR $\boldsymbol{\beta}(\mathbf{v})$ of μ in $\mathcal{M}(\mathbf{v})$ to be the *distinguished BMR* of μ, and define $\mathbf{L}(\mu) = \mathbf{L}_{\mathbf{v}}(\mu)$.

5 The periodic function

In this section we will define a function on $\mathbb{Z}^r$ which is loosely periodic with period lattice $N\varLambda$ in the sense of Definition 1 where $\varLambda = \mathbf{Log}\, U$, and N in $O((\log\varDelta)^r)$ is chosen to satisfy the assumption of Lemma 5.

For any $\mathbf{v} \in \mathbb{Z}_N^r$ we say that $\mu = \mu(\mathbf{v}) \in M_{\mathcal{O}}$ is the minimum closest to $\mathbf{v}$ if for any $\mu' \in \mathcal{M}(\mathbf{v})$ we have

$$\begin{array}{ll} \text{either} & \|\mathbf{v} - \mathbf{L}(\mu)\|_2 < \|\mathbf{v} - \mathbf{L}(\mu')\|_2, \\ \text{or} & \|\mathbf{v} - \mathbf{L}(\mu)\|_2 = \|\mathbf{v} - \mathbf{L}(\mu')\|_2, \quad \text{and} \quad \mathbf{L}(\mu) <_{\text{lex}} \mathbf{L}(\mu'). \end{array}$$

We then define the function

$$f : \mathbb{Z}^r \longrightarrow \mathcal{R}_{\mathcal{O}} \times \mathbb{Z}_N^r : \mathbf{v} \longmapsto ((1/\mu), \lceil \mathbf{v}/N - \mathbf{L}(\mu) \rceil_N),$$

where μ is the minimum closest to $\mathbf{v}/N$, and the ceiling is taken componentwise up to integral multiples of $1/N$.

Proposition 3. *The function f is loosely periodic with period lattice $N\mathit{\Lambda}$ where $\mathit{\Lambda} = \mathbf{Log}\, U$. It can be evaluated in polynomial time.*

The polynomial run-time bound is clear from the preceding two sections. Loose periodicity follows from the following two lemmata. Proposition 3 together with Theorem 2 implies Theorem 1.

Lemma 4. *Let $\mathbf{v} \in \mathbb{Z}^r$. Assume that there exists $\mu \in M_{\mathcal{O}}$ such that for any $\mu' \in M_{\mathcal{O}}$ we have*

$$\|\mathbf{v}/N - \mathbf{L}(\mu)\|_2 + 6\sqrt{r}/N < \|\mathbf{v}/N - \mathbf{L}(\mu')\|_2. \tag{3}$$

Then there exists for any $\lambda \in N\mathit{\Lambda}$ a unique $\mathbf{w} \in \mathbb{R}^r$ such that

1. $\|\mathbf{w}\|_\infty < 2$*,*
2. $\mathbf{v} + \lambda + \mathbf{w} \in \mathbb{Z}^r$*,*
3. $f(\mathbf{v}) = f(\mathbf{v} + \lambda + \mathbf{w})$*.*

Proof (of Lemma 4). We sketch a proof of Lemma 4.

Let $\mathbf{v} \in \mathbb{Z}^r$ be such that the assumptions of the lemma hold. Let $\lambda = N\mathbf{Log}\,\varepsilon$ for some unit ε. Let further $\mathbf{w} \in \mathbb{R}^r$ be such that $\|\mathbf{w}\|_\infty < 2$, and $\mathbf{v} + \lambda + \mathbf{w} \in \mathbb{Z}^r$. Then (3) implies that $\varepsilon\mu$ is the minimum closest to $(\mathbf{v} + \lambda + \mathbf{w})/N$.

Write $\mathbf{L} = (l_1, \ldots, l_r)$. Due to (2) we have for all $1 \le i \le r$

$$\left|\log|\varepsilon|_i - (l_i(\varepsilon\mu) - l_i(\mu))\right| < 2\delta < 1/N.$$

Hence we have also

$$\left|\lceil (v_i + \lambda_i)/N - l_i(\varepsilon\mu)\rceil_N - \lceil v_i/N - l_i(\mu)\rceil_N\right| \le 2/N,$$

and there is a unique $w_i \in \mathbb{R}$ with $|w_i| < 2$ such that $v_i + \lambda_i + w_i \in \mathbb{Z}$ and

$$\lceil (v_i + \lambda_i + w_i)/N - l_i(\varepsilon\mu)\rceil_N = \lceil v_i/N - l_i(\mu)\rceil_N\,. \qquad \square$$

For any $\mathbf{v} \in \mathbb{Z}^r$ let $\mathcal{Q}(v) = \{\, \mathbf{w} \in \mathbb{Z}^r \mid 0 \le w_i - v_i < (N/8)\log\mathit{\Delta}\,\}$. Let $\mathcal{Q}^+(\mathbf{v})$ denote the set of all $\mathbf{w} \in \mathcal{Q}(\mathbf{v})$ for which there exists a $\mu \in M_{\mathcal{O}}$ such that for any $\mu' \in M_{\mathcal{O}}$ the inequality (3) holds.

Lemma 5. *For $\mathit{\Delta} \gg 0$ and $N \gg (\log\mathit{\Delta})^r$, we have $\frac{\operatorname{card}\mathcal{Q}^+(\mathbf{v})}{\operatorname{card}\mathcal{Q}(\mathbf{v})} > \frac{1}{2}$*

Proof. We sketch a proof of Lemma 5.

Let $\mathbf{w} \in \mathcal{Q}(\mathbf{v}) \setminus \mathcal{Q}^+(\mathbf{v})$. Choose two minima μ, μ' with minimal distance to $\mathbf{w}$ in the Euclidean norm for which (3) is violated. Then $\mathbf{w}$ lies between two hyperplanes perpendicular to $\mathbf{L}(\mu) - \mathbf{L}(\mu')$ with distance smaller than $6\sqrt{r}/N$.

The set of all points in $\mathcal{Q}(\mathbf{v})$ lying between these two hyperplanes is contained in a body with volume $O((\log \varDelta)^{r-1}/N)$ determined by the minima μ and μ'. Call this body $\mathcal{T}(\mu, \mu')$.

The minima μ and μ' are contained in a box of side length $\log \varDelta/4$. By a result due to Buchmann, and proved in detail in [Thi95], there are no more than $O((\log \varDelta)^r)$ minima in such a box.

By summing the volumina of $\mathcal{T}(\mu, \mu')$ with μ and μ' running through all possibly occurring pairs of minima, and comparing this sum to the volume of $\mathcal{Q}(\mathbf{v})$ we obtain a constant upper bound for the fraction $\frac{\operatorname{card}(\mathcal{Q}(\mathbf{v}) \smallsetminus \mathcal{Q}^+(\mathbf{v}))}{\operatorname{card} \mathcal{Q}(\mathbf{v})}$ provided $\varDelta \gg 0$ and $N \gg (\log \varDelta)^r$. □

6 Conclusion

In this paper, we have shown how to compute the period lattice of loosely periodic functions, and applied the technique to the computation of the unit group of a finite extension K of $\mathbb{Q}$. The resulting algorithm is of Monte-Carlo type: it succeeds and prints a correct result with pre-determined probability. Its success probability can be arbitrarily increased by repeating the algorithm. A correct lattice can be singled-out from a string of outputs since it has the smallest occurring determinant.

It is easy to extend the algorithm so that it computes a generator to a given ideal of an order in K. Here it is possible to check the result with a classical algorithm in polynomial time. (We will, however, not be assured to obtain a generator with the shortest possible logarithm vector.) Thus the algorithm can be applied to attack crypto-systems that rely on the difficulty of the principal ideal problem yielding a better idea about which parameter sizes for these crypto-systems remain secure in the presence of quantum computers.

In order to obtain a Las Vegas algorithm that never prints an in-correct result, but might fail, we need to compute the class number, or, better, the relations between a polynomial size set of generators of the class group. Any result in this direction is likely to depend on the validity of a Generalized Riemann Hypothesis. This is work in progress.

Finally, we have not attempted to minimize the influence of the dimension of the lattice (i.e., the unit rank of the order) on the run-time which is at the current state of affairs unavoidably exponential.

In the more abstract setting, it seems likely that the still rather stringent properties required from loosely periodic functions can be further relaxed. Larger disturbances can be permitted at the cost of a longer run-time. Local injectivity can almost certainly be weakened considerably or entirely dropped.

Moreover, it would be interesting to see a version of our algorithm using the Eigenvalue Estimation which would be very likely to require many fewer qubits.

References

Ban93. W. Banaszczyk. New bounds in some transference theorems in the geometry of numbers. *Mathematische Annalen*, 296(4):625–635, 1993.

BJP94. Johannes Buchmann, Max Jüntgen, and Michael Pohst. A practical version of the generalized lagrange algorithm. *Exp. Math.*, (3):200–207, 1994.

BL95. D. Boneh and R. Lipton. Quantum cryptanalysis of hidden linear functions (extended abstract). In Don Coppersmith, editor, *Advances in Cryptology - CRYPTO '95*, volume 963 of *Lecture Notes in Computer Science*. Springer, 1995.

BMM00. Johannes Buchmann, Markus Maurer, and Bodo Möller. Cryptography based on number fields with large regulator. Technical Report TI-5/00, Technische Universität Darmstadt, Fachbereich Informatik, 2000. `http://www.informatik.tu-darmstadt.de/TI/Veroeffentlichung/TR/`.

Buc87a. J. Buchmann. On the computation of units and class numbers by a generalization of Lagrange's algorithm. *Journal of Number Theory*, 26:8–30, 1987.

Buc87b. Johannes Buchmann. Zur Komplexität der Berechnung von Einheiten und Klassenzahlen algebraischer Zahlkörper, 1987. Habilitationsschrift.

Buc90. Johannes Buchmann. A subexponential algorithm for the determination of class groups and regulators of algebraic number fields. In Catherine Goldstein, editor, *Séminaire de Théorie des Nombres, Paris 1988–1989*, volume 91 of *Progress in Mathematics*, pages 27–41. Birkhäuser, 1990.

Des02. Simon-Pierre Desrosier. De la cryptographie sur les corps quadratiques rels. Master's thesis, Université McGill, Montréal, 2002.

Hal02. Sean Hallgren. Polynomial-time quantum algorithms for pell's equation and the principal ideal problem. In *Proceedings of the thiry-fourth annual ACM symposium on the theory of computing*, pages 653–658. ACM Press, 2002.

HH00. Lisa Hales and Sean Hallgren. An improved quantum fourier transform algorithm and applications. In *IEEE Symposium on Foundations of Computer Science*, pages 515–525, 2000.

HV00. Boris Hemkemeier and Frank Vallentin. Incremental construction algorithms for lattices generated by many lattice points. http://www.matha.mathematik.uni-dortmund.de/~fv/odsa/odsa_bhfv_paper.pdf, 2000.

Joz98. Richard Jozsa. Quantum algorithms and the fourier transform. *Proc Roy Soc Lond A*, pages 323–337, 1998.

Kit96. Alexei Kitaev. Quantum measurements and the abelian stabilizer problem. *Electronic Colloquium on Computational Complexity (ECCC)*, 3(3), 1996.

ME99. Michele Mosca and Artur Ekert. The hidden subgroup problem and eigenvalue estimation on a quantum computer. *Lecture Notes in Computer Science*, 1509:174–188, 1999.

Sho97. Peter W. Shor. Polynomial time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

Sim94. David R. Simon. On the power of quantum computation. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pages 116–123, Los Alamitos, CA, 1994. Institute of Electrical and Electronic Engineers Computer Society Press.

Thi95. Christoph Thiel. *On the complexity of some problems in algorithmic algebraic number theory.* PhD thesis, Universität des Saarlandes, Saarbrücken, Germany, 1995.