Shor's Algorithm: Exponentially Speeding Up Factorization

Rohan Biswas
Dept. of Computer Science and Engineering
Tezpur University, India

January 27, 2024

Abstract

Shor's Algorithm is a groundbreaking quantum algorithm that demonstrates exponential speedup over classical algorithms for integer factorization. This paper provides an overview of the algorithm, its theoretical foundations, and potential implications for modern cryptography. We explore the mathematical principles behind Shor's Algorithm and discuss its significance in the context of quantum computing advancements.

1 Introduction

Quantum computing has emerged as a revolutionary paradigm with the potential to solve certain problems exponentially faster than classical computers. Given an integer N , Classical factorization algorithms , such as the Number Field Sieve has a complexity of:

$$O(exp[(logN)^{1/3}(loglogN)^{2/3}]) \tag{1}$$

Shor's quantum factorization has a time complexity of :

$$O((logN)^2(loglogN)(logloglogN)) \tag{2}$$

Shor's Algorithm exhibits exponential speedup, threatening the security of widely used cryptographic schemes based on the difficulty of integer factorization.
In this paper, we delve into the fundamental concepts of Shor's Algorithm, elucidate its quantum mechanical underpinnings, and discuss its practical implications. The objective is to provide a comprehensive understanding of how Shor's Algorithm exploits quantum parallelism and Fourier transform to achieve exponential speedup in the factorization process.

2 Theoretical Foundations

Lets take a look at the things we got to know prior to diving deep into the algorithm.

2.1 Factoring Problem

The factoring problem is a fundamental mathematical task that involves decomposing a composite number into a product of its prime factors. Given an integer N, the factoring problem seeks to find two non-trivial integers, usually prime numbers, whose product equals N.

So basically, we want to write N , and we want to write it as product of : $P_1^{e_1}, P_2^{e_2}, ..., P_k^{e_k}$ where , $P_i^{e_i}$ are primes that divide N.

Most difficult case is when : $N = P * Q$ where, P and Q are two distinct primes .

The factoring problem is of particular significance in the field of number theory and has practical applications in cryptography. Public-key cryptographic systems, such as the widely used RSA algorithm, rely on the presumed difficulty of factoring large numbers to ensure the security of encrypted communications.

2.2 Basics of Modular arithmetic used here

We want to factor : N.
We know , $a \equiv b(mod N)$. This gives : $b = qN + a$, where , q is quotient , and a is remainder.

Let us consider an example with : $N = 21$ as the value we want to factor.
Solve $x^2 \equiv 1(mod\ 21)$. Basically we are looking for a number$x$ such that when a multiple of N is subtracted from x^2 , yields 1.
One such number , lets say is 8. So,

$$8^2 \equiv 1(mod\ 21)$$

$$8^2 - 1^2 \equiv 0(mod\ 21)$$

So, 21 divides $(8-1)(8+1)$. But what are the factors ?
This can be found using gcd : $gcd(21, 8+1) = 3$, and $gcd(21, 8-1) = 7$ so the factors are 3 and 7 .

Thus, our problem arises when the value x such that $x \not\equiv \pm 1(mod\ N)$ but $x^2 \equiv \pm 1(mod\ N)$, in a way that N divides $(x+1)(x-1)$.
But, since $x \mp 1 \not\equiv 0(mod\ N)$ so N does not divide $(x \pm 1)$. And hence :
$gcd(N, x+1) \neq gcd(N, x-1)$...

2.3 Quantum Fourier Transform

Quantum Fourier Transform is exactly same as the discrete fourier transform, except for the fact that the notations are somewhat different. Quantum Fourier Transform (QFT) on an orthonormal basis $|0\rangle, ..., |N-1\rangle$ is defined to be linear operator with the following action on the basis states,

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{2\pi i \phi x} |x\rangle \tag{3}$$

Here, N is the size of the quantum system(also can be given by 2^n where n is the number of qubits), $|x\rangle$ represents the basis states, and ϕ is the phase that determines the periodicity.

The Quantum Fourier Transform operation on $|\psi\rangle$ is defined as:

$$QFT|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \sum_{x=0}^{N-1} e^{2\pi i x y/N} |\psi_x\rangle \tag{4}$$

Where $|\psi_x\rangle$ is the state obtained by applying the phase shift $e^{2\pi i \phi x}$ to each basis state $|x\rangle$ in $|\psi\rangle$.

The QFT operation is implemented using quantum gates. For n-qubit quantum systems, the QFT circuit can be represented as:

$$QFT_n = H^{\otimes n} \cdot R_{2\pi}^{(n-1)} \cdot \ldots \cdot R_{2\pi}^{(1)} \tag{5}$$

Here, H is the Hadamard gate, and $R_{2\pi}^{(k)}$ represents a controlled rotation gate.

Algorithm 1 Quantum Fourier Transform (QFT)

procedure QFT(n)
    Create a quantum circuit with n qubits
    for q in range n **do**
        Apply Hadamard gate on qubit q
        for t in range $(q+1, n)$ **do**
            Apply controlled phase gate with angle $\frac{\pi}{2^{(t-q)}}$ from qubit q to target qubit t
        end for
    end for
    Swap the qubits (reverse their order)
end procedure

The circuit for the Quantum Fourier Transform is :

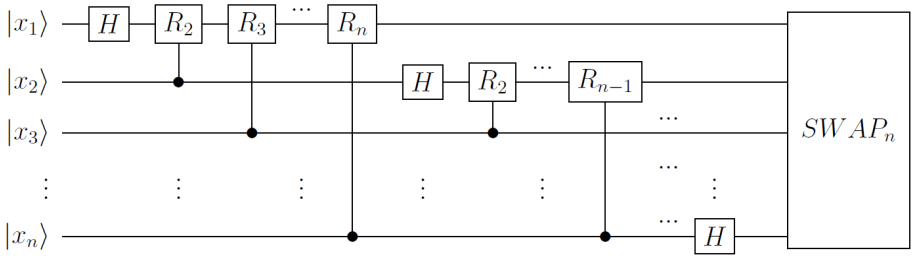

Figure 1: Quantum Fourier Transform

3 Shor's Factoring Algorithm

The lemma that we have with us is :
Let N be an odd composite number, with atleast two distinct prime factors, and let x be another uniformly random number between 0 and $N-1$. If $gcd(x,N)=1$ then with probability of atleast $\frac{1}{2}$, order r of $x(mod\ N)$ is even , and $x^{r/2}$ is a non- trivial square root of $1(modN)$.
So, if N divides $(x^{r/2}-1)(x^{r/2}+1)$ then $gcd(N,x^{r/2}-1)$ and $gcd(N,x^{r/2}+1)$ gives us the factors.

The Algorithm is as follows :

Algorithm 2 Shor's Algorithm

```
procedure SHOR(N)
    Choose a random integer a such that 1 < a < N
    Use a quantum computer to find the period r of a^x mod N (r is the
smallest positive integer such that a^r ≡ 1 mod N)
    if r is even and a^{r/2} ≢ −1 mod N then
        The factors of N are gcd(a^{r/2} + 1, N) and gcd(a^{r/2} − 1, N)
    else
        Choose a different random a and repeat the algorithm
    end if
end procedure
```

The process of finding the period r of $f_{a,N}=a^x mod\ N$ is :

1. Prepare two L-bit quantum register in initial state.

$$\left(\frac{1}{\sqrt{2^L}}\sum_{x=0}^{2^L-1}|x\rangle\right)|0\rangle \tag{6}$$

where , $N^2 \leq 2^L < 2N^2$

2. Apply $U_f : |x\rangle|0\rangle \rightarrow |x\rangle|f_{a.N}(x)\rangle$:

$$\frac{1}{\sqrt{2^L}} \sum_{x=0}^{2^L-1} |x\rangle|0\rangle \rightarrow \frac{1}{\sqrt{2^L}} \sum_{x=0}^{2^L-1} |x\rangle|f_{a.N}\rangle \tag{7}$$

3.Apply QFT to the first register :

$$\frac{1}{\sqrt{2^L}} \sum_{x=0}^{2^L-1} |x\rangle|f_{a.N}\rangle \rightarrow \frac{1}{\sqrt{2^L}} \sum_{y=0}^{2^L-1} \left(\sum_{x=0}^{2^L-1} e^{2\pi i x y/2^L} |y\rangle \right) |f_{a.N}\rangle \tag{8}$$

4. Make measurement on the register, obtaining y.
5. Find r from y via continued fraction for $y/2^L$. If it fails in some case, repeat (1).

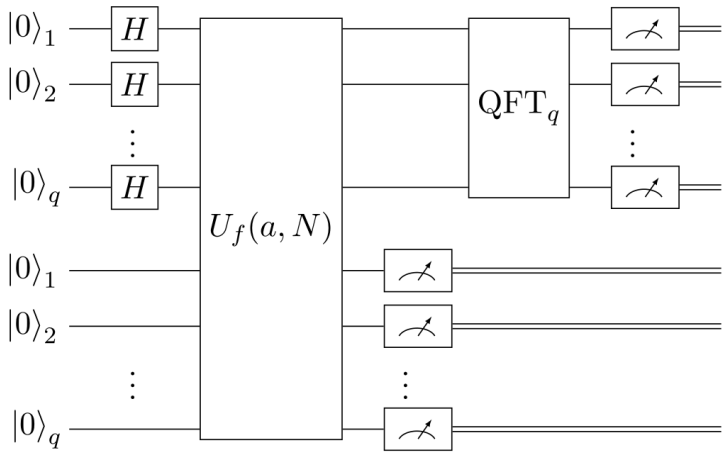

Figure 2: Shor's Algorithm

4 Applications and Implications

Shor's Algorithm, a groundbreaking quantum algorithm, has profound applications and implications across multiple domains. In this section, we delve into some of the key areas where Shor's Algorithm is expected to have a significant impact.

4.1 Cryptography, Security and Encryption

One of the most noteworthy applications of Shor's Algorithm is in the field of cryptography, Security and Encryption. Researchers are actively exploring post-quantum cryptography to develop encryption schemes that resist the quantum

threat. The algorithm efficiently factors large composite numbers into their prime factors, posing a threat to widely used public-key cryptographic systems such as RSA.

4.2 Optimization Problems

Quantum computers, including those employing Shor's Algorithm, have the potential to address complex optimization problems more efficiently than classical computers. Quantum parallelism allows simultaneous evaluation of multiple possibilities. In certain optimization problems, quantum speedup is captured by the formula:

$$\text{Quantum Speedup} = \frac{\text{Number of possibilities classically}}{\text{Square root of the number of possibilities quantumly}}$$

Also, the graph below shows the speedup achieved using Shor's algorithm vs the classical Number Field Sieve Method:

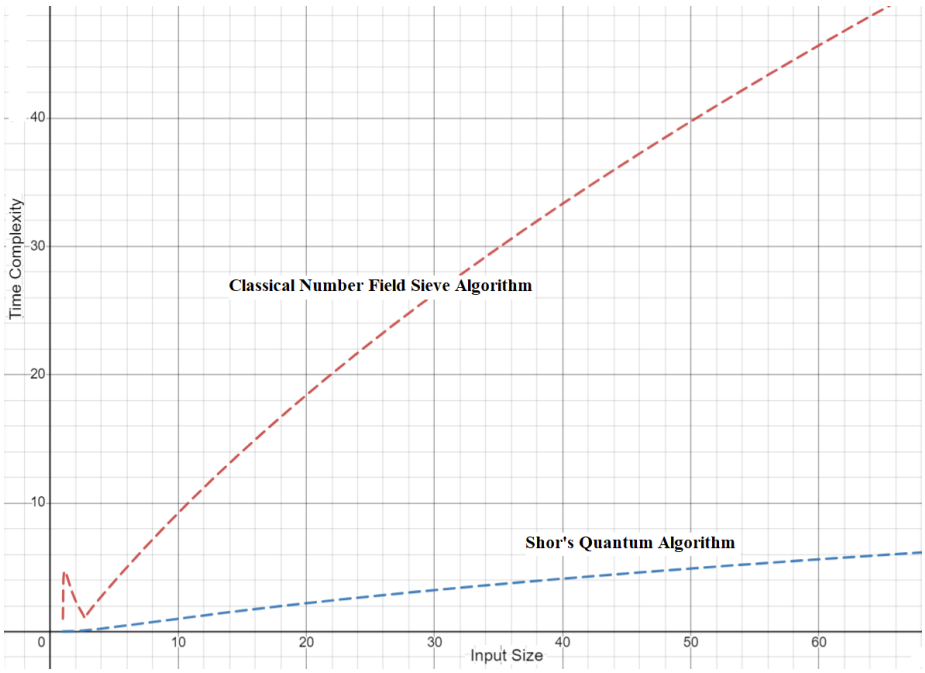

Figure 3: Speedup with Shor's Algorithm

4.3 Drug Discovery and Molecular Modeling

Shor's Algorithm, along with other quantum algorithms, holds promise in the field of quantum chemistry. Quantum computers can simulate molecular struc-

tures and interactions more accurately than classical computers.

4.4 Machine Learning

The quantum parallelism in quantum algorithms, including Shor's Algorithm, may find applications in machine learning. Quantum computing may provide speedups in certain machine learning tasks, with the quantum version of the support vector machine (QSVM) being an example.

5 Conclusion

In conclusion, Shor's Algorithm is a transformative quantum algorithm with widespread implications, ranging from the security landscape to optimizations and various applications in computational science.

6 References

6.1 Quantum Computation and Quantum Information

- **Authors:** Michael A. Nielsen and Issac L. Chuang
- **Edition:** 10th Anniversary Edition
- **Year:** 2010
- **Publisher:** Cambridge University Press

6.2 Quantum Computing Devices: Principles, Designs, and Analysis

- **Authors:** Goong Chen and David A. Church and Berthold-Georg Englert and Carsten Henkel and Bernd Rohwedder and Marlan O. Scully and M. Suhail Zubairy
- **Edition:** 1st
- **Year:** 2014
- **Publisher:** Chapman and Hall/CRC