SHOR'S ALGORITHM

JACOB HEGNA

ABSTRACT. We give a short exposition of Shor's algorithm, which decides primality in polynomial time on a quantum computer. We utilize a standard exposition found in the literature which exports a bulk of the work to a quantum Fourier transform.

CONTENTS

1. INTRODUCTION

It is a famous theorem that given an integer $n \in \mathbb{Z}$, there is a unique expression

$$n = \alpha \prod_{i=0}^{k} p_i, \quad p_i \text{ prime for all } i, \quad \alpha \in \mathbb{Z}^\times.$$

In fact, this property is one of the most desirable properties that an algebra can have. Many other algebraic properties (locality, regularity, depth, etc) are a way to measure how close the structure is to achieving unique factorization. One could argue that the entire field of number theory is based on this simple fact.

This result is also fundamental to modern cryptography. The exact details are out of the scope of this expository note, but it is conjectured that the problem of prime factorization cannot be solved in polynomial time on a classical computer. Clearly, however, given n and a collection of primes $\{p_i\}$, one can verify with $\mathcal{O}(n^3)$ steps that $n = \pm \prod p_i$.

The situation is slightly different with quantum circuits.

Theorem 1.1 (Peter Shor)**.** *Supposing access to quantum circuits, primality is decidable in polynomial time.*

Date: May 16, 2019.

The proof requires a reduction via classical methods, an analysis of an eigenvalue problem, then concludes with a standard phase estimation circuit common in quantum computing.

2. The classical reduction

Throughout, let $y \in \mathbb{Z}$ be fixed. We compute the predicate

$$\psi(y) = \begin{cases} 0 & \text{if } y \text{ is prime,} \\ 1 & \text{else.} \end{cases}.$$

As it imposes no additional complexity, our algorithm will additionally return a single prime divisor p of y if $\psi(y) = 1$. Before giving the algorithm, we refresh the reader on an important definition.

Definition 2.1. Given a group $\mathbb{G}$ written multiplicatively and an element $g \in G$, the *period* of g is the integer $\min\{n \in \mathbb{Z}_{>1} \mid g^n = 1_{\mathbb{G}}\}$. If $\mathbb{G} = \mathbb{Z}_q$, we use the notation $\text{per}_q(g)$ for the period of g in $\mathbb{G}$.

2.1. **The algorithm.** This classical procedure is taken quite directly from [1]. The input is an integer $y \in \mathbb{Z}_{>1}$. The output is a pair (α, β) where $\alpha = \psi(y)$ and β is a (not necessarily prime) divisor of y if $\alpha = 1$.

Step 1. Return $(1, 2)$ if $y \equiv 0 \mod 2$. Else, continue.

Step 2. Check if $y = m^k$ for $m \in \{2, \dots, \log_2 y\}$. If so, return $(1, m)$. Else, continue.

Step 3. Impose a uniform distribution on the set $\{0, \dots, y-1\}$ and sample it for an integer a. If $\gcd(a, y) = b > 1$, return $(1, b)$. Else, continue with a reserved.

Step 4. Compute $r = \text{per}_y(a)$ using quantum methods. If r is odd, output $(0, 0)$. Else, continue with r, a reserved.

Step 5. Compute $d = \gcd(a^{r/2} - 1, y)$. If $d > 1$, return $(1, d)$. Else, return $(0, 0)$.

We have the following lemmas from [1] which verify correctness of the algorithm.

Lemma 2.2. *If the given algorithm returns $(1, d)$, then d is a nontrivial divisor of the input. However, if the algorithm returns $(0, s)$ for some s, it is not necessarily true that the input is prime.*

Proof. Omitted. □

Lemma 2.3. *The probability that the algorithm is correct for a given input y with k distinct prime divisors is at least $1 - 1/2^{k-1}$.*

Proof. Omitted. □

3. Determining the period

To determine the period, we begin by noting that the map

$$x \mapsto a^x \mod q,$$

for a, q coprime is a permutation of the integers $\{0, 1, \dots, q\}$. The orbit of this action which contains 1 is precisely size $\text{per}_q(a)$ (this is a rephrasing of the definition). So, given some encoding of an integer x on n bits (so that $q \leq 2^n$), we define a function f which maps x to $a^x \mod q$ if $x \leq q$ and to x otherwise. f is a permutation on n bits, so we may consider the operator $U_a := \widehat{f}$. We have the following lemma, taken from [2].

Lemma 3.1. $|\xi_k\rangle = \frac{1}{\sqrt{t}} \sum_{m=0}^{t-1} e^{-2\pi i(km/t)} |a^m\rangle$ *is an eigenvector of* U_a *with eigenvalue* $\lambda_k = e^{2\pi i(k/t)}$.

Proof. The operator U_a induces a permutation on the set of vectors $\{|1\rangle, |a^1\rangle, |a^2\rangle, \ldots, |a^t\rangle\}$ which maps $|a^\ell\rangle$ to $|a^{\ell+1}\rangle$, where addition in the exponent is interpreted modulo t. For $\ell \neq t-1$, we have that the $\ell+1$'th summand in $|\xi_k\rangle$ is equal to $e^{2\pi i(k/t)}$ times the ℓth summand. For the exceptional case $\ell = t-1$, one must observe that $e^{-2\pi i(t-1)k/t} = e^{2\pi ik/t}$ (the exponent in the first expression distributes into $-2\pi ik + 2\pi ik/t$, which is the same rotation as the second expression). □

Indeed, the t in the expansion of the eigenvalue λ_k is precisely $\mathrm{per}_q(a)$. Thus, if we can estimate this value with a probability bounded above $1/2$, we are done. Unfortunately, given an eigenvalue λ_k, we only know the value k/t, which may be reduced if $\gcd(k,t) > 1$. However, this problem will be resolved later.

4. Quantum Fourier Transform

We digress to implement a necessary circuit efficiently. We follow the exposition in [3].

Definition 4.1. The *Quantum Fourier Transform* is the unitary operation which maps a pure state $|x\rangle$ on 2^n qubits to

$$\frac{1}{2^{n/2}} \sum_{k=1}^{2^n-1} \omega^{xk} |k\rangle,$$

where ω is a 2^nth root of unity. It is defined for mixed states by linearity.

To write an efficient circuit for QFT, we need the following fact.

Theorem 4.2. *Let* $|x\rangle$ *be a pure state. Let* $(0.x_1x_2\ldots x_n) = x_1 2^{-1} + x_2 2^{-2} + \cdots + x_n 2^{-n}$ *be the binary decimal. Then,*

$$QFT(|x\rangle) = \frac{1}{2^{n/2}} \bigotimes_{r=1}^{n} \left(|0\rangle + e^{-2\pi i x 2^{-r}} |1\rangle \right).$$

Proof. The proof is a direct calculation.

$$\begin{aligned}
\sum_{k=1}^{2^n-1} \omega^{xk} |k\rangle &= \sum_{k_1,\ldots,k_n \in \{0,1\}} \omega^{-x \sum_{r=1}^{n} 2^{n-r} k_r} |k_1\rangle \otimes \cdots \otimes |k_n\rangle \\
&= \sum_{k_1,\ldots,k_n \in \{0,1\}} \bigotimes_{r=1}^{n} \omega^{-x 2^{n-r}} |k_r\rangle \\
&= \bigotimes_{r=1}^{n} \left(\sum_{k_r \in \{0,1\}} \omega^{-x 2^{n-r} k_r} |k_r\rangle \right)
\end{aligned}$$

At this point, note that we are summing over two values and we can just expand the sum.

$$= \bigotimes_{r=1}^{n} \left(|0\rangle + \omega^{-x2^{n-r}} |1\rangle \right)$$
$$= \bigotimes_{r=1}^{n} \left(|0\rangle + e^{-2\pi i x 2^{-r}} |1\rangle \right)$$

We now compute the exponent of the root of unity.

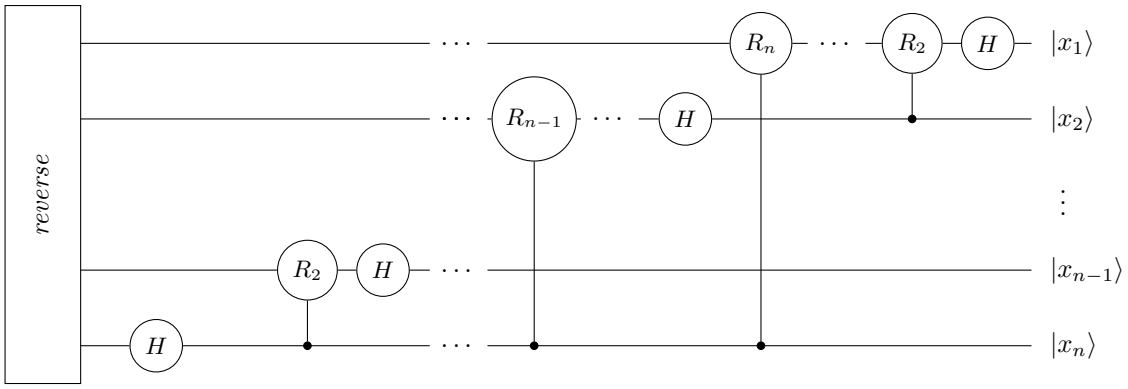
$$-2\pi i \sum_{\ell=1}^{n} 2^{n-r-\ell} x_\ell = -2\pi i (0.x_{n-r+1} x_{n-2+2} \dots x_n).$$

Multiply everything by $\frac{1}{2^{n/2}}$ and the proof is complete. □

We want to operate on qubits by multiplying their $|1\rangle$th coordinate by $e^{-2\pi i 2^{-s}}$ if $x_s = 1$, while fixing the $|0\rangle$th coordinate. By the magic of linear algebra, let us define

$$R_n := \begin{pmatrix} 1 & 0 \\ 0 & e^{-2\pi i 2^{-s}} \end{pmatrix}.$$

It is unitary by inspection (othonormal columns). Note that in the expression of the QFT from the prior problem, the value of the jth coordinate qubit in the original state only affects the value of the ith coordinate of the new state if $i \leq j$. With these two observations, we give the following circuit.



Proposition 4.3. *The circuit computes $QFT(|x\rangle)$ for a pure state $|x\rangle$.*

Proof. For the ith qubit in $|x\rangle$, the circuit prior to the reverse gate gives

$$\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i (0.j_i j_{i+1} \dots j_n)} \right)$$

by definition of $\Lambda(R_n)$. This is the value we wish to have in the $n-i$th qubit. Thus, after application of the reverse gate, the circuit is correct. □

Proposition 4.4. *QFT is unitary, as it is representable by a quantum circuit.*

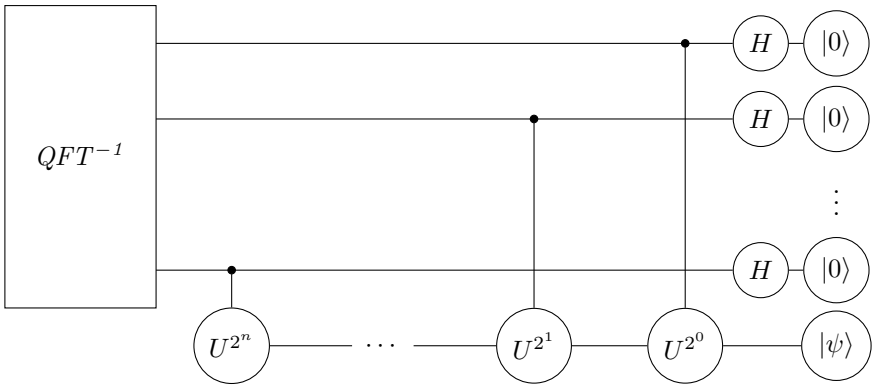
Theorem 4.5. *QFT and QFT^{-1} are computable with $\mathcal{O}(n^2)$ quantum gates.*

Proof. Proving the theorem for QFT proves it for QFT^{-1} automatically (they require the same number of gates). There are $n(n+1)/2$ gates before the reverse circuit, which contains the floor of $n/2$ gates of its own. □

5. Phase estimation

Currently the goal, more generally, is to compute ϕ where $U|\psi\rangle = e^{2\pi i\phi}|\psi\rangle$ (an eigenvalue problem).

Begin with an n-qubit register initialized to 0, and an n-qubit register initialized to the encoding of ψ, so we have the state $|0^n\rangle \otimes |\psi\rangle$. We apply the n-qubit Hadamard gate $H^{\otimes n}$ to the first register, and have the ith qubit of the first register control the operator U^{2^i} on the second register. Diagrammatically,



This circuit has $\mathcal{O}(n^2)$ gates for the inverse Quantum Fourier transform, and (when only given $U := U_a$), $\sum_{k=1}^{n} 2^k + n \leq n^3 + n$ gates for the rest of the circuit. This gives a total complexity of $\mathcal{O}(n^3)$ gates.

Now, let's compute the state in the first register before the inverse quantum Fourier transform. Trivially, we have that the state is

$$\frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} |k\rangle U^k |\psi\rangle.$$

However, we know that $U^k|\phi\rangle = e^{2\pi k i\phi}|\psi\rangle$, so the state is indeed

$$\frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi k i\phi} |k\rangle |\psi\rangle.$$

This is precisely the quantum Fourier transform of $|\psi\rangle \otimes |\phi\rangle$! Now, if we apply the inverse quantum Fourier transform and measure the first register, we will measure state ϕ.

Unfortunately, the eigenvalues of U_a themselves encode the period we desire. Fortunately, we have the following lemma from [2].

Lemma 5.1. *The sum of the eigenvectors ξ_k of U_a are equal to $|1\rangle$.*

Proof. Consider the coefficients of the vector on the right hand side of the following:

$$|1\rangle = \frac{1}{\sqrt{t}} \sum_{k=0}^{t-1} |\xi_k\rangle.$$

Each coefficient is of the form

$$\frac{1}{t}\sum_{k=0}^{t-1} e^{-2\pi i(km/t)},$$

for some m. In the case $m = 0$, we clearly have the coefficient is 1. To analyze the case $m > 1$, we recall from problem 2 that $e^{-2\pi i(m/t)}$ satisfies $x^t - 1 = 0$. Thus, it satisfies either $x - 1 = 0$ or $\sum_{k=0}^{t-1} x^k = 0$ (one can see geometrically that it must be the second). However, this implies all the coordinates outside of the $|1\rangle$th are zero. □

Thus, if we use $|\phi\rangle = |1\rangle$, we will sample a uniform distribution over km/t for $k \in \{0, \dots, t-1\}$. There are now two ways to recover t. The first is involves continued fractions.

5.1. **Estimating t with continued fractions.** We cite the following results from the literature. For a reference, see [4].

Theorem 5.2. *Let $x \in \mathbb{Q}$. Let $s, r \neq 0$ be two integers. If*

$$\left|x - \frac{s}{r}\right| < \frac{1}{2r^2},$$

then s/r is a convergent of x.

Theorem 5.3. *Let $c := km/t$ as the measurement of the previous quantum circuit. Then, the probability that there exists an integer s so that $\gcd(s,t) = 0$ and*

$$\left|\frac{c}{2^n} - \frac{s}{r}\right| < \frac{1}{2r^2}$$

is bounded below by

$$\frac{4}{\pi^2}\frac{\phi(t)}{t}\left(1 - \frac{1}{N}\right)$$

where $\phi(t)$ is Euler's totient function.

Now, with these two results, we may end the proof of the algorithm. There exists (with bounded probability) a measurement of the first quantum register c such that $|c/2^n - s/t| < \frac{1}{2t^2}$ for t the period and $\gcd(s,t) = 1$. We compute (in polynomial time) the value s for the expansion of $c/2^n$ (this is just Euler's algorithm), then simply check if the denominator of $\frac{s}{t}$ (by hypothesis this is reduced) is $\text{per}_q(a)$.

5.2. **Estimating t by** lcd **methods.**

Proposition 5.4. *Given $\ell > 2$ fractions of the form k_i/t written in their reduced form as k_i'/t_i', the probability that their least common denominator is not t is less than $3 \cdot 2^{-\ell}$.*

Proof. The problem is equivalent to determining the probability that $\gcd(k_1, \dots, k_\ell)$ is greater than 1. Given a fixed prime p, the probability that p divides each k is bounded above by $1/p^\ell$. To compute the probability that the k_i's have a common divisor greater than 1, we must sum the prior estimate for all primes p, so we have

$$\sum_{p \text{ prime}} \frac{1}{p^\ell} < \sum_{k=1}^{\infty} \frac{1}{k^\ell} < 3 \cdot 2^\ell,$$

computed as a geometric series. □

We many compute the lcd in $\mathcal{O}(n^3)$ steps, giving t.

References

[1] A. Y. Kitaev, A. H. Shen, and M. N. Vyalyi, *Classical and Quantum Computation*. American Mathematical Society, 2002.
[2] J. Hegna, "Problem set 12," *EECS 700*, 2019.
[3] F. X. Lin, "Shor's algorithm and the quantum fourier transform," 2013.
[4] C. Pittet, "Mathematical aspects of shor's algorithm," 11 2013.