Shor's Algorithm and Its Impact on Modern Cryptography

Alexandra Veliche - veliche.a@husky.neu.edu

Northeastern University, Boston, MA

NCUWM

Objectives

- To gain an intuitive understanding of how the quantum Fourier transform and Shor's algorithm work by visualizing the role of the roots of unity involved.
- To understand the impact of Shor's algorithm on the RSA cryptosystem, and thereby understand the importance of quantum computing in relation to modern cryptography.

Introduction

The factoring problem is formalized in the following manner: given a composite odd integer N, find its prime factorization $N = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_n^{\alpha_n}$. Since the number of operations required to find factors increases exponentially relative to the size of N, this is an infeasible problem. The fastest classical algorithm to date is the General Number Field Sieve (GNFS) algorithm, which has an asymptotic running time of $O(e^{c(logn)1/3(loglogn)2/3})$ in terms of the length n of N. Because it is widely believed that $P \neq NP$, it is thought that no polynomial-time classical factoring algorithm exists. In quantum computing, however, this is possible: in 1995, Peter Shor formulated a quantum algorithm for factoring. One of the most commonly-used cryptosystems is RSA, which relies on the infeasibility of the factoring problem. In particular, the encryption and decryption function are defined modulo N, where N is of the form $N = p \cdot q$, for large primes $p, q \in \mathbb{Z}_+$. Because this cryptosystem plays a major role in the secure transmission of data, the potential ability to quickly factor N poses a threat. According to the National Institute of Standards and Technology (NIST), quantum computers will bring an end to modern cryptography as we know it.

Quantum Computing Basics

Qubits - quantum bits, can be in any linear combination, or *superposition*, of the basis states $|0\rangle$ and $|1\rangle$: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $\alpha, \beta \in \mathbb{C}$ with normalization condition $|\alpha|^2 + |\beta|^2 = 1$.

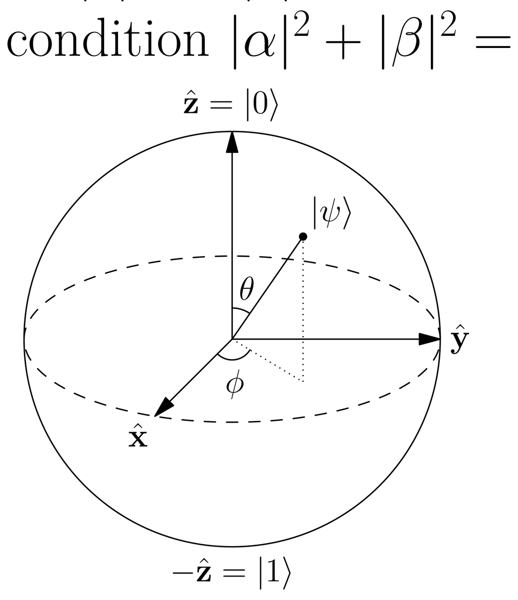

Figure 1:Bloch sphere

Quantum logic gates used in QFT:

Hadamard gate: $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.

Controlled-phase gate: $R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{bmatrix}$

Shor's Algorithm

I. Reduction of factoring to order-finding algorithm:
Input: odd composite $N \in \mathbb{Z}_+$
Output: non-trivial factors of N

1. Choose a random $a \in \mathbb{Z}_+$, $a < N$.
2. Compute $gcd(a, N)$ using Euclidean Algorithm.
3. If $gcd(a, N) \neq 1$, return $gcd(a, N)$.
   Else, use subroutine (II) to find the order r, $a^r \equiv 1 \ mod \ N$.
4. If r odd or $a^{\frac{r}{2}} \equiv -1 \ (mod \ N)$, return to (1.).
   Else, return $gcd(a^{\frac{r}{2}} + 1, N)$ and/or $gcd(a^{\frac{r}{2}} - 1, N)$.

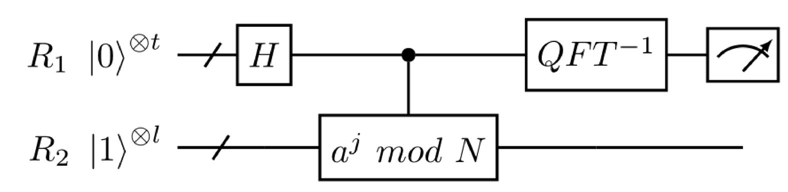

Figure 2:Quantum Subroutine Circuit

II. Quantum subroutine for order-finding:
Inputs:

(i) black box transformation
$U_{a,N} : |j\rangle|k\rangle \rightarrow |j\rangle|a^j k \ (mod \ N)\rangle$ for $a \in \mathbb{Z}_+$

(ii) t qubits intialized to $|0\rangle$, where
$t := 2l + 1 + \lceil log(2 + \frac{1}{2\epsilon})\rceil$ and $l := |N|$

(iii) l qubits intialized to $|1\rangle$

Output: order of a modulo N

1. Apply the Hadamard gate to each qubit in R_1:
   $$H^{\otimes t}(|0\rangle^{\otimes t}) = (\tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle))^{\otimes t} = \tfrac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle.$$
2. Apply $U_{a,N}$ to each qubit in R_2:
   $$\begin{aligned} U_{a,N}(\tfrac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle|1\rangle) &= \tfrac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle|a^j mod \ N\rangle \\ &= \tfrac{1}{\sqrt{r2^t}}\sum_{s=0}^{r-1}\sum_{j=0}^{2^t-1}e^{\frac{2\pi ijs}{r}}|j\rangle|u_s\rangle \\ &=: |\psi\rangle \end{aligned}$$
   where $|u_s\rangle = \frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}e^{\frac{-2\pi ijs}{r}}|a^j mod \ N\rangle$ an eigenstate of U defined by $U|x\rangle = |ax \ mod \ N\rangle$.
3. Apply inverse QFT to R_1:
   $$\begin{aligned} \mathrm{QFT}^{-1}(|\psi\rangle) &= \tfrac{1}{\sqrt{r2^t}}\sum_{s=0}^{r-1}\sum_{j=0}^{2^t-1}e^{\frac{2\pi ijs}{r}} \\ &\quad (\tfrac{1}{\sqrt{2^t}}\sum_{k=0}^{2^t-1}e^{\frac{-2\pi ijk}{2^t}}|k\rangle)|u_s\rangle \\ &= \tfrac{1}{\sqrt{r}}\sum_{s=0}^{r-1}\sum_{k=0}^{2^t-1}\alpha_{k,s}|k\rangle|u_s\rangle \end{aligned}$$
4. Measure R_2 to choose an s, then measure R_1 to obtain a value $\tilde{k}$ for this s.
5. Apply continued fractions algorithm to $\frac{\tilde{k}}{2^t}$ to find partial denominators $r_0, r_1, ...r_l$, and test r_i at each step to find the order r.

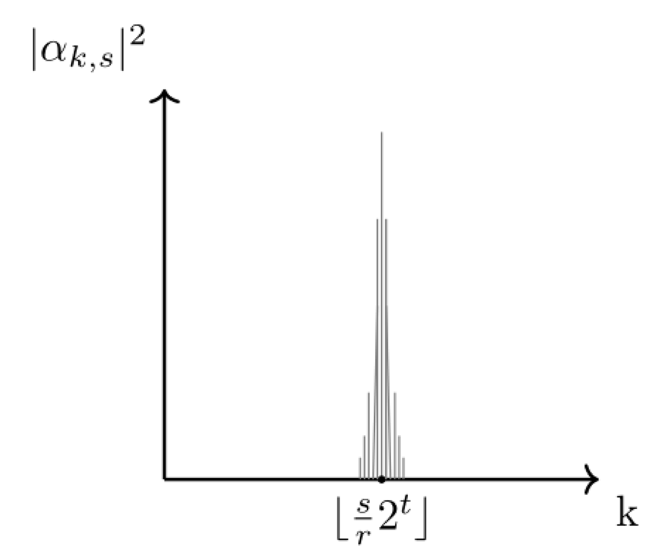

Figure 3:Probability Distribution for R_1 Given R_2

Quantum Fourier Transform

An n-qubit system has basis states $|0\rangle, ...|2^n - 1\rangle$. A state $|j\rangle$ can be written in binary form $|j\rangle = j_1 \cdot 2^{n-1} + j_2 \cdot 2^{n-2} + ... + j_n \cdot 2^0 = |j_1 j_2 ... j_n\rangle$. The QFT acts on an input state $|\psi\rangle$ by transforming each basis state $|j\rangle$ by the following:

$$\begin{aligned} |j\rangle \rightarrow & \tfrac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1}e^{\frac{2\pi ijk}{2^n}}|k\rangle \\ &= \tfrac{1}{\sqrt{2^n}}(|0\rangle + e^{2\pi i0.j_n}|1\rangle)(|0\rangle + e^{2\pi i0.j_{n-1}j_n}|1\rangle)... \\ &\quad ...(|0\rangle + e^{2\pi i0.j_1j_2...j_n}|1\rangle). \end{aligned}$$

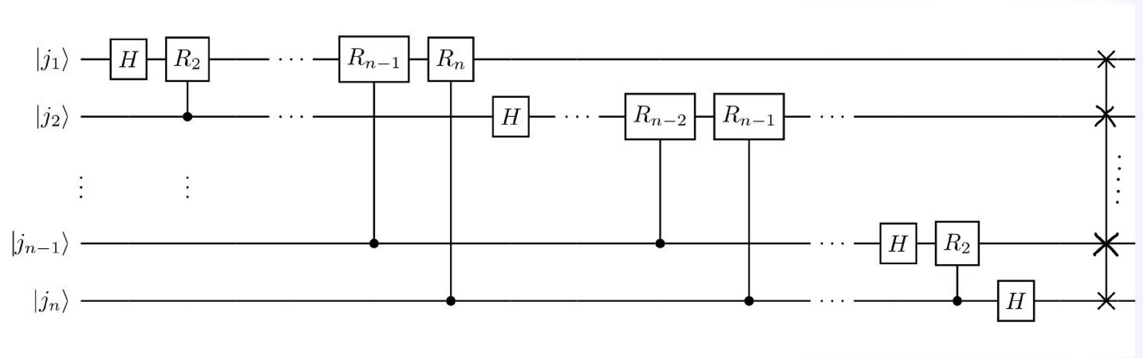

Figure 4:QFT Circuit Representation

Roots of Unity

Let $b + \delta := \frac{s2^t}{r} - k$, where $b = \lfloor \frac{s2^t}{r} - k \rfloor$, and $\omega := e^{\frac{2\pi i}{2^t}}$. Then the amplitude in step II, 3. can be rewritten as

$$\alpha_{k,s} = \frac{1}{2^t}\sum_{j=0}^{2^t-1}\omega^{j(b+\delta)}.$$

Black roots correspond to $b \geq 1$ and $\delta = 0$, shifted by a factor of ω^b for $b > 1$. Grey roots correspond to error produced by $\delta \neq 0$, with shifting amount relative to exponent of ω^j. For $\delta = 0$, the total sum is $\alpha_{k,s} = 1$ resulting in no error, but is inexact otherwise.

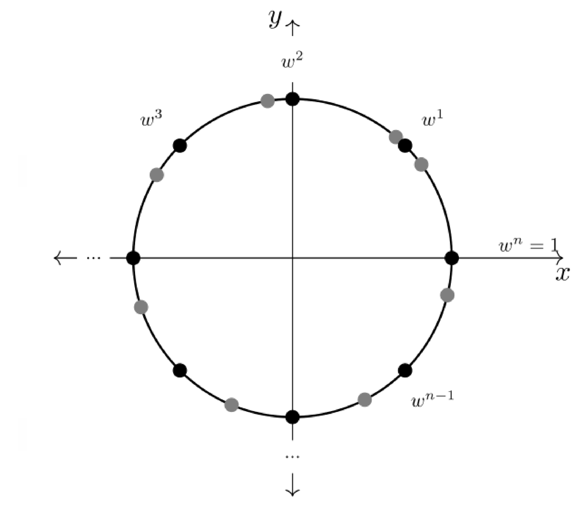

Figure 5:Roots of Unity for Quantum Subroutine

Acknowledgements

Advisor and Faculty consultant: Professor Christopher King
Research Capstone Instructor: Professor Anthony Iarrobino

References

- Nielsen, M.A. and Chuang I.L., *Quantum Computation and Quantum Information*, 2000
- Shor, Peter W., *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, 1995
- Weisstein, Eric W., *Number Field Sieve*, Wolfram MathWorld
- Rupert, Steven, et al., *Shor's Algorithm Simulator*, Colorado School of Mines, 2011