Shor's Algorithm and the Period Finding Problem

Sebastian Zhu, William Yue, Vincent Fan

December 10, 2019

MIT PRIMES

Agenda

Motivation

- Modern day cryptosystems rely on problems that are *difficult to solve*.
- One common cryptosystem is RSA (Rivest-Shamir-Adleman) which relies on the difficult problem of factoring a composite number N.
- Classical algorithms can factor with runtimes of $2^{(\log N)^\alpha}$, where $\alpha \approx \frac{1}{3}$, which is exponential in the input size $\log N$.
- A quantum algorithm like Shor's Algorithm can factor a composite number N in $\approx (\log N)^2$ steps, which is polynomial in the input size $n = \log N$.

Agenda

Reduction to Period-Finding

Suppose we are trying to factor odd N which is not a prime power.

- Randomly choose $x < N$ coprime to N (Euclidean Algorithm).
- Now $x \in \mathbb{Z}_N^*$, so consider it's order r.
- In particular, this is the *period* of the sequence

$$1 = x^0 \pmod{N},\quad x^1 \pmod{N},\quad x^2 \pmod{N}, \ldots$$

Reduction to Period-Finding

Fact

With probability $\geq 1/2$, the period r is even and $x^{r/2} - 1$ and $x^{r/2} + 1$ are not multiples of N.

Pick multiple x until we get a valid r. Then,

$$x^r - 1 \equiv 0 \pmod{N} \implies (x^{r/2} - 1)(x^{r/2} + 1) \equiv 0 \pmod{N}.$$

Compute $\gcd(x^{r/2} \pm 1, N)$ for non-trivial factors of N.

The crux of this algorithm relies on being able to find the period r.

We can do this using quantum computers.

Agenda

Qubits

- Classical bit: $|0\rangle$ or $|1\rangle$.
- **Qubit** is a superposition:

$$|\phi\rangle = x_0|0\rangle + x_1|1\rangle \in \mathbb{C}^2,$$

  $x_i \in \mathbb{C}$ and $\sum |x_i|^2 = 1$.
- Multiple qubit system is **tensor product space**: two-qubit system has bases $|0\rangle \otimes |0\rangle$, $|1\rangle \otimes |0\rangle$, $|0\rangle \otimes |1\rangle$, $|1\rangle \otimes |1\rangle$. Abbreviate $|1\rangle \otimes |0\rangle$ as $|1\rangle|0\rangle$ or even $|10\rangle$ or $|2\rangle$
- n qubit system:

$$x_0|0\rangle + x_1|1\rangle + \cdots + x_{N-1}|N-1\rangle \text{ with } \sum |x_i|^2 = 1,$$

  where $N = 2^n$.

Measurement and Entanglement

We cannot see superpositions, only measure them. When you *measure* a qubit system $|\phi\rangle$, we will see a classical state $|j\rangle$, each with probability $|x_j|^2$. Then $\sum |x_j|^2 = 1$ is good.

2-qubit state **EPR Pair (Einstein, Podolsky, Rosen)**:

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle.$$

Measuring the first qubit collapses state and forces second qubit. This state is called *entangled*.

Unitary Transformations

Instead of measuring a qubit state, we can also apply transformations to send

$$\left[|\phi\rangle = \sum_{i=0}^{N-1} x_i|i\rangle\right] \mapsto \left[|\psi\rangle = \sum_{i=0}^{N-1} y_i|i\rangle\right].$$

Quantum mechanics only allows *linear* transformations, so we can view this transformation as multiplication by a unitary matrix U:

$$U \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N-1} \end{pmatrix} = \begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_{N-1} \end{pmatrix}.$$

The matrix U must be unitary to preserve the norm of 1. This process is reversable by U^{-1}, unlike measurement.

One-Qubit Quantum Gates

Call unitary matrices on qubits gates, analogous to classical AND,OR,NOT.

On one qubit, consider

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

X is a bitflip gate which switches the coefficients of $|0\rangle$ and $|1\rangle$, where Z is phaseflip which switches the sign of $|1\rangle$. Another important gate is

$$R_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix},$$

the phase gate which rotates the phase of the $|1\rangle$ state by an angle θ.

The Hadamard Transform

Hadamard gate:

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

This maps $|0\rangle$ to $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$, the state which has equal probability of observing $|0\rangle$ or $|1\rangle$. However, if we apply the Hadamard again, we get

$$H\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) = \frac{1}{\sqrt{2}}H|0\rangle + \frac{1}{\sqrt{2}}H|1\rangle = |0\rangle!$$

Here, we see an example of *interference*, as the $|1\rangle$ cancels out.

Controlled Gates

CNOT gate:

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Performs bitflip X if first qubit is $|1\rangle$, nothing if first qubit is $|0\rangle$.
Controlled-U gate:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & U_{11} & U_{12} \\ 0 & 0 & U_{21} & U_{22} \end{pmatrix}.$$

The Circuit Model

A quantum circuit generalizes the idea of classical circuits, replacing AND, OR, NOT gates with quantum linear transformation gates. We will construct a circuit for Shor's Algorithm that will allow us to find the period r.

Agenda

Fourier Transforms

(Note: here specifically $N = 2^n$ is a power of two.)
Classical (Discrete) Fourier Transform: maps vector $(x_0, x_1, \ldots, x_{N-1}) \in \mathbb{C}^N$ to $(y_0, y_1, \ldots, y_{N-1}) \in \mathbb{C}^N$ by the rule

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \omega_N^{-jk},$$

where $\omega_N = e^{\frac{2\pi i}{N}}$ is an Nth root of unity.

Quantum Fourier Transform (QFT): maps quantum state $|x\rangle = \sum_{j=0}^{N-1} x_j |j\rangle$ to the quantum state $\sum_{j=0}^{N-1} y_j |j\rangle$ by the rule

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \omega_N^{jk},$$

where $\omega_N = e^{\frac{2\pi i}{N}}$ is an Nth root of unity.

QFT

If $|x\rangle$ is a basis state, then QFT can also be expressed as

$$U_{QFT}(|x\rangle) = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \omega_N^{xj} |j\rangle .$$

Since QFT (specifically F_N) is a quantum operation expressible by the unitary matrix

$$\frac{1}{\sqrt{N}} \begin{bmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & \omega_N & \omega_N^2 & \omega_N^3 & \dots & \omega_N^{N-1} \\ 1 & \omega_N^2 & \omega_N^4 & \omega_N^6 & \dots & \omega_N^{2(N-1)} \\ 1 & \omega_N^3 & \omega_N^6 & \omega_N^9 & \dots & \omega_N^{3(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_N^{N-1} & \omega_N^{2(N-1)} & \omega_N^{3(N-1)} & \dots & \omega_N^{(N-1)(N-1)} \end{bmatrix},$$

it can also be viewed as a quantum gate.

QFT Circuit Implementation

Can put QFT in a form that is implementable by a quantum circuit:

$$\begin{aligned}
U_{QFT}(|x\rangle) &= \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i j x/2^n} |j\rangle \\
&= \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i (\sum_{\ell=1}^{n} j_\ell 2^{-\ell}) x} |j_1 j_2 \ldots j_n\rangle \\
&= \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \prod_{\ell=1}^{n} e^{2\pi i j_\ell x/2^\ell} |j_1 j_2 \ldots j_n\rangle \\
&= \bigotimes_{\ell=1}^{n} \frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i x/2^\ell} |1\rangle \right).
\end{aligned}$$

Agenda

The Period-Finding Problem

Recall that we are trying to solve the following problem to break RSA:

Problem

Given some function $f : \mathbb{N} \to \{0, 1, \ldots, N-1\}$ with period r ($f(a) = f(b)$ if $a \equiv b \pmod{r}$), find r.

- Suppose we are given a machine (a unitary matrix) that maps $|a\rangle|0^n\rangle \mapsto |a\rangle|f(a)\rangle$.
- Idea is to pick $2^\ell = q \in (N^2, 2N^2]$ and evaluate $f(0), f(1), \ldots, f(q-1)$.
- Now use QFT to separate the frequencies and determine the period.

Overview of Circuit

1. We begin with a register of $(\ell + n)$ $|0\rangle$s
2. Apply QFT to the first ℓ
3. Apply the previously mentioned unitary matrix to all qubits
4. Make an observation of the last n qubits
5. Apply a QFT to the first ℓ qubits again, and then make a measurement.

First Two Steps

- The first QFT is applied to $|0^\ell\rangle|0^n\rangle$ yields the superposition $\frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}|a\rangle|0^n\rangle$
- Applying the unitary matrix on $\frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}|a\rangle|0^n\rangle$ yields the superposition $\frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}|a\rangle|f(a)\rangle$

First Observation

- We make an observation of the second register, yielding some value $f(s)$ with $s < r$.
- Thus, the superposition in the first register collapses to only those values that also map to $f(s)$. (Entanglement!)
- Let m be the number of elements in this new superposition of the first register
- The second register has just collapsed to $|f(s)\rangle$. We ignore it from now on.
- In the first we have: $\frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} |jr + s\rangle$.

Second QFT

- Apply another QFT to the first register, yielding $\frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} \frac{1}{\sqrt{q}} \sum_{b=0}^{q-1} e^{2\pi i \frac{(jr+s)b}{q}} |b\rangle$ which we rearrange into: $\frac{1}{\sqrt{mq}} \sum_{b=0}^{q-1} e^{2\pi i \frac{sb}{q}} (\sum_{j=0}^{m-1} (e^{2\pi i \frac{rb}{q}})^j)|b\rangle$
- Using the fact that $\sum_{j=0}^{m-1} z^j = \frac{1-z^m}{1-z}$ for $z \neq 1$, the term $\sum_{j=0}^{m-1} (e^{2\pi i \frac{rb}{q}})^j = m$ or $\frac{1-e^{2\pi i \frac{mrb}{q}}}{1-e^{2\pi i \frac{rb}{q}}}$.
- We will observe this superposition, and will probabilistically get values of b whose squared amplitude is large.

The Easy Case

- $r | q$ and $m = \frac{q}{r}$.
- We observe that $e^{\frac{2\pi irb}{q}} = 1$ iff $\frac{rb}{q}$ iff b is a multiple of q/r
- Such b will have squared amplitude equal to $(\frac{m}{\sqrt{mq}})^2 = \frac{m}{q} = \frac{1}{r}$ and there are r such b, so they account for the amplitude.
- In this final superposition, we are left with only integer multiples multiples of $\frac{q}{r}$ or in other words, we get b such that $\frac{b}{q} = \frac{c}{r}$ for some c.
- With $O(\log \log N)$ repititions of this procedure, we can recover the value of r.

- Using the fact that $|1 - e^{i\theta}| = 2|\sin\frac{\theta}{2}|$ we can rewrite the absolute value of the earlier fraction as $\frac{|\sin \pi mrb/q)|}{|\sin \pi rb/q)|}$
- This ratio is large for b that are close to integer multiples of $\frac{q}{r}$
- Thus, with high probablity, a measurement of this superposition yields b that satisfies $|\frac{b}{q} - \frac{c}{r}| \leq \frac{1}{2q}$
- It's easy to recover the exact value of $\frac{c}{r}$ now, and we recover r just as we did in the easy case.

Limitations and Conclusion

- Need to build a new circuit for every number you want to factor, as well as every random choice of a.
- Still use classical computation for beginning and ending, QC is only applicable for period finding problem
- Take advantage of the superposition of things in a period, and apply QFT.
- Entanglement of the above states is the key to the success of this algorithm.

Acknowledgments

We would like to thank

- MIT PRIMES
- Our Mentor, Chun Hong Lo
- Our Parents

Reference

We consulted **Quantum Computing: Lecture Notes** by Ronald de Wolf, QuSoft, CWI and University of Amsterdam