Shor's Algorithm

Manu Isaacs
manu.isaacs@gmail.com

July 17, 2023

What is Shor's Algorithm?

Shor's algorithm is an algorithm which runs on a quantum computer which factors the n-bit number M in polynomial time in n. It outperforms all classical factoring algorithms, none of which run in polynomial time. The algorithm, developed by Peter Shor in 1995, is one of the most important algorithms in quantum computing.

This talk begins with the basics of quantum computing and builds up to Shor's algorithm

What is a Qubit?

A qubit is the smallest possible unit of information in quantum computing. It can be physically realized by the spin of an electron or the polarization of a photon, for example. For our purposes, we can define a qubit as a two-element unit vector of complex numbers.

What is a Qubit?

A qubit is the smallest possible unit of information in quantum computing. It can be physically realized by the spin of an electron or the polarization of a photon, for example. For our purposes, we can define a qubit as a two-element unit vector of complex numbers.

Throughout this talk, we will use Dirac's braket notation. Defining $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, we can write a qubit $|\phi\rangle$ as

$$|\phi\rangle = a\,|0\rangle + b\,|1\rangle \,,$$

where $|a|^2 + |b|^2 = 1$.

Bases of the Vector Space of a Qubit

Notice that $\{|0\rangle, |1\rangle\}$ is a basis of the vector space V of a qubit. We call this the *standard basis*. Defining

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle),$$

we see that $\{|+\rangle, |-\rangle\}$ is also a basis of V. This basis is called the *Hadamard Basis*.

Measurement of a Single Qubit

The first operation on a qubit that we will look at is called measurement. This is the only way in which we can obtain information about a qubit.

Measurement of a Single Qubit

The first operation on a qubit that we will look at is called measurement. This is the only way in which we can obtain information about a qubit.

When we measure the qubit

$$|\phi\rangle = a\,|\beta_1\rangle + b\,|\beta_2\rangle$$

in the basis $\{\beta_1, \beta_2\}$, we observe $|\beta_1\rangle$ with probability $|a|^2$ and $|\beta_2\rangle$ with probability $|b|^2$. Furthermore, the state of the qubit itself changes to what it is measured as.

Measurement of a Single Qubit

The first operation on a qubit that we will look at is called measurement. This is the only way in which we can obtain information about a qubit.

When we measure the qubit

$$|\phi\rangle = a\,|\beta_1\rangle + b\,|\beta_2\rangle$$

in the basis $\{\beta_1, \beta_2\}$, we observe $|\beta_1\rangle$ with probability $|a|^2$ and $|\beta_2\rangle$ with probability $|b|^2$. Furthermore, the state of the qubit itself changes to what it is measured as.

Note that the restriction of a qubit is what disallows a qubit from carrying infinite information, despite a and b being of arbitrary precision, a single qubit carries only one bit of information, because, like a bit, there are only two outcomes when it is observed.

Example of Single-Qubit Measurement

Let's consider what happens when the qubit $|0\rangle$ is measured first in the Hadamard basis and then in the standard basis.

Example of Single-Qubit Measurement

Let's consider what happens when the qubit $|0\rangle$ is measured first in the Hadamard basis and then in the standard basis.

To compute the probabilities for measurement in the standard basis, we have to write $|0\rangle$ in the Hadamard basis: $|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$. In this case, we see that $|a|^2 = |b|^2 = \frac{1}{2}$, so after measuring in the Hadamard basis, the qubit becomes either $|+\rangle$ or $|-\rangle$ each with equal probability. Then, recalling the definitions of $|+\rangle$ and $|-\rangle$, we see that measurement of either of them in the standard basis results in $|0\rangle$ or $|1\rangle$ again with equal chance.

Multi-Qubit Systems

The vector space of an n-qubit system is $V = V_0 \otimes V_1 \otimes V_2 \dots V_n$, where V_i is the vector space of the i-th qubit and $\otimes$ is the *tensor product*.

Multi-Qubit Systems

The vector space of an n-qubit system is $V = V_0 \otimes V_1 \otimes V_2 \ldots V_n$, where V_i is the vector space of the i-th qubit and $\otimes$ is the *tensor product*. Then the basis of V is

$$\begin{gathered}\{|0\rangle_{n-1} \otimes |0\rangle_{n-2} \otimes \cdots \otimes |0\rangle_1 \otimes |0\rangle_0 , \\ |0\rangle_{n-1} \otimes |0\rangle_{n-2} \otimes \cdots \otimes |0\rangle_1 \otimes |1\rangle_0 , \\ |0\rangle_{n-1} \otimes |0\rangle_{n-2} \otimes \cdots \otimes |1\rangle_1 \otimes |0\rangle_0 , \\ \vdots \\ |1\rangle_{n-1} \otimes |1\rangle_{n-2} \otimes \cdots \otimes |1\rangle_1 \otimes |1\rangle_0\}\end{gathered}$$

but this is extremely clunky. Let's remove the tensor products and subscripts, and combine the kets together:

$$\{|00\ldots00\rangle , |00\ldots01\rangle , |00\ldots10\rangle \ldots |11\ldots11\rangle\}.$$

Different representation of the Basis of a Multi-Qubit System

We can also write the basis as

$$\{|0\rangle, |1\rangle, |2\rangle \ldots |N-1\rangle\}$$

where $N = 2^n$ by writing each basis element in binary.

Different representation of the Basis of a Multi-Qubit System

We can also write the basis as

$$\{|0\rangle, |1\rangle, |2\rangle \dots |N-1\rangle\}$$

where $N = 2^n$ by writing each basis element in binary. We can also write the basis in vector notation, where each basis vector has N elements:

$$\left\{ \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \dots \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \right\}.$$

Example of a Multi-Qubit System

In ket notation, $|a\rangle \otimes |b\rangle = |a\rangle |b\rangle = |ab\rangle$ all mean the same thing. Let's consider the multiplication of two qubits as an example:

$$(a|0\rangle + b|1\rangle)(c|0\rangle + d|1\rangle) = ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle .$$

Example of a Multi-Qubit System

In ket notation, $|a\rangle \otimes |b\rangle = |a\rangle |b\rangle = |ab\rangle$ all mean the same thing. Let's consider the multiplication of two qubits as an example:

$$(a|0\rangle + b|1\rangle)(c|0\rangle + d|1\rangle) = ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle .$$

In vector notation, that would be

$$\begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix} .$$

A Useful Observation

We make the following claim which will be useful in Shor's Algorithm:

$$\underbrace{|+\rangle\,|+\rangle\ldots|+\rangle}_{n \text{ times}} = \frac{1}{\sqrt{N}}(|0\rangle + |1\rangle + \ldots |N-1\rangle).$$

A Useful Observation

We make the following claim which will be useful in Shor's Algorithm:

$$\underbrace{|+\rangle\,|+\rangle \ldots |+\rangle}_{n \text{ times}} = \frac{1}{\sqrt{N}}(|0\rangle + |1\rangle + \ldots |N-1\rangle).$$

We can rewrite the left hand side as $\frac{1}{\sqrt{N}}\underbrace{(|0\rangle + |1\rangle)(|0\rangle + |1\rangle) \ldots (|0\rangle + |1\rangle)}_{n \text{ times}}$. For each term in the binomial expansion of this expression, we get a distinct number whose binary representation ranges from $|0\rangle$ to $|N-1\rangle$, and this is the right hand side.

Measurement of a Multi-Qubit system

How does measurement of a single qubit generalize to measurement of multiple qubits? For a vector space V of an n-qubit system, we say that a measuring device is defined by a *subspace decomposition* of V, that is, some $\{S_i\}$ satisfying

$$S_1 \oplus S_2 \oplus \cdots \oplus S_k = V$$

Measurement of a Multi-Qubit system

How does measurement of a single qubit generalize to measurement of multiple qubits? For a vector space V of an n-qubit system, we say that a measuring device is defined by a *subspace decomposition* of V, that is, some $\{S_i\}$ satisfying

$$S_1 \oplus S_2 \oplus \cdots \oplus S_k = V$$

where $\oplus$ is the *direct sum*. Then, what happens when this device measures some $|v\rangle \in V$?

Measurement of a Multi-Qubit system

How does measurement of a single qubit generalize to measurement of multiple qubits? For a vector space V of an n-qubit system, we say that a measuring device is defined by a *subspace decomposition* of V, that is, some $\{S_i\}$ satisfying

$$S_1 \oplus S_2 \oplus \cdots \oplus S_k = V$$

where $\oplus$ is the *direct sum*. Then, what happens when this device measures some $|v\rangle \in V$? We know $|v\rangle$ satisfies

$$|v\rangle = c_1 |s_1\rangle + c_2 |s_2\rangle + \cdots + c_k |s_k\rangle$$

for unit vectors $|s_i\rangle \in S_i$. When $|v\rangle$ is measured, we get the state $|s_i\rangle$ with probability $|c_i|^2$, and as before, the state itself changes to what we measure it as.

Example of Multi-Qubit Measurement

Let's say we want to measure the first qubit of the qubit

$$|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle .$$

Example of Multi-Qubit Measurement

Let's say we want to measure the first qubit of the qubit

$$|\psi\rangle = a_{00}\,|00\rangle + a_{01}\,|01\rangle + a_{10}\,|10\rangle + a_{11}\,|11\rangle\,.$$

Then, S_1 is spanned by $\{|00\rangle\,, |01\rangle\}$ and S_2 is spanned by $\{|10\rangle\,, |11\rangle\}$.

Example of Multi-Qubit Measurement

Let's say we want to measure the first qubit of the qubit

$$|\psi\rangle = a_{00}\,|00\rangle + a_{01}\,|01\rangle + a_{10}\,|10\rangle + a_{11}\,|11\rangle\,.$$

Then, S_1 is spanned by $\{|00\rangle\,,|01\rangle\}$ and S_2 is spanned by $\{|10\rangle\,,|11\rangle\}$. So, if $|\psi\rangle = c_1\,|s_1\rangle + c_2\,|s_2\rangle$ then we have:

$$\begin{aligned}
c_1 &= \sqrt{|a_{00}|^2 + |a_{01}|^2} \\
c_2 &= \sqrt{|a_{10}|^2 + |a_{11}|^2} \\
|s_1\rangle &= \frac{1}{c_1}(a_{00}\,|00\rangle + a_{01}\,|01\rangle) \\
|s_2\rangle &= \frac{1}{c_2}(a_{10}\,|10\rangle + a_{11}\,|11\rangle)
\end{aligned}$$

Example of Multi-Qubit Measurement

Then, when we measure $|\psi\rangle$, we will get the state $|s_1\rangle$ with probability $|c_1|^2 = |a_{00}|^2 + |a_{01}|^2$ and the state $|s_2\rangle$ with probability $|c_2|^2 = |a_{10}|^2 + |a_{11}|^2$.

Example of Multi-Qubit Measurement

Then, when we measure $|\psi\rangle$, we will get the state $|s_1\rangle$ with probability $|c_1|^2 = |a_{00}|^2 + |a_{01}|^2$ and the state $|s_2\rangle$ with probability $|c_2|^2 = |a_{10}|^2 + |a_{11}|^2$.

Notice that in $|s_1\rangle$ the first qubit is $|0\rangle$ and in $|s_2\rangle$ the first qubit is $|1\rangle$. Because of this, measurement of a single qubit can be thought of as collapsing that qubit from a superposition (nontrivial linear combination) of $|0\rangle$ and $|1\rangle$ into either $|0\rangle$ or $|1\rangle$.

Quantum State Transformations

The other type of operation on a quantum state are transformations, or gates. These transformations can be represented by unitary matrices. A unitary matrix U satisfies $UU^\dagger = I$ where $U^\dagger$ is the conjugate transpose of U. We start by looking at some important quantum gates.

The Not, Hadamard, and Toffoli Gates

We define the not gate X, Hadamard gate H, and Toffoli gate T as follows:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$T = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

The Function of the Not and Hadamard Gates

Notice that the not gate sends $|0\rangle$ to $|1\rangle$ and vice versa:

$$X|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle ,$$

$$X|1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle .$$

The Function of the Not and Hadamard Gates

Notice that the not gate sends $|0\rangle$ to $|1\rangle$ and vice versa:

$$X|0\rangle = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix} = \begin{pmatrix}0\\ 1\end{pmatrix} = |1\rangle\,,$$

$$X|1\rangle = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}0\\ 1\end{pmatrix} = \begin{pmatrix}1\\ 0\end{pmatrix} = |0\rangle\,.$$

Notice also that the Hadamard gate sends $|0\rangle$ to $|+\rangle$ and $|1\rangle$ to $|-\rangle$:

$$H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 1\end{pmatrix} = |+\rangle\,,$$

$$H|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0\\ 1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ -1\end{pmatrix} = |-\rangle\,.$$

The Function of the Toffoli Gate

The Toffoli gate acts on 3 qubits. It applies the X gate to the last qubit, called the target qubit, only if the first two qubits (called control qubits) are both $|1\rangle$. In other words, the Toffoli gate sends $|110\rangle$ to $|111\rangle$ and vice versa but sends all other basis elements to themselves.

How to Perform Classical Computations

Notice that if U is unitary, so is U^{-1}. This means that all quantum gates are reversible. But the same is not true of classical gates. For example, consider the **AND** gate $\wedge$. There is no way to recover x and y given $x \wedge y$. However, it is still possible to construct classical gates using quantum gates.

How to Perform Classical Computations

Notice that if U is unitary, so is U^{-1}. This means that all quantum gates are reversible. But the same is not true of classical gates. For example, consider the **AND** gate $\wedge$. There is no way to recover x and y given $x \wedge y$. However, it is still possible to construct classical gates using quantum gates.

It is well known that the set of classical gates $\{\textbf{AND}, \textbf{NOT}\}$ is *functionally complete*, meaning that using these two gates it is possible to do any classical computation. Then, it suffices to find quantum analogues of these two gates.

The Quantum Analogue of the AND and NOT Gates

Notice that the quantum gate X is essentially the classical **NOT** gate. But how do we create a quantum **AND** gate? One way is to use the Toffoli gate:

$$T\left|x, y, 0\right\rangle = \left|x, y, x \wedge y\right\rangle .$$

Then we can simply ignore the first two qubits and only use the third one. The problem with this is that this approach will take up a lot of space. However, there is a way to reduce the space with minimal increase in the number of gates.

A Note on Efficiency of Classical Computations

The key to performing space-efficient computations is to undo operations after they have served their purpose, and then use those qubits again. If we do this in the right way, then it possible to construct quantum circuit with similar efficiency as their classical counterpart.

A Note on Efficiency of Classical Computations

The key to performing space-efficient computations is to undo operations after they have served their purpose, and then use those qubits again. If we do this in the right way, then it possible to construct quantum circuit with similar efficiency as their classical counterpart.

Specifically, if any classical circuit uses t gates and s bits, it has a quantum (reversible) counterpart using only $O(t^{1+\epsilon})$ gates and $O(s \log t)$ qubits.

The Quantum Fourier Transform

The quantum Fourier transform (QFT) is a key part of Shor's algorithm and other quantum algorithms. It is very similar to the discrete Fourier transform.

The Quantum Fourier Transform

The quantum Fourier transform (QFT) is a key part of Shor's algorithm and other quantum algorithms. It is very similar to the discrete Fourier transform.

We define the *quantum Fourier transform* as

$$U_f^{(n)} : \sum_{x=0}^{N-1} a(x) \left| x \right\rangle \to \sum_x A(x) \left| x \right\rangle ,$$

where

$$A(x) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} a(k) \exp\left(2\pi i \frac{kx}{N}\right) .$$

where $N = 2^n$ and the domain of a and A is $\{0, 1, \ldots N-1\}$. It can be shown that $U_f^{(n)}$ is indeed a unitary matrix.

Example: Applying the QFT to a Periodic Function

Consider the function $a(x) = \exp(-2\pi i \frac{ux}{N})$ where $0 \leq u < N$ Notice that a is a periodic function with period $r = N/u$ dividing N. Let's compute $A(x)$:

$$\begin{aligned} A(x) &= \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} a(k) \exp\left(2\pi i \frac{kx}{N}\right) \\ &= \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp\left(-2\pi i \frac{uk}{N}\right) \exp\left(2\pi i \frac{kx}{N}\right) \\ &= \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp\left(2\pi i \frac{k(u-x)}{N}\right). \end{aligned}$$

Applying the QFT to a Periodic Function

Letting $y = u - x$, we can see that

$$\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp\left(2\pi ik\frac{y}{N}\right) = 0$$

if $y \not\equiv 0 \pmod{N}$ by the roots of unity. However, it is clear that if $y \equiv 0 \pmod{N}$, we have that each term in the sum is simply 1 and we get

$$\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp\left(2\pi ik\frac{r}{N}\right) = \frac{1}{\sqrt{N}}N = \sqrt{N}$$

So, for $0 \leq x < N$, the only x such that $A(x) \neq 0$ is $x = u$. That is,

$$A(x) = \begin{cases} 0 & \text{if } x \neq u \\ \sqrt{N} & \text{if } x = u. \end{cases}$$

Applying the QFT to a Periodic Function

It is well known that any function with period u can be approximated as the sum of exponentials with periods which are multiples of u. Suppose we measure the quantum state after applying the QFT. Then, we are guarenteed to measure a state of the form $|uj\rangle = |j\frac{N}{r}\rangle$ for some integer j.

Applying the QFT to a Periodic Function

It is well known that any function with period u can be approximated as the sum of exponentials with periods which are multiples of u. Suppose we measure the quantum state after applying the QFT. Then, we are guarenteed to measure a state of the form $|uj\rangle = |j\frac{N}{r}\rangle$ for some integer j.

But what if the period of a, r, doesn't evenly divide N? It can be shown that we will still measure integers close to $j\frac{N}{r}$ with high probability.

Applying the QFT to a Periodic Function

It is well known that any function with period u can be approximated as the sum of exponentials with periods which are multiples of u. Suppose we measure the quantum state after applying the QFT. Then, we are guarenteed to measure a state of the form $|uj\rangle = |j\frac{N}{r}\rangle$ for some integer j.

But what if the period of a, r, doesn't evenly divide N? It can be shown that we will still measure integers close to $j\frac{N}{r}$ with high probability.

In Shor's algorithm, we will use the QFT to find the period of a function with high probability. We will be able to use this number to factor.

Converting the Factoring Problem to a Period Finding Problem

This is the first step of Shor's Algorithm. Say we want to factor the number M. Consider the function $f(k) = a^k \pmod{M}$. Let the period of this function be r. Notice that when $n > 2$, $r = \phi(n)$ is even, so we can write

$$0 \equiv a^r - 1 \equiv (a^{r/2} - 1)(a^{r/2} + 1) \pmod{M}$$

Then, with high probability, $\gcd(a^{r/2} + 1, M)$ is a nontrivial factor of M.

Converting the Factoring Problem to a Period Finding Problem

This is the first step of Shor's Algorithm. Say we want to factor the number M. Consider the function $f(k) = a^k \pmod{M}$. Let the period of this function be r. Notice that when $n > 2$, $r = \phi(n)$ is even, so we can write

$$0 \equiv a^r - 1 \equiv (a^{r/2} - 1)(a^{r/2} + 1) \pmod{M}$$

Then, with high probability, $\gcd(a^{r/2} + 1, M)$ is a nontrivial factor of M.

If we can find the period of f, that will allow us to factor M. Now let's discuss the quantum core of the algorithm, finding the period of f.

The Quantum Part Of Shor's Algorithm

First, pick the $N = 2^n$ such that $M^2 < N < 2M^2$. Consider the state $|00\dots0\rangle$ with n zeroes. Then consider

$$\underbrace{H \otimes H \otimes \cdots \otimes H}_{n \text{ times}} |00\dots0\rangle$$

Recalling that $H|0\rangle = |+\rangle$ and the expansion of $|+\rangle|+\rangle\dots|+\rangle$, we see that this state can also be written as

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

Then we can add another n qubits each in the $|0\rangle$ state:

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

The Quantum Part of Shor's Algorithm

We won't go into the details here, but it is possible to construct an efficient gate $F : |x\rangle |0\rangle \to |x\rangle |f(x)\rangle$. We can apply this gate to our state, then by linearity we will get

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

The Quantum Part of Shor's Algorithm

We won't go into the details here, but it is possible to construct an efficient gate $F : |x\rangle |0\rangle \to |x\rangle |f(x)\rangle$. We can apply this gate to our state, then by linearity we will get

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

Now, we measure the second qubit. We will get some random value u for $f(x)$. Then, the state becomes

$$C \sum_{x=0}^{N-1} g(x) |x\rangle |u\rangle$$

where C is the appropriate scale factor and

$$g(x) = \begin{cases} 1 & \text{if } f(x) = u \\ 0 & \text{otherwise.} \end{cases}$$

The Quantum Part of Shor's Algorithm

At this point, we will ignore the second ket. Notice that the function g has the same period as the function f. Because we want to find the period, let's try performing the quantum Fourier transform:

$$U_F(C\sum_{x=0}^{N-1} g(x)\left|x\right\rangle) = C'\sum_{c=0}^{N-1} G(c)\left|c\right\rangle,$$

where $G(c) = \sum_x g(x)\exp(\frac{2\pi icx}{N})$.

The Quantum Part of Shor's Algorithm

At this point, we will ignore the second ket. Notice that the function g has the same period as the function f. Because we want to find the period, let's try performing the quantum Fourier transform:

$$U_F(C\sum_{x=0}^{N-1} g(x)\left|x\right\rangle) = C'\sum_{c=0}^{N-1} G(c)\left|c\right\rangle,$$

where $G(c) = \sum_x g(x)\exp(\frac{2\pi icx}{N})$.Now we measure this state. As we saw earlier, we will obtain the state $\left|v\right\rangle$ corresponding to a value v which is close to a multiple of N/r. Now, we need to find r from v.

Extracting the Factor from Measurement

Shor shows that with high probability

$$\left| v - j\frac{N}{r} \right| < \frac{1}{2}.$$

Extracting the Factor from Measurement

Shor shows that with high probability

$$\left| v - j\frac{N}{r} \right| < \frac{1}{2}.$$

Recalling that $M^2 \leq N$, we have

$$\left| \frac{v}{N} - \frac{j}{r} \right| < \frac{1}{2N} \leq \frac{1}{2M^2}.$$

Extracting the Factor from Measurement

Shor shows that with high probability

$$\left| v - j\frac{N}{r} \right| < \frac{1}{2}.$$

Recalling that $M^2 \leq N$, we have

$$\left| \frac{v}{N} - \frac{j}{r} \right| < \frac{1}{2N} \leq \frac{1}{2M^2}.$$

Then, we can evaluate v/N and use the *continued fractions algorithm* to find the best fractional approximation b/c for v/N with $b, c < N$. Because any two fractions of this form differ by more than $\frac{1}{N^2} > \frac{1}{2M^2}$, the value of b/c that we find must be equal to j/r. Thus, have found r - it is just c.

Factorizing M

Now that we have r, as described earlier, we can factor M by computing $\gcd(a^{r/2}+1, M)$ and checking if this number is a nontrivial divisor of M.

The Complexity of Shor's Algorithm

The complexity one iteration of Shor's Algorithm is $O(n^2 \log n \log \log n)$. No classical factoring algorithm even comes close to this - the current best classical factoring algorithm, the general number feild sieve, runs in

$$O\left(\exp\left(((64/9)^{\frac{1}{3}} + o(1))(\ln n)^{\frac{1}{3}}(\ln \ln n)^{\frac{2}{3}}\right)\right).$$

Applications in Cryptography

The difficulty of factoring lies at the heart of many cryptographic systems, such as RSA and Diffie-Hellman. In the future, due to it's polynomial time complexity, Shor's algorithm may pose a threat to these systems. As a result, a new field, called *post quantum cryptography* is emerging. The goal of post-quantum cryptography is to develop algorithms which are safe from attacks from a quantum computer.

Further Reading

If you are interested in learning more about Shor's algorithm or quantum computing in general, consider reading some of the following:

Further Reading

If you are interested in learning more about Shor's algorithm or quantum computing in general, consider reading some of the following:

- Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer by Peter Shor

Further Reading

If you are interested in learning more about Shor's algorithm or quantum computing in general, consider reading some of the following:

- Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer by Peter Shor
- Quantum Computing a Gentle Introduction by Rieffel and Polak

Further Reading

If you are interested in learning more about Shor's algorithm or quantum computing in general, consider reading some of the following:

- Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer by Peter Shor
- Quantum Computing a Gentle Introduction by Rieffel and Polak
- My paper