Chapter 4

(More) Quantum Algorithms Based on the Fourier Transform

The goal of this chapter will be to explain and analyze Shor's quantum algorithms for factoring large integers and for computing discrete logarithms. These algorithms run in polynomial time (in the description length of the problem), in contrast to the best-known classical algorithms (like the number-field sieve), which run in superpolynomial time.[1] These quantum algorithms are particularly exciting — or troubling, depending on the point of view — given that the security of (almost) all of currently used public-key cryptography relies on the assumed hardness of these two computational problems. This means that a scalable quantum computer that is capable of running Shor's algorithms would render today's internet completely insecure.

We start the chapter by introducing the Fourier transform, which is at the core of Shor's algorithms, and we then first discuss some algorithms that avoid some of the technical difficulties but still reflect the basic idea behind Shor's algorithms. As a matter of fact, at the heart of the chapter will be a meta quantum algorithm for solving the so-called *hidden subgroup problem* for Abelian groups; almost all quantum algorithms we treat in these notes can be understood as an instantiation of the meta algorithm up to some modifications.

4.1 The Classical and the Quantum Fourier Transform

Fix an integer $N \geq 2$ and consider the ring $\mathbb{Z}/N\mathbb{Z}$. By default, the elements are represented by integers in $\{0, \ldots, N-1\}$, and so we will typically not distinguish between an integer and its coset modulo N. We let $\omega_N := e^{2\pi i/N} \in \mathcal{S}(\mathbb{C}) \subset \mathbb{C}$ and write ω when N is clear.[2] Recall that, by Euler's identity, the function $\mathbb{Z} \to \mathbb{C}$, $j \mapsto \omega_N^j = e^{2\pi i j/N}$ is a group homomorphism with kernel $N\mathbb{Z}$, and so we may also understand it as a function $\mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$. By allowing j to be real valued, we can also consider it as a function $\mathbb{R} \to \mathbb{C}$, or $\mathbb{R}/N\mathbb{Z} \to \mathbb{C}$.

Definition 4.1. *For any function $\alpha : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ the (discrete)* **Fourier transform** *of α is the function $\hat{\alpha} : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ given by*

$$\hat{\alpha}(k) = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \omega_N^{jk} \alpha(j)$$

[1] In case of computing discrete logarithms, the running time of classical algorithms depends on the group considered and ranges from polynomial time (for "easy" groups) to exponential time (e.g. for elliptic curves).

[2] As is common, we use e^z as a shorthand for $\exp(z)$. This is consistent with the basic property of the exponential function that $\exp(z+w) = \exp(z)\exp(w)$, and, thus, $\exp(n \cdot z) = \exp(z)^n$ for any integer n.

for any $k \in \mathbb{Z}/N\mathbb{Z}$.[3]

We may also write α_j instead of $\alpha(j)$ and $\hat{\alpha}_k$ instead of $\hat{\alpha}(k)$.

We quickly look at a simple yet important example. The Fourier transform of the all-1 function $1_N : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$, $j \mapsto 1$ is given by

$$\hat{1}_N(k) = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \omega_N^{jk} = \begin{cases} \sqrt{N} & \text{if } k = 0 \\ 0 & \text{else} \end{cases}$$

for $k \in \mathbb{Z}/N\mathbb{Z}$, sometimes referred to as **Dirac function**.

We point out, and this will become important later on, that the definition of $\hat{\alpha} : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ above extends to $\hat{\alpha} : \mathbb{R}/N\mathbb{Z} \to \mathbb{C}$, simply by allowing k in Definition 4.1 to be in the ring $\mathbb{R}/N\mathbb{Z}$, with the understanding that $\omega_N^{jk} = e^{2\pi ijk/N}$. In particular, we will consider $\hat{1}_N(k)$ as above but for real-valued k. The function $\hat{1}_N(k)$ will then not necessarily vanish for non-zero k (see Figure 4.1); what will be important for us that that in the neighbourhood of 0, it is still relatively large, as captured by the following.

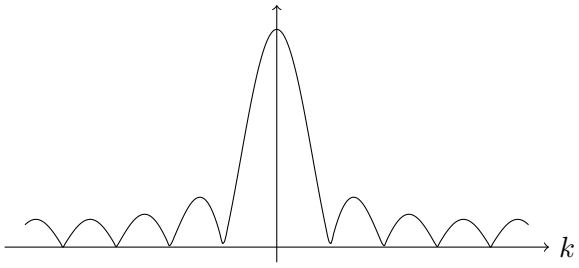


Figure 4.1: The absolute value of $\hat{1}_N$ as a function $\mathbb{R}/N\mathbb{Z} \to \mathbb{C}$.

Lemma 4.1. *As function* $\hat{1}_N : \mathbb{R}/N\mathbb{Z} \to \mathbb{C}$*, and for* $\xi \in \mathbb{R}$ *with* $|\xi| \leq 1/2$*,*

$$\left|\hat{1}_N(\xi)\right| \geq \frac{2\sqrt{N}}{\pi} = \frac{2}{\pi} \cdot \hat{1}_N(0)\,.$$

Proof. We observe that

$$\hat{1}_N(\xi) = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \omega^{j\xi} = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \left(\omega^{\xi}\right)^j = \frac{1}{\sqrt{N}} \frac{1-\omega^{\xi N}}{1-\omega^{\xi}} = \frac{1}{\sqrt{N}} \frac{1-e^{2\pi i\xi}}{1-e^{2\pi i\xi/N}}\,.$$

where the last equality is the well-known closed form of a geometric series, assuming that $\xi \neq 0$. From the goemetric picture, by comparing chord and arc, it is easy to convince yourself that $2\pi\nu \geq |1 - e^{2\pi i\nu}| \geq 4\nu$ for $\nu \in [-1/2, 1/2]$, so that

$$\left|\hat{1}_N(\xi)\right| \geq \frac{1}{\sqrt{N}} \frac{4\xi}{2\pi\xi/N} = \frac{2\sqrt{N}}{\pi}\,,$$

as claimed. □

We now introduce the *quantum* Fourier transform. Given the integer $N \geq 2$, we consider an arbitrary N-dimensional Hilbert space $\mathcal{H}_N$ with an orthonormal basis $\{|0\rangle, \ldots, |N-1\rangle\}$, where the basis vectors are labelled by the integers in $\{0, \ldots, N-1\}$, which we identify with the elements in $\mathbb{Z}/N\mathbb{Z}$. The quantum Fourier transform is simply the classical Fourier transform applied to the amplitudes.

[3]The deviation from the typical definition, which uses the conjugate coefficients $e^{-2\pi ijk/N}$, is an artefact of having inner products conjugate-linear in the *first* argument, rather than in the second.

Definition 4.2. *The* **quantum Fourier transform** *on $\mathcal{H}_N$ (w.r.t. $\{|j\rangle\}_{j\in\{0,\dots,N-1\}}$) is the unitary operator $F \in \mathcal{U}(\mathcal{H}_N)$ given by*

$$F : \sum_{j=0}^{N-1} \alpha_j |j\rangle \mapsto \sum_{k=0}^{N-1} \hat{\alpha}_k |k\rangle \,.$$

In other words,

$$F : |j\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega_N^{jk} |k\rangle$$

for any $j \in \{0, \dots, N-1\}$.

As for F being unitary, we observe that for any pair $|m\rangle$ and $|k\rangle$ of basis vectors,

$$\langle m|F^\dagger F|k\rangle = \frac{1}{N} \sum_{j,\ell} \omega^{jk-\ell m} \langle \ell | j \rangle = \frac{1}{N} \sum_{j} \omega^{j(k-m)} = \frac{1}{\sqrt{N}} \hat{1}_N(k-m) = \langle m|k\rangle \,.$$

We point out that mathematically, the quantum Fourier transform is identical to the ordinary Fourier transform, except that it is made explicit that the functions $\alpha : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ form a Hilbert space, and Dirac's bra-ket notation is used. Furthermore, when it comes to *computing* the quantum Fourier transform, a different model of computation is used.

4.2 Period Finding in $\mathbb{Z}/N\mathbb{Z}$

As a first application, we show here that the quantum Fourier transform gives rise to a variant of Simon's algorithm. Consider a black-box function $f : \mathbb{Z}/N\mathbb{Z} \to \mathcal{R}$ with an arbitrary finite domain $\mathcal{R}$, with the promise that there exists a non-zero divisor s of N such that $f(x) = f(x')$ if and only if s divides $x - x'$. The goal is to find s. Looking ahead, Shor's factoring algorithm will also work by finding the period of some function; however, there and in contrast to here, no multiple of the period will be given.

We show that, very much in spirit of Simon's algorithm, the following quantum circuit will allow us to obtain useful information on s. Note that the state $|0\rangle$ of the first register is given by the first basis vector of the fixed basis for $\mathcal{H}_N$. On the other hand, the state of the second register, which is also denoted $|0\rangle$, is a quantum encoding of the neutral element of $\mathcal{R}$ when considered as a group, as done for defining U_f.

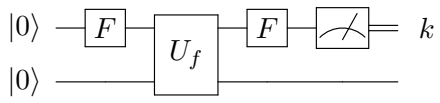


Figure 4.2: Quantum circuit for period-finding on $\mathbb{Z}/N\mathbb{Z}$.

Proposition 4.2. *Given that f is as promised, the quantum circuit in Figure 4.2 produces a uniformly random $k \in \mathbb{Z}/N\mathbb{Z}$ subject to $k \cdot s = 0$ (in $\mathbb{Z}/N\mathbb{Z}$).*

Note that $ks = 0$ in $\mathbb{Z}/N\mathbb{Z}$ means that $ks = cN$ over the integers, for a random integer $c \in \{0, \dots, s-1\}$. In order to obtain s, we can then bring the fraction k/N, which equals c/s, into reduced form and read out the denominator; this results in $s' = s/\gcd(c, s)$. Thus, if c happens to be coprime, we have $s' = s$, and we can easily check whether $s' = s$. Furthermore, by running the procedure twice, we obtain s by taking the least common multiple of the two

corresponding s''s *if* the two corresponding c's are coprime. The latter can be shown to happen with probability at least[4] $2-\pi^2/6 \approx 0.35$ and approaches $1/\zeta(2) = 6/\pi^2 \approx 0.6$ for large s. Thus, the correct s can be obtained with overhelming probability by repeating the above procedure a few times.

Proof. Applying F to the first register, and then appling U_f, results in

$$|0\rangle|0\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|0\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|f(x)\rangle \,.$$

For the purpose of the analysis, let as assume that the second register is now measured. The measurement outcome is a element $y \in \mathcal{R}$, and the state of the first register collapses to a superposition of all $x \in \mathbb{Z}/N\mathbb{Z}$ with $f(x) = y$. By assumption on f, this means that the state of the first register becomes

$$\frac{1}{\sqrt{m}} \sum_{\ell=0}^{m-1} |\ell s + x\rangle \,,$$

where x is some $x \in \mathbb{Z}/N\mathbb{Z}$ with $f(x) = y$, and $m := N/s$. Applying F then results in

$$\begin{aligned}
\frac{1}{\sqrt{Nm}} \sum_{\ell=0}^{m-1} \sum_{k=0}^{N-1} \omega_N^{(\ell s+x)k} |k\rangle &= \frac{1}{\sqrt{Nm}} \sum_{k=0}^{N-1} \sum_{\ell=0}^{m-1} \omega_N^{\ell sk} \omega_N^{xk} |k\rangle \\
&= \frac{1}{\sqrt{Nm}} \sum_{k=0}^{N-1} \Bigg(\sum_{\ell=0}^{m-1} \omega_m^{\ell k} \Bigg) \omega_N^{xk} |k\rangle \\
&= \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \hat{1}_m(k)\, \omega_N^{xk} |k\rangle \,.
\end{aligned}$$

where we used that $\omega_N^s = e^{2\pi i s/N} = e^{2\pi i/m} = \omega_m$. From this, given that $\hat{1}_m(k)$ does not vanish if and only if k is an integer multiple of $m = N/s$, we see that measuring this register results in a uniformly random $k \in \mathbb{Z}/N\mathbb{Z}$ subject to $k \cdot s = 0$. □

4.3 Period Finding in $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$

We consider a small variation of the period finding problem from Section 4.2 above, where now $f : \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \to \mathcal{R}$, and it is promised that there exists a non-zero $s \in \mathbb{Z}/N\mathbb{Z}$ such that $f(x, y) = f(x', y')$ if and only if $x - x' = s(y - y')$, i.e., $(s, 1)$ divides $(x, y) - (x', y')$. We remark that restricting the second component of the period to be 1, or, equivalently, to be co-prime with N, is merely for simplicity. Looking ahead, we point out that applied to the function $(x, y) \mapsto g^x h^y$ for two group elements g, h, finding s is equivalent to computing the discrete logarithm of h with respect to g.

Proposition 4.3. *Assuming that $f : \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \to \mathcal{R}$ is such that there exists a non-zero $s \in \mathbb{Z}/N\mathbb{Z}$ such that $f(x, y) = f(x', y')$ if and only if $x - x' = s(y - y')$, the quantum circuit in Figure 4.3 produces uniformly random $k, m \in \mathbb{Z}/N\mathbb{Z}$ subject to $sk + m = 0$ (in $\mathbb{Z}/N\mathbb{Z}$).*

Similarly to before, if we are unlucky and k and N are not coprime then the procedure needs to be repeated, and with high probability s will be recovered after a few repetitions.

[4]Indeed, the probability of the two c's to share a common factor is at most $\sum_{n \geq 2} 1/n^2 = \zeta(2) - 1 = \pi^2/6 - 1$.

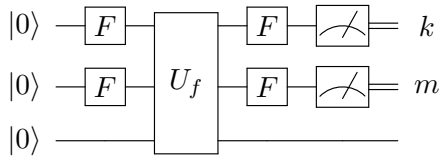


Figure 4.3: Quantum circuit for period-finding on $\mathbb{Z}/N\mathbb{Z}$.

Proof. Applying F to the first two registers, and then appling U_f, results in

$$|0\rangle|0\rangle|0\rangle \mapsto \frac{1}{N}\sum_{x,y=0}^{N-1}|x\rangle|y\rangle|0\rangle \mapsto \frac{1}{N}\sum_{x,y=0}^{N-1}|x\rangle|y\rangle|f(x,y)\rangle\,.$$

Again, let us assume that the last register is now measured. The measurement outcome is a element $z \in \mathcal{R}$, and the state of the first two registers collapses to a superposition of all x and y in $\mathbb{Z}/N\mathbb{Z}$ with $f(x,y) = z$. By the assumption on f, this means that the state of the first two registers becomes

$$\frac{1}{\sqrt{N}}\sum_{\ell=0}^{N-1}|\ell s + x\rangle|\ell + y\rangle\,,$$

where x and y are so that with $f(x,y) = z$. Applying F individually to both registers then results in

$$\begin{aligned}\frac{1}{N^{3/2}}\sum_{\ell,k,m}\omega^{(\ell s+x)k}\omega^{(\ell+y)m}|k\rangle|m\rangle &= \frac{1}{N^{3/2}}\sum_{\ell,k,m}\omega^{\ell(sk+m)}\omega^{xk}\omega^{ym}|k\rangle|m\rangle \\ &= \frac{1}{N}\sum_{k,m}\hat{1}_N(sk+m)\,\omega^{xk}\omega^{ym}|k\rangle|m\rangle\,.\end{aligned}$$

From this we see that measuring these two registers results in uniformly random $k, m \in \mathbb{Z}/N\mathbb{Z}$ subject to $sk + m = 0$, as claimed. □

4.4 The Hidden Subgroup Problem

The reader should start to see a pattern. Indeed, the computational problems solved by Deutsch's algorithm, by Bernstein-Vazirani's algorithm, and by Simon's algorithm, as well as the two period finding problems above, are all instances of the **hidden subgroup problem (HSP)**. In its most generality, the HSP reads as follows. Given a group G and a black-box function $f : G \to \mathcal{R}$ with the promise that $f(x) = f(x')$ if and only if $x^{-1}x' \in H$, where H is an unknown subgroup of G, the goal is to find (a representation of) the "hidden subgroup" H. In other words, f acts identically within each coset xH, but differently on different cosets.

For Deutsch's problem, we have $G = \mathbb{Z}/2\mathbb{Z}$ and H is either $\mathbb{Z}/2\mathbb{Z}$ or $\{0\}$. For Bernstein-Vazirani's problem and for Simon's problem, we have $G = \mathbb{F}_2^n = \mathbb{F}_2 \times \cdots \times \mathbb{F}_2$, understood as vector space over the binary field $\mathbb{F}_2$ (with standard inner product), and H is the orthogonal complement of $a \in G$ for the former, and the linear span of (non-zero) $s \in G$. For period finding in $\mathbb{Z}/N\mathbb{Z}$, we have $G = \mathbb{Z}/N\mathbb{Z}$ and H is generated by (non-zero) $s \in G$. And, eventually, for period finding in $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$, we have $G = \mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$ and H generated by $(s, 1) \in G$.

Not so suprising, the techniques for solving the above specific problems by means of quantum algorithms unify and generalize. We note, however, that Deutsch's algorithm and Bernstein-Vazirani's algorithm are both slighty different than the generic hidden subgroup algorithm

outlined below; indeed, they produce the right answer in one go and with certainty. Similarly, the Deutsch-Jozsa problem does not fit into the HSP framework (unless $n = 1$).

We start with the following definition.

Definition 4.3. *For a finite Abelian group G, the* **dual group** $\hat{G}$ *is the group of homomorphisms χ from G to the multiplicative group $\mathcal{S}(\mathbb{C})$. $\chi \in \hat{G}$ is called a* **character**.

The following captures some basic properties of the dual group.

Proposition 4.4. $|\hat{G}| = |G|$. *Furthermore, the* **orthogonality relations**

$$\sum_x \overline{\chi(x)}\chi'(x) = \begin{cases} 0 & \text{if } \chi \neq \chi' \\ |G| & \text{if } \chi = \chi' \end{cases} \quad \text{and} \quad \sum_\chi \overline{\chi(x)}\chi(x') = \begin{cases} 0 & \text{if } x \neq x' \\ |\hat{G}| & \text{if } x = x' \end{cases}$$

hold for all $x, x' \in G$ and $\chi, \chi' \in \hat{G}$. In particular, for every $1 \neq x \in G$ and $1 \neq \chi \in \hat{G}$,

$$\sum_{x \in G} \chi(x) = 0 \qquad \text{and} \qquad \sum_{\chi \in \hat{G}} \chi(x) = 0\,.$$

Proof. We start by observing that $\hat{G}$ must be finite, given that G is. This follows from the fact that $\chi(g)^{|G|} = \chi(g^{|G|}) = \chi(1) = 1$, and thus $\chi(g)$ must be a $|G|$-th root of unity for any g.

As for the last two claims of the statement, the first one follows from the observation that

$$\sum_x \chi(x) = \sum_x \chi(xy) = \chi(y) \sum_x \chi(x)$$

for any $y \in G$, and the existence of $y \in G$ with $\chi(y) \neq 1$. Similarly for the other one, using that $|\hat{G}| < \infty$, and that for any $x \neq 1$ there exists $\chi \in \hat{G}$ with $\chi(x) \neq 1$ (which follows from Lemma 4.5 below). Since χ maps into $\mathcal{S}(\mathbb{C})$, we have that $\chi^{-1} = \overline{\chi}$, and the two orthogonality relations then follow easily. Also, the orthogonality relations then imply that $|\hat{G}| = |G|$. □

Lemma 4.5. *Let $H \subsetneq G$ be a subgroup of G and $x \in G \setminus H$, and let $\pi \in \hat{H}$ be a character of H. Then there exists a character $\chi \in \hat{G}$ so that $\chi(h) = \pi(h)$ for all $h \in H$, and $\chi(x) \neq 1$.*

Proof. By repeated application, it is enough to show the claim in case G is generated by H and x, i.e., $G = \{x^i h \,|\, h \in H,\, i \in \mathbb{Z}\}$. For that, let $n \geq 2$ is the smallest positive integer for which $x^n \in H$, and let $\omega \neq 1$ be such that $\omega^n = \pi(x^n)$. For any $g = x^i h \in G$, we now define $\chi(g) = \chi(x^i h) := \omega^i \pi(h)$. We first need to show that this is well defined. Let $h, h' \in H$ and $i, j \in \mathbb{Z}$ with $x^i h = x^j h'$. Then $x^{i-j} = h/h' \in H$, and thus $i - j = kn$ for $k \in \mathbb{Z}$. Therefore,

$$\chi(x^i h)/\chi(x^j h') = \omega^{i-j}\chi(h/h') = \omega^{kn}\pi(h/h') = \pi(x^n)^k \pi(h/h') = \pi(x^{kn}h/h') = \pi(1) = 1\,.$$

Finally, it is obvious that χ is a homomorphism, i.e., $\chi \in \hat{G}$, and $\chi(x) = \omega \neq 1$. □

As an immediate consequence, for any pair of fixed orthonormal bases $\{|x\rangle\}_{x \in G}$ and $\{|\chi\rangle\}_{\chi \in \hat{G}}$ of the Hilbert space $\mathbb{C}^{|G|}$, the **generalized quantum Fourier transform** F, given as follows, is unitary:

$$F : |x\rangle \mapsto \frac{1}{\sqrt{|G|}} \sum_{\chi \in \hat{G}} \chi(x)|\chi\rangle\,.$$

In case of $G = \mathbb{Z}/N\mathbb{Z}$, the characters are the homomorphisms that map j to ω_N^{jk} for k in $\{0, \ldots, N-1\}$, and so F coincides with Definition 4.2. In case of $G = \mathbb{Z}/2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/2\mathbb{Z}$, the characters are the functions $x \mapsto (-1)^{x \cdot y}$ for all possible choices of y, and then F matches $H^{\otimes n}$. This allows us to generalize above quantum algorithms and obtain the following general result.

Theorem 4.6. *For any finite Abelian group G with hidden subgroup H, there exists a quantum circuit with black-box access to U_f and query complexity 1 that outputs a random character χ that acts trivially on H.*

In general, in order to uniquely identify H, the algorithm needs to be repeated several times; how (a representation of) H can then be computed depends on the structure of G and H.

Proof. We produce a superposition of all $x \in G$ (e.g., by applying $F^\dagger$ to $|1\rangle$) and an ancilla and apply U_f to get

$$\frac{1}{\sqrt{|G|}} \sum_{x \in G} |x\rangle|0\rangle \mapsto \frac{1}{\sqrt{|G|}} \sum_{x \in G} |x\rangle|f(x)\rangle \,.$$

Measuring the second register to observe $y = f(x)$ has the effect that the state collapses to

$$\frac{1}{\sqrt{|H|}} \sum_{h \in H} |xh\rangle \,.$$

Applying the generalized quantum Fourier transform F then results in

$$\frac{1}{\sqrt{|G||H|}} \sum_{h \in H} \sum_{\chi \in \hat{G}} \chi(xh)|\chi\rangle = \frac{1}{\sqrt{|G||H|}} \sum_{\chi \in \hat{G}} \chi(x) \sum_{h \in H} \chi(h)\,|\chi\rangle$$

and so, given that the restriction of χ to H is a character in $\hat{H}$, and thus Proposition 4.4 applies correspondingly, we see that $|\chi\rangle$ has a non-trivial amplitude only if χ acts trivially on H. □

Later, we show that the technique even generalizes to *infinite* Abelian groups to some extent. This will then eventually lead to Shor's famous factoring algorithm.

4.5 Computing the Quantum Fourier Transform

We have seen that the quantum Fourier transform is very powerful and gives rise to various quantum algorithms with low *query* complexity. In order to obtain quantum algorithms with low *computational* complexity, we need to be able to efficiently compute the quantum Fourier transform. We show here how this is done.

Note that in order to fit into our model of computation, we need F to act on qubits. As such, we set $N = 2^n$ for a positive integer n, and we let $\mathcal{H}_N$ be $\mathcal{H}_N = \mathcal{H}^{\otimes n} = \mathcal{H} \otimes \cdots \otimes \mathcal{H}$. Finally, we require the basis $\{|0\rangle, \ldots, |N-1\rangle\}$ to be given by $|j\rangle = |j_1\rangle \cdots |j_n\rangle$, where $(j_1, \ldots, j_n) \in \{0,1\}^n$ is the **binary representation** of $j \in \{0, \ldots, N-1\}$, uniquely determined by the equality

$$j = [j_1 \cdots j_n] := \sum_{\ell=1}^{n} j_\ell \, 2^{n-\ell} \,.$$

By a variation of this formalism, we also write

$$[0.j_1 \cdots j_n] := j/2^n = \sum_{\ell=1}^{n} j_\ell \, 2^{-\ell}$$

The following observation is at the core of the efficient computability of the quantum Fourier transform F, which we will denote by F_n below, in order to make the dependency on the parameter n explicit.

Lemma 4.7. *For any positive integer n and any $j = [j_1 \cdots j_n] \in \{0, \ldots, 2^n - 1\}$:*

$$F_n|j\rangle = F_n|j_1\rangle \cdots |j_n\rangle = \frac{1}{\sqrt{2^n}} \bigotimes_{\ell=1}^{n} \Big(|0\rangle + \omega_{2^\ell}^{j}|1\rangle\Big),$$

or, in other words,

$$= \frac{1}{\sqrt{2^n}} \Big(|0\rangle + e^{2\pi i[0.j_n]}|1\rangle\Big) \Big(|0\rangle + e^{2\pi i[0.j_{n-1}j_n]}|1\rangle\Big) \cdots \Big(|0\rangle + e^{2\pi i[0.j_1 \cdots j_{n-1}j_n]}|1\rangle\Big).$$

Proof. By basic term manipulations, we see that

$$\begin{aligned}
F_n|j\rangle &= \frac{1}{\sqrt{2^n}} \sum_k e^{2\pi i jk/2^n} |k_1\rangle \cdots |k_n\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{k_1 \ldots k_n} \prod_\ell e^{\pi i j k_\ell / 2^{n-\ell}} |k_1\rangle \cdots |k_n\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{k_1 \ldots k_n} \bigotimes_\ell e^{2\pi i j k_\ell / 2^\ell} |k_\ell\rangle \\
&= \frac{1}{\sqrt{2^n}} \bigotimes_\ell \sum_{k_\ell} e^{2\pi i j k_\ell / 2^\ell} |k_\ell\rangle \\
&= \frac{1}{\sqrt{2^n}} \bigotimes_\ell \Big(|0\rangle + e^{2\pi i j / 2^\ell}|1\rangle\Big).
\end{aligned}$$

This shows the claim. The second variant follows from the fact that $x \mapsto e^{2\pi i x}$ is cyclic with period 1, and noting that $j/2^\ell \bmod 1 = [0.j_{n-\ell+1} \cdots j_n]$. □

Recalling the definition of the phase shift gate, the above shows that the first qubit of $F_n|j_1\rangle \cdots |j_n\rangle$ equals $S_{2\pi[0.j_n]}|+\rangle$, and the remaining qubits are given by

$$S_{2\pi[0.0j_n]}\Big(|0\rangle + e^{2\pi i[0.j_{n-1}]}|1\rangle\Big) \otimes \cdots \otimes S_{2\pi[0.0\cdots 0j_n]}\Big(|0\rangle + e^{2\pi i[0.j_1 \cdots j_{n-1}]}|1\rangle\Big).$$

This proves the following.

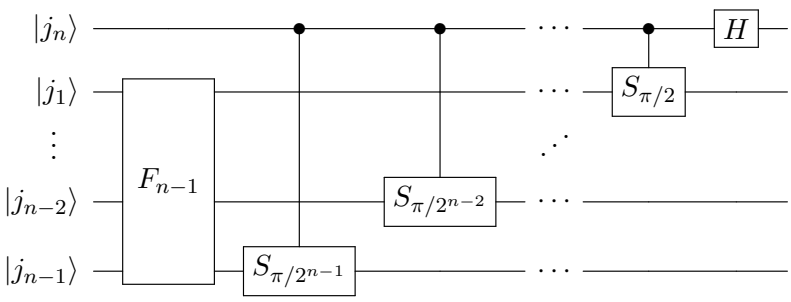
Corollary 4.8. *For any integer $n > 1$ and any $j_1, \ldots, j_n \in \{0, 1\}$:*

$$F_n|j_1\rangle \cdots |j_n\rangle = \big(S_{\pi j_n} \otimes S_{\pi j_n/2} \otimes \cdots \otimes S_{\pi j_n/2^{n-1}}\big)\big(|+\rangle \otimes F_{n-1}|j_1\rangle \cdots |j_{n-1}\rangle\big).$$

Thus, F_n can be recursively computed. In particular, the following holds.

Theorem 4.9. *The n-qubit quantum Fourier transform F_n can be computed with computational complexity $O(n^2)$ with a quantum circuit with gate set consisting of H, swap gates, and controlled phase shift gates. The same holds for the inverse $F_n^\dagger$.*

Proof. Given the above corollary, it follows by trivial inspection that, up to the order of the wires, F_n can be recursively computed by means of the following quantum circuit.



This proves the claim on F_n. For the inverse, we observe that we can invert the circuit for F_n by running the circuit "backwards" and that the considered gate set is preserved under inversion. □

4.6 Shor's Algorithm for Period Finding in $\mathbb{Z}$

Here, we consider a black-box function $f : \mathbb{Z} \to \mathcal{R}$ with an arbitrary finite domain $\mathcal{R}$, with the promise that there exists $s \in \mathbb{Z}$ in the range $1 < s \leq N = 2^n$ such that $f(x) = f(x')$ if and only if $x - x'$ is an integer multiple of s. The goal is to find s.

The crucial difference to Section 4.2 is that, here, s does not divide N, and therefore f does not naturally induce a function $\mathbb{Z}/N\mathbb{Z} \to \mathcal{R}$. Therefore, if we apply the Fourier transform to $f : \{0, \ldots, N-1\} \to \mathcal{R}$, the wrap-around we get by taking numbers modulo N messes up things. Fortunately, we will be able to control how much things are messed up. As a starting point, let us simply take the circuit from Figure 4.2 in order to try to solve the above variation of the period-finding problem, and we follow the analysis from Section 4.2 as far as we can.

Applying F to the first register, which is now an n-qubit register, applying U_f, and then measuring the second register produces a state of the form

$$\frac{1}{\sqrt{m}} \sum_{\ell=0}^{m-1} |\ell s + x\rangle \,,$$

where x is some $x \in \{0, \ldots, s-1\}$ with $f(x) = y$, and m is either $\lfloor N/s \rfloor$ or $\lfloor N/s \rfloor + 1$. Applying F then results in

$$\begin{aligned}
\frac{1}{\sqrt{Nm}} \sum_{\ell=0}^{m-1} \sum_{k=0}^{N-1} \omega_N^{(\ell s + x)k} |k\rangle &= \frac{1}{\sqrt{Nm}} \sum_{k=0}^{N-1} \sum_{\ell=0}^{m-1} \omega_N^{\ell s k} \omega_N^{xk} |k\rangle \\
&= \frac{1}{\sqrt{Nm}} \sum_{k=0}^{N-1} \Big(\sum_{\ell=0}^{m-1} \omega_m^{\ell s k m/N} \Big) \omega_N^{xk} |k\rangle \\
&= \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \hat{1}_m\Big(\frac{ks}{N} m\Big)\, \omega_N^{xk} |k\rangle \,.
\end{aligned}$$

where we used that $\omega_N^t = e^{2\pi i t/N} = e^{2\pi i (t/N) m/m} = \omega_m^{tm/N}$, and where we consider $\hat{1}_m$ as a function on $\mathbb{R}/m\mathbb{Z}$. Recall that in Section 4.2, in the proof of Proposition 4.3, the only k's for which $\hat{1}_m$ did not vanish where the multiples of N/s; therefore, we would observe such a k with certainty. Here, in order to obtain information on s, we may hope that we still get sufficient contribution from those k's that are *close* to a multiple of N/s, so that we observe such a k with sufficient probability upon measuring the register. Indeed, for k of the form $k = cN/s + \delta$ with $|\delta| \leq 1/2$, since $\hat{1}_m$ is periodic we can re-write

$$\hat{1}_m\Big(\frac{ks}{N} m\Big) = \hat{1}_m\Big(cm + \frac{\delta s}{N} m\Big) = \hat{1}_m\Big(\frac{\delta s}{N} m\Big) \,.$$

Furthermore, since $|\delta| \leq 1/2$ and $m \approx N/s$, we expect the argument $\xi := \delta s m/N$ to be bounded in absolute value by $|\xi| \lesssim 1/2$, so that Lemma 4.1 applies and ensures that this particular k will be observed with good probability. Even though this intuition can be rigorously worked out, we provide here a slightly different analysis. Below, $\lfloor \cdot \rceil$ denotes rounding to the nearest integer.

Theorem 4.10. *Let $f : \mathbb{Z} \to \mathcal{R}$ be so that there exists a positive integer $s \leq N = 2^n$ such that $f(x) = f(x')$ if and only if $x - x'$ is an integer multiple of s. Then, the circuit in Figure 4.2*

produces $k \in \{0, \ldots, N-1\}$ of the form $k = \lfloor \ell N/s \rceil$ with probability at least $4/\pi^2$ for a random (but unknown) $\ell \in \{0, \ldots, s-1\}$.

Proof. Consider the subspace spanned by the vectors $|f(x)\rangle$ for $x \in \{0, \ldots, s-1\}$, and let $\tilde{F}$ be the quantum Fourier transform with respect to this basis. Then, we can rewrite the intermediary state of the quantum circuit, after U_f is applied, as

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|f(x)\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \otimes \tilde{F}\tilde{F}^\dagger |f(x)\rangle = \frac{1}{\sqrt{sN}} \sum_{\ell=0}^{s-1} \sum_{x=0}^{N-1} \omega_s^{-x\ell} |x\rangle \otimes \tilde{F}|f(\ell)\rangle \,.$$

Again, for the purpose of the analysis, we assume that the second register is measured, but now in the basis given by the $\tilde{F}|f(\ell)\rangle$'s. As a result, the state collapses to

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \omega_s^{-x\ell} |x\rangle$$

for a random $\ell \in \{0, \ldots, s-1\}$. We emphasize that this measurement is a thought experiment, which does not affect the (marginal) distribution of k. Applying F then results in

$$\frac{1}{N} \sum_{x=0}^{N-1} \sum_{k=0}^{N-1} \omega_s^{-x\ell} \omega_N^{xk} |k\rangle = \frac{1}{N} \sum_{k=0}^{N-1} \sum_{x=0}^{N-1} \omega_N^{x(k-\ell N/s)} |k\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \hat{1}_N(k - \ell N/s) |k\rangle \,,$$

and therefore, by Lemma 4.1, the final measurement produces $k = \lfloor \ell N/s \rceil$ with probability

$$p_{k|\ell} := \frac{\hat{1}_N(k - \ell N/s)^2}{N} \geq \frac{4}{\pi^2} \,,$$

which proves the claim. □

Given such a k as promised (with constant probability) by Theorem 4.10, we still need to solve the problem of finding s. Choosing $N \geq s^2$, we have that

$$\left| \frac{k}{N} - \frac{\ell}{s} \right| \leq \frac{1}{2N} \leq \frac{1}{2s^2} \,.$$

Thus, we may understand ℓ/s to be a *good* approximation of k/N by means of a fraction with a *small* denominator. Furthermore, it is easy to see that such an approximation is unique. Finally, Theorem 4.14 below shows that such an approximation ℓ/s, with a relation between approximation quality and denominator size as promised here, can be efficiently computed by means of the *continued fraction* of k/N.

Thus, if ℓ and s happen to be coprime (and k is as promised), s can directly be recovered; otherwise, $s' = s/\gcd(\ell, s)$ is obtained. Thus, similarly to period finding in $\mathbb{Z}/N\mathbb{Z}$, we can recover s from two executions *if* the respective ℓ's are coprime and the k's are of the right form $k = \lfloor \ell N/s \rceil$. With the bound/approximation on the probability of two numbers being coprime mentioned in Section 4.2, and the guarantee from Theorem 4.10, the probability of the above happening is shown to be lower bounded by a constant in the range 5% to 10%.

4.7 Continued Fractions

We briefly introduce here the basics of continued fractions, so as to understand the above claim on the efficient computability of good approximations.

Definition 4.4. *For any integer $n \geq 0$, and for any sequence of integers $a_0, a_1, \ldots, a_n$ with $a_0 \geq 0$ and $a_1, \ldots, a_n > 0$, we define $[a_0; a_1, \ldots, a_n]$ to be the* **continued fraction***, recursively defined via $[a_n] := a_n$ and*

$$[a_i; a_{i+1}, \ldots, a_n] := a_i + \frac{1}{[a_{i+1}; a_{i+2}, \ldots, a_n]}$$

for $0 \leq i < n$. In other words,

$$[a_0; a_1, \ldots, a_n] := a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots}}}$$

The a_i's are called the **partial quotients***, and $[a_0; a_1, \ldots, a_i]$ is called the i-th* **convergent***.*

We remark that, by definition, we require the partial quotients a_i to be (non-negative) integers; in some cases though, we will explicitly allow a_n to be in $\mathbb{R}$. This then allows us to write

$$[a_0; a_1, \ldots, a_n] = \left[a_0; a_1, \ldots, a_{n-1} + \tfrac{1}{a_n}\right]$$

or, more generally,

$$[a_0; a_1, \ldots, a_n] = \left[a_0; a_1, \ldots, a_{i-1}, [a_i; a_{i+1}, \ldots, a_n]\right].$$

Proposition 4.11. *Every positive $x \in \mathbb{Q}$ is a (finite) continued fraction $x = [a_0; a_1, \ldots, a_n]$, and the partial quotients are unique up to $[a_0; a_1, \ldots, a_{n-1}, 1] = [a_0; a_1, \ldots, a_{n-1}+1]$.*

Proof. We first note that for $x = [a_0; a_1, \ldots, a_n]$ with $n \geq 1$, $[a_1; a_2, \ldots, a_n] > 1$ unless $n = 1$ and $a_1 = 1$, and thus $x = [x - 1; 1] \in \mathbb{Z}$. This in particular shows uniqueness of a_0 for $x \notin \mathbb{Z}$.

Now, for a given positive $x \in \mathbb{Q}$, write $x = p/q$ for positive coprime integers p, q. If $q = 1$ then $x \in \mathbb{Z}$, and existence is thus clear: $x = [x]$, and (almost) uniqueness follows from the observation that if $x = [a_0; a_1, \ldots, a_n]$ then, by the above, x can be an integer only if $x = [x - 1; 1]$. Otherwise, we can write $p = a_0 q + r$ for integers a_0 and r with $0 < r < q$, and therefore

$$x = \frac{a_0 q + r}{q} = a_0 + \frac{r}{q} = a_0 + \frac{1}{x'}$$

for $x' := q/r > 1$. Given that $r < q$, we may assume by induction that $x' = [a_1; a_2, \ldots, a_n]$ exists and is (almost) unique, and we conclude existence and (almost) uniqueness of $x = [a_0; a_1, \ldots, a_n]$, where the latter exploits uniqueness of a_0 here. □

The above existence proof also shows that the partial quotients can be efficiently computed, essentially by means of the Euclidean algorithm.

Theorem 4.12. *For any continued fraction $x = [a_0; a_1, \ldots, a_n]$, let $(p_{-1}, q_{-1}), (p_0, q_0), \ldots, (p_n, q_n)$ be the sequence recursively defined as*

$$\begin{matrix} p_{-1} := 1 \\ q_{-1} := 0 \end{matrix}, \quad \begin{matrix} p_0 := a_0 \\ q_0 := 1 \end{matrix} \quad \text{and} \quad \begin{matrix} p_i := a_i p_{i-1} + p_{i-2} \\ q_i := a_i q_{i-1} + q_{i-2} \end{matrix}$$

for $i = 1, \ldots, n$. Then

$$\frac{p_i}{q_i} = [a_0; a_1, \ldots, a_i], \qquad \frac{p_{i-1}}{q_{i-1}} - \frac{p_i}{q_i} = \frac{(-1)^i}{q_i q_{i-1}} \qquad \text{and} \qquad \left|\frac{p_{i-1}}{q_{i-1}} - x\right| \leq \frac{1}{q_i q_{i-1}}$$

for all $i \in \{0, 1, \ldots, n\}$, respectively $i \in \{1, \ldots, n\}$ for the latter two claims.

From the second claim, it follows in particular that for *odd* indices i, the sequence of convergents p_i/q_i is monotonically *decreasing*, and monotonically *increasing* for *even* indices i; see the proof for some more details. Furthermore, given that it implies that $q_i p_{i-1} - p_i q_{i-1} = \pm 1$, the second claim ensures that p_i and q_i are coprime.

We also observe that, given that the q_i's are lower bounded by the Fibonacci numbers, which grow exponentially, the third claim implies that the convergents $[a_0; a_1, \dots, a_i]$ converge fast.

Before proving Theorem 4.12, we first prove the following.

Lemma 4.13. *For $n \geq 1$, let $x = [a_0; a_1, \dots, a_{n-1}, \xi_n]$ with an arbitrary $\xi_n \in \mathbb{R}$. Then,*

$$x = \frac{p_{n-1}\xi_n + p_{n-2}}{q_{n-1}\xi_n + q_{n-2}}\,.$$

Proof. For $n = 1$, the right hand side equals

$$\frac{a_0\xi_1 + 1}{\xi_1} = a_0 + \frac{1}{\xi_1} = x\,.$$

For $n > 1$ we recall that $[a_0; a_1, \dots, a_{n-1}, \xi_n] = [a_0; a_1, \dots, a_{n-1} + \frac{1}{\xi_n}]$ and apply induction to conclude that

$$x = \frac{p_{n-2}\big(a_{n-1} + \frac{1}{\xi_n}\big) + p_{n-3}}{q_{n-2}\big(a_{n-1} + \frac{1}{\xi_n}\big) + q_{n-3}} = \frac{p_{n-2}a_{n-1}\xi_n + p_{n-2} + p_{n-3}\xi_n}{q_{n-2}a_{n-1}\xi_n + q_{n-2} + q_{n-3}\xi_n} = \frac{p_{n-1}\xi_n + p_{n-2}}{q_{n-1}\xi_n + q_{n-2}}\,.$$

Thus, the claim holds for all $n \geq 1$. □

Proof (of Theorem 4.12). For the first claim, we simply apply Lemma 4.13 and conclude that

$$[a_0; a_1, \dots, a_i] = \frac{p_{i-1}a_i + p_{i-2}}{q_{i-1}a_i + q_{i-2}} = \frac{p_i}{q_i}$$

by definition of p_i and q_i. For the second claim, we observe that

$$q_i p_{i-1} - p_i q_{i-1} = (a_i q_{i-1} + q_{i-2})p_{i-1} - (a_i p_{i-1} + p_{i-2})q_{i-1} = p_{i-1}q_{i-2} - q_{i-1}p_{i-2}$$

and conclude by induction. Finally, as for the last claim, we show that

$$0 \leq (-1)^i\left(\frac{p_{i-1}}{q_{i-1}} - x\right) \leq \frac{1}{q_i q_{i-1}}$$

for all $i \leq n$. The case $i = n$ follows from the second claim, and for $i < n$ we observe that

$$(-1)^i\left(\frac{p_{i-1}}{q_{i-1}} - x\right) = (-1)^i\left(\frac{p_{i-1}}{q_{i-1}} - \frac{p_i}{q_i}\right) - (-1)^{i+1}\left(\frac{p_i}{q_i} - x\right) = \frac{1}{q_i q_{i-1}} - (-1)^{i+1}\left(\frac{p_i}{q_i} - x\right),$$

and so the claimed bounds follow by induction, noting that $q_{i+1} \geq q_{i-1}$. □

Theorem 4.12 in particular shows that the convergents are *good approximations*. What we need in Section 4.6 above is the converse: any good enough approximation must be a convergent.

Theorem 4.14. *If*

$$\left|\frac{p}{q} - x\right| \leq \frac{1}{2q^2}$$

then p/q is a convergent of x.

Proof. We may assume p and q to be coprime. Write $p/q = [a_0; a_1, \ldots, a_n]$ and let $\xi_{n+1} \in \mathbb{Q}$ be so that $x = [a_0; a_1, \ldots, a_n, \xi_{n+1}]$. We want to show that $\xi_{n+1} \geq 1$; this then implies that we can write $\xi_{n+1} = [b_0; b_1, \ldots, b_m]$ with $b_0 \geq 1$, so that $x = [a_0; a_1, \ldots, a_n, b_0, \ldots, b_m]$ and thus p/q is indeed a convergent of x.

For this purpose, write

$$\frac{p}{q} - x = \varepsilon \frac{\gamma}{q^2}$$

with $\varepsilon = \pm 1$ and $0 \leq \gamma \leq 1/2$. By the degree of freedom in choosing n one more or less, we may assume that $\varepsilon = (-1)^{n-1}$. Using that $p = p_n$ and $q = q_n$, which holds since $p/q = p_n/q_n$ and both are in lowest terms, and applying Lemma 4.13, we obtain

$$\varepsilon \frac{\gamma}{q_n^2} = \frac{p_n}{q_n} - x = \frac{p_n}{q_n} - \frac{p_n \xi_{n+1} + p_{n-1}}{q_n \xi_{n+1} + q_{n-1}} = \frac{p_n q_{n-1} - q_n p_{n-1}}{q_n (q_n \xi_{n+1} + q_{n-1})} = \frac{(-1)^{n-1}}{q_n (q_n \xi_{n+1} + q_{n-1})}\,,$$

where the last equality is due to Theorem 4.12. Thus, $\gamma(q_n \xi_{n+1} + q_{n-1}) = q_n$, and solving for ξ_{n+1} shows that

$$\xi_{n+1} = \frac{q_n - \gamma q_{n-1}}{\gamma q_n} = \frac{1}{\gamma} - \frac{q_{n-1}}{q_n} \geq 1\,,$$

which concludes the proof. □

4.8 Shor's Factoring Algorithm

We are now ready to understand Shor's quantum algorithm for factoring integers. As a matter of fact, all that is left to do is to to reduce factoring to period finding in $\mathbb{Z}$, and then we can apply the quantum algorithm from Section 4.6 to solve the latter.

Let N be the (odd) integer that we want to factor, and let $N = p_1^{e_1} \cdots p_m^{e_m}$ be its prime factorization. Let a be an integer in the range $\{1, \ldots, N-1\}$ that is coprime to N; if a is not coprime then we immediately can get a nontrivial factor of N. Shor's algorithm now simply works by computing the order $s := \mathrm{ord}(a)$ of a modulo N, i.e., the order of a as element in the group $(\mathbb{Z}/N\mathbb{Z})^*$, by applying the period finding algorithm to the function

$$f : \mathbb{Z} \to (\mathbb{Z}/N\mathbb{Z})^*,\ x \mapsto a^x\,,$$

where we understand a as an element in $(\mathbb{Z}/N\mathbb{Z})^*$. Indeed, by basic algebra, $a^x = a^{x'}$ if and only if $x - x'$ is a multiple of $\mathrm{ord}(a)$. The reduction from factoring to period finding in $\mathbb{Z}$ now follows from the following two propositions.

Proposition 4.15. *Let $N > 2$ be a positive integer and $a \in (\mathbb{Z}/N\mathbb{Z})^*$. If $s := \mathrm{ord}(a)$ is even and $b := a^{s/2}$ is neither 1 nor -1, then $\gcd(b+1, N)$ is a nontrivial divisor of N.*

Proof. Since, as integer, $b^2 \equiv 1 \pmod N$, it follows that N divides $b^2 - 1 = (b+1)(b-1)$. However, since $b \not\equiv \pm 1 \pmod N$, it follows that N divides neither $b+1$ nor $b-1$. Thus, some non-trivial factor of N must divide $b+1$ but not $b-1$, and vice versa. □

We also offer the following alternative proof (assuming N to be odd), which requires some basic understanding of the structure of $(\mathbb{Z}/N\mathbb{Z})^*$, but prepares for the proof of Proposition 4.16 below. Concretely, the proof makes use of the *Chinese Remainder Theorem*, which states that the canonical map

$$(\mathbb{Z}/N\mathbb{Z})^* \to (\mathbb{Z}/p_1^{e_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_m^{e_m}\mathbb{Z})^*\,,\ x \mapsto (x_1, \ldots, x_m)\,,$$

where x_i is the reduction of x modulo $p_1^{e_1}$, is an isomorphism, and of the fact that $(\mathbb{Z}/p^e\mathbb{Z})^*$ is cyclic with even order $p^{e-1}(p-1)$ for odd primes p, and so -1 is the only element with order 2.

Proof. We have $b^2 = a^s = 1$. Thus, for $i \in \{1, \ldots, m\}$, $b_i^2 = 1$ and hence $b_i = \pm 1$. However, as $b \neq \pm 1$, we must have that $b_i = -1$ for some i and $b_j = 1$ for some j. This then implies that, as integer, $b + 1$ is a multiple of $p_i^{e_i}$ but not of $p_j^{e_j}$. □

The following shows that if a is chosen uniformly at random then it satisfies the required properties with probability at least $1/2$, unless N is prime.

Proposition 4.16. *Let $N > 2$ be an odd integer with m distinct prime factors. Then, at most a 2^{-m+1}-fraction of the elements $a \in (\mathbb{Z}/N\mathbb{Z})^*$ are such that $s := \mathrm{ord}(a)$ is odd or $a^{s/2} = \pm 1$.*

Proof. We exploit the above isomorphism of $(\mathbb{Z}/N\mathbb{Z})^*$ into m cyclic groups $(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^*$ with even order. For instance, for any $a \in (\mathbb{Z}/N\mathbb{Z})^*$ the order s of a is the *lcm* of the respective orders s_i of the components a_i. We write $s = 2^d t$ for $0 \leq d \in \mathbb{Z}$ and $1 \leq t \in \mathbb{Z}$ odd, and similarly $s_i = 2^{d_i} t_i$. Then, $d = \max(d_1, \ldots, d_m)$, and thus $d = d_i$ for some i, and $t = lcm(t_1, \ldots, t_m)$.

Assume that $d_j < d$ for some j. Then, in particular, $d \geq 1$ and thus s is even. Furthermore,

$$a_i^{s/2} = a_i^{2^{d-1}t} = \left(a_i^{2^{d_i-1}t_i}\right)^{t/t_i} = \left(a_i^{s_i/2}\right)^{t/t_i} = (-1)^{t/t_i} = -1\,,$$

while, given that $s/2 = 2^{d-1}t$ is a multiple of $s_j = 2^{d_j}t_j$,

$$a_j^{s/2} = 1\,.$$

Thus, $a^{s/2} \neq \pm 1$.

Now, exploiting that $(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^*$ is cyclic with even order, say order $2^{\ell_i} r_i$ with $1 \leq \ell_i \in \mathbb{Z}$ and $1 \leq r_i \in \mathbb{Z}$ odd, half of the elements $a_i \in (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^*$ have $d_i = \ell_i$ (namely all the odd powers of a given generator), while all the other half has $d_i < \ell_i$. Thus, for any i, no matter what $a_1, \ldots, a_i$ and thus $d_1, \ldots, d_i$ are, at most half of the elements a_{i+1} have $d_{i+1} = d_i$, and thus may potentially give rise to an a with s odd or $a^{s/2} = \pm 1$. Thus, at most a $1/2^{m-1}$ fraction of $(a_1, \ldots, a_m)$ may give rise to such an a. □

4.9 Shor's Discrete-Logarithm Algorithm

Let G be a finite cyclic group with generator g. The order q of G may or may not be known. The **discrete logarithm** (with respect to g) of an element $h \in G$ is the unique $s \in \{0, \ldots, q-1\}$ with $g^s = h$. Given such an h, we observe that

$$f : \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \to G,\ (x, y) \mapsto g^x h^{-y} = g^{x-sy}$$

is such that $f(x, y) = f(x', y')$ if and only if $x - x' = s(y - y')$. Thus, the problem of computing the discrete logarithm reduces to period finding as considered in Section 4.3, up to some insignificant difference in the problem statement. Thus, one is tempted to invoke the quantum circuit from Figure 4.3 to find s. However, there are two issues with this approach: q may not be known, and, even if it is known, it may not be a power of 2, and so it is not clear whether the quantum Fourier transform over $\mathbb{Z}/q\mathbb{Z}$ could be done efficiently.

The solution (to both problems) is to choose a prime power $N = 2^n > q$, understand f as a function $\{0, \ldots, N-1\} \times \{0, \ldots, N-1\} \to G$ in the obvious way, and apply the quantum circuit from Figure 4.3, but now with the quantum Fourier transform over $\mathbb{Z}/N\mathbb{Z}$. The analysis is very similar to the analysis of the quantum circuit for period finding in $\mathbb{Z}$. Indeed, applying

F to the first two registers of $|0\rangle|0\rangle|0\rangle$, which are n-qubits each, and then applying U_f, results in

$$|0\rangle|0\rangle|0\rangle \mapsto \frac{1}{N}\sum_{x,y=0}^{N-1}|x\rangle|y\rangle|0\rangle \mapsto \frac{1}{N}\sum_{x,y=0}^{N-1}|x\rangle|y\rangle|f(x,y)\rangle = \frac{1}{N}\sum_{x,y=0}^{N-1}|x\rangle|y\rangle|f(x-sy,0)\rangle\,.$$

Somewhat similar to Section 4.6, we consider the subspace spanned by the vectors $|f(x,0)\rangle$ for $x \in \{0,\dots,q-1\}$, and we let $\tilde{F}$ be the quantum Fourier transform with respect to this basis. The above intermediary state, after U_f is applied, can then be written as

$$\frac{1}{N}\sum_{x,y=0}^{N-1}|x\rangle|y\rangle|f(x-sy,0)\rangle = \frac{1}{N\sqrt{q}}\sum_{\ell=0}^{q-1}\sum_{x,y=0}^{N-1}\omega_q^{-\ell(x-sy)}|x\rangle|y\rangle\otimes\tilde{F}|f(\ell,0)\rangle\,,$$

which, upon measuring the third register, collapses to

$$\frac{1}{N}\sum_{x,y=0}^{N-1}\omega_q^{-\ell(x-sy)}|x\rangle|y\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}\omega_q^{-\ell x}|x\rangle\otimes\frac{1}{\sqrt{N}}\sum_{y=0}^{N-1}\omega_q^{\ell sy}|y\rangle$$

for some $\ell \in \{0,\dots,q-1\}$. Applying F to the remaining two registers results in the tensor product of

$$\frac{1}{N}\sum_{x,k}\omega_q^{-\ell x}\omega_N^{xk}|k\rangle = \frac{1}{\sqrt{N}}\sum_{k}\hat{1}_N(k-\ell N/q)|k\rangle$$

and

$$\frac{1}{N}\sum_{y,m}\omega_q^{\ell sy}\omega_N^{ym}|m\rangle = \frac{1}{\sqrt{N}}\sum_{m}\hat{1}_N(m+\ell sN/q)|m\rangle\,.$$

Thus, when measuring, we observe $k = \lfloor \ell N/q \rceil$ and $m = -\lfloor \ell sN/q \rceil \bmod N$ with probability at least $16/\pi^4$, which is approximately 0.16. Here, if q is known (which is typically the case) then ℓ and ℓs, and thus s, can be recovered using elementary techniques; indeed, given that $q/N < 1$, we see that $\ell = \lfloor kq/N \rceil$ and $\ell s \bmod q = -\lfloor \ell mq/N \rceil$. Otherwise, i.e. if q is not know, ℓ and ℓs can be recovered using the techniques from continued fractions.