An Introduction to Shor's Algorithm

Qiyu Liu[1]

[1]Department of Physics, University of California at San Diego, La Jolla, CA 92093

March 24, 2023

1 Abstract

In this paper, we first analyze the reduction from factorization to period-finding. Then, we look at the quantum circuit that finds the period. Lastly, we explain why this circuit works by analyzing the eigenstates of the unitary operator and see how QPE give us the period back.

2 Introduction

Many modern encryption algorithms rely on the concept that the factorization of large integer N takes exponential time on classical machines. However, the advent of quantum technologies and algorithms revolutionize the field of encryption that there exist quantum algorithms that can solve the factorization problem in polynomial time. This paper aims to explain one of the most famous such algorithms, the Shor's algorithm, and how it achieves the exponential speed-up of the factorization problem.

3 Factorization to Period-Finding

To utilize the power of quantum machines, we want to reduce the problem of finding prime factors p, q such that $N = p * q$ to the finding the period of modular exponential function. Let's define the function as follow:

$$f(x) = a^x \bmod N$$

Note that if we find the smallest positive integer value r that satisfy $f(r) = a^r \bmod N = 1$, we are very close to find the prime factorization p, q as I have shown below.

$$\begin{aligned} a^r - 1 &= (a^{r/2} - 1)(a^{r/2} + 1) \\ &= kN \text{ where k is a postive integer} \end{aligned}$$

It is promising to see that if we find the solution for $f(r) = 1$, we can find the prime factorization of N. However, we don't actually know what is the constraints on a and if this function has a solution for $r > 0$. To actually prove that there's solutions to $f(r) = 1$ for some value a, we want to invoke the Euler's theorem.

$$a^{\phi(N)} = 1 \bmod N$$

$\phi(N)$ is the Euler's totient function, and this theorem holds when a, N are co-prime of each other. Using this theorem, we can show that $f(x)$ is, in fact, a periodic function.

$$\begin{aligned} f(x + \phi(N)) &= (a^x \bmod N) * (a^{\phi(N)} \bmod N) \\ &= a^x \bmod N \\ &= f(x) \end{aligned}$$

Since $f(x)$ is periodic and $f(0) = 1$, there must exist a periodic value $r > 0$ at a later period where $f(0 + r) = 1$, proving that a non-trivial solution exist for $f(r) = 1$. One caveat to note is that the

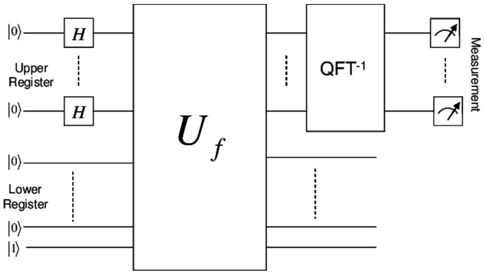

Figure 1: Shor's Circuit

period r is not necessarily a even number for the factorization to work. In that case, we just have to select another co-prime value a.

4 Quantum Circuit

The circuit in Figure 1 is the quantum circuit that finds the period r. Let's walk through the circuit and analyze what it is doing. Let's call the upper register x and the lower register w.

$$|\psi\rangle = |x\rangle_n |w\rangle_n = |0\rangle_n^{\otimes n} |0\rangle_n^{\otimes n}$$

Applying Hadamard gate to the x registers

$$|0\rangle_n^{\otimes n} |0\rangle_n^{\otimes n} \rightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle_n |0\rangle_n^{\otimes n}$$

Next, controlled unitary gates that compute the modular exponential is applied to w registers with x registers as the control, and we can obtain

$$\frac{1}{\sqrt{2^n}} \sum_{i}^{2^n-1} |k\rangle_n \left|a^k(\text{mod} N)\right\rangle_n$$

Recall from section 1 that $f(x) = a^x \bmod N$ is periodic. Then the terms in the w registers follow a periodic pattern and will form a set. Let's define the element of set as m_k, where k denotes the input argument. Due to the periodic nature of this function, $m_k = m_0$ for some k where $k =$ integer$*r$.

Next, we will take measurement on the w registers. Note that if we measure some value m, all the other terms where $m_k \neq m$ will collapse. So we are left with the following, we define the number of terms remaining as A for normalization.

Table 1:

x registers	w registers
$\vert 0\rangle$	$\vert m_0\rangle$
$\vert 1\rangle$	$\vert m_1\rangle$
...	...
$\vert 0+r\rangle$	$\vert m_0\rangle$
$\vert 1+r\rangle$	$\vert m_1\rangle$
...	...

$$\frac{1}{\sqrt{A}}(|k_0\rangle_n + |k_0 + r\rangle_n + |k_0 + 2r\rangle_n + \dots)$$

This looks very promising, as we are seeing that each term are separated by the period r. Now, applying the inverse quantum Fourier transform will give us the period back[1].

5 Analysis

We now know the circuit in figure 1 helps us find the period r. But why does it? What's the physical meaning behind this circuit. To fully understand it, we have to understand quantum phase estimation[2], since this circuit is almost identical to the QPE circuit. Let's first look at the eigenstates of the $U|w\rangle = |xw \bmod N\rangle$.

$$|u_i\rangle = \frac{1}{\sqrt{2}} \sum_{k=0}^{r-1} e^{-2\pi i k/r} \left|a^k \bmod N\right\rangle$$

If we ought to sum up these states, all the phases cancel and we will be left with $|1\rangle$ in the computational basis.

$$\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |u_s\rangle = |1\rangle$$

[1] See Appendix A for explanation of quantum fourier transformation

[2] See Appendix B for explanation of quantum phase estimation

If we do quantum phase estimation on U, we will measure a phase, since $|1\rangle$ is the superposition of all the eigenstates.

$$\theta = \frac{k}{r}$$

Knowing that k and r are finite and integers, we can use the continued fraction algorithm to find the period r. The continued fraction algorithm is very mature in classical machine, and can be easily computed on modern computers. Thus, we can find the period r from θ.

A Quantum Fourier Transformation

Quantum Fourier Transform take computational basis to Fourier basis, acting it on n states is as follow:

$$|x\rangle \rightarrow \frac{1}{\sqrt{2^n}}(|0\rangle+e^{2\pi i x/2^0}|1\rangle)\otimes\cdots\otimes(|0\rangle+e^{2\pi i x/2^n}|1\rangle)$$

B Quantum Phase Estimation

Quantum Phase Estimation allows for estimation of θ in $U|\psi\rangle = e^{2\pi i\theta}|\psi\rangle$ for unitary gates. A general QPE circuit is consisted of $|0\rangle^n \otimes |\psi\rangle$. The QPE circuit first applies the Hadamard gate to the first n qubits.

$$\frac{1}{\sqrt{2^n}}(|0\rangle + |1\rangle)^{\otimes n} \otimes |\psi\rangle$$

Then, we controlled unitary is applied on the target register, the $|\psi\rangle$, only if the control register, the upper n bits, is 1. Applying the n controlled operations CU^{2j} to the circuit, we get

$$\frac{1}{\sqrt{2}}\sum_{k}^{2^n-1} e^{2\pi i\theta k}|k\rangle \otimes |\psi\rangle$$

This result looks exactly like if we apply QFT to n states with $x = \theta 2^n$. Therefore, we apply the inverse QFT:

$$\frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{k=0}^{2^n-1} e^{-2\pi i k(x-\theta 2^n)/2^n}|x\rangle \otimes |psi\rangle$$

Now, measurement on the upper qubits will yield high probability for $\theta 2^n$. Since n is known, we can thus find the phase θ.

References

[1] Dave Bacon, “CSE 599d - Quantum Computing Shor’s Algorithm”

[2] N. David Mermin, Physics Today, B **60**, 10, 10(2017); doi: 10.1063/1.2800253

[3] Team, T. Q. Quantum phase estimation. qiskit.org (2022). Available at: https://qiskit.org/textbook/ch-algorithms/quantum-phase-estimation.html.

[4] Fast Quantum Modular Exponentiation Architecture for Shor’s Factorization Algorithm - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/High-level-diagram-of-Shors-algorithm-Upper-register-consists-of-2n-qubits-and-holdsfig228102587 [accessed 22 Mar, 2023]