Introduction to Quantum Computing: From Fundamentals to Quantum Algorithms

Ahyan Hassan
Mentor: Divyaansh Kumar

June 27, 2025

Abstract

This report provides a comprehensive introduction to quantum computing, covering fundamental concepts like qubits, superposition, entanglement, and quantum gates. It explores key quantum algorithms including Deutsch-Jozsa, Bernstein-Vazirani, Simon's, Shor's, and Grover's algorithms, with detailed mathematical analysis and quantum circuit implementations. The report also discusses practical implementations on quantum hardware and future directions for the field.

Contents

Chapter 1

Introduction to Quantum Computing

1.1 The Quantum Revolution

Quantum computing represents a paradigm shift from classical computing by leveraging quantum mechanical phenomena. While classical computers use bits (0/1), quantum computers use **qubits** that can exist in superpositions of states:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \text{where} \quad |\alpha|^2 + |\beta|^2 = 1$$

This enables parallel computation on exponentially many states simultaneously.

1.2 Key Quantum Phenomena

1.2.1 Superposition

Qubits can exist in linear combinations of basis states. A qubit's state is represented as a unit vector in Hilbert space:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$$

which can visualized on the Bloch sphere.

1.2.2 Entanglement

When qubits become correlated such that their state cannot be described independently:

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Entanglement enables quantum parallelism and is essential for quantum speedups.

1.3 Quantum vs. Classical Computing

Feature	**Classical**	**Quantum**
Basic unit	Bit (0/1)	Qubit ($\alpha\|0\rangle + \beta\|1\rangle$)
Operations	Boolean logic	Unitary transformations
Parallelism	Limited	Exponential (superposition)
Information	Copyable	No-cloning theorem

Table 1.1: Comparison of computing paradigms

Chapter 2

Quantum Circuits and Gates

2.1 Single-Qubit Gates

2.1.1 Hadamard Gate

Creates superposition: $H|0\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$

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

2.1.2 Pauli Gates

$$X = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} \quad \text{(quantum NOT)}$$

$$Y = \begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}$$

$$Z = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$$

2.2 Multi-Qubit Gates

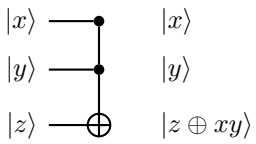
2.2.1 CNOT Gate

Entangles qubits: $CNOT|10\rangle = |11\rangle$

$$CNOT = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}$$

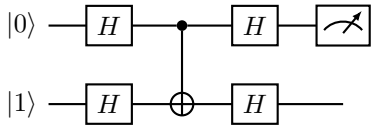
2.2.2 Toffoli Gate (CCNOT)

Three-qubit gate: $CCNOT|110\rangle = |111\rangle$



2.3 Quantum Circuit Model

Quantum algorithms are implemented as sequences of quantum gates:



Circuits must satisfy unitarity: $U^\dagger U = I$, preserving the norm.

Chapter 3

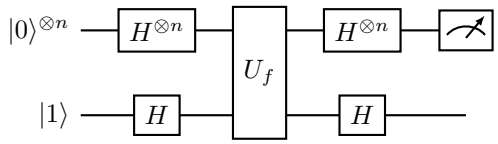
Quantum Algorithms

3.1 Deutsch-Jozsa Algorithm

3.1.1 Problem Formulation

Determine if $f : \{0,1\}^n \to \{0,1\}$ is **constant** (all outputs equal) or **balanced** (50% 0s and 1s) using minimal queries.

3.1.2 Quantum Circuit



3.1.3 Mathematical Analysis

Initial State:

$$|\psi_0\rangle = |0\rangle^{\otimes n}|1\rangle$$

After Hadamard Gates:

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \otimes \underbrace{\frac{|0\rangle - |1\rangle}{\sqrt{2}}}_{|-\rangle}$$

After Oracle U_f:

$$U_f|x\rangle|j\rangle = |x\rangle|j \oplus f(x)\rangle$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x} (-1)^{f(x)}|x\rangle \otimes |-\rangle$$

After Final Hadamards:

$$|\psi_3\rangle = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \left(\sum_{x=0}^{2^n-1} (-1)^{x\cdot y + f(x)} \right) |y\rangle \otimes |1\rangle$$

Measurement Probability:

$$P(y=0) = \left| \frac{1}{2^n} \sum_{x} (-1)^{f(x)} \right|^2 = \begin{cases} 1 & \text{if } f \text{ constant} \\ 0 & \text{if } f \text{ balanced} \end{cases}$$

3.1.4 Entanglement Analysis

States remain separable throughout:

$$|\psi_1\rangle = \left(\frac{1}{\sqrt{2^n}} \sum_{x} |x\rangle \right) \otimes |-\rangle$$

$$|\psi_2\rangle = \left(\frac{1}{\sqrt{2^n}} \sum_{x} (-1)^{f(x)}|x\rangle \right) \otimes |-\rangle$$

No entanglement is created or destroyed by U_f for this oracle.

3.1.5 Efficiency

Algorithm	Classical Queries	Quantum Queries
Deutsch-Jozsa	$\Omega(2^{n-1}+1$	1

Table 3.1: Query complexity comparison (n-bit functions)

3.2 Simon's Algorithm

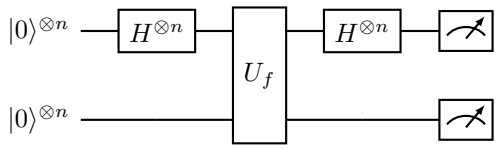
3.2.1 Problem Formulation

Find hidden string $s \neq 0$ where $f : \{0,1\}^n \to \{0,1\}^n$ satisfies:

$$f(x) = f(y) \iff y = x \oplus s$$

for all $x, y \in \{0,1\}^n$.

3.2.2 Quantum Circuit



3.2.3 Mathematical Analysis

Initial State:

$$|\psi_0\rangle = |0\rangle^{\otimes n}|0\rangle^{\otimes n}$$

After First Hadamards:

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle|0\rangle^{\otimes n}$$

After Oracle U_f:

$$U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle|f(x)\rangle$$

After Measuring Second Register (outcome z): Collapses to two preimages:

$$|\psi_3\rangle = \frac{1}{\sqrt{2}} \left(|x'\rangle + |x' \oplus s\rangle\right) \otimes |z\rangle$$

After Final Hadamards:

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_y (-1)^{x \cdot y}|y\rangle$$

$$|\psi_4\rangle = \frac{1}{\sqrt{2^{n-1}}} \sum_{\substack{y \\ y \cdot s = 0}} (-1)^{x' \cdot y}|y\rangle$$

Measurement: Outputs random y satisfying $y \cdot s = 0$ with uniform probability.

3.2.4 Classical Post-Processing

After k iterations, solve linear system over $\mathbb{Z}_2$:

$$\begin{cases} y^{(1)} \cdot s = 0 \\ \vdots \\ y^{(k)} \cdot s = 0 \end{cases}$$

Success Probability for $k = n - 1$:

$$p(n-1) = \prod_{i=0}^{n-2} \left(1 - \frac{2^i}{2^n}\right) > \frac{1}{2} + \frac{1}{2^n}$$

3.2.5 Entanglement Analysis

The state after measurement:

$$|\psi_3\rangle = \frac{|x'\rangle + |x' \oplus s\rangle}{\sqrt{2}} \otimes |z\rangle$$

is maximally entangled when HammingWeight$(s) = n$:

$$\text{GHZ State: } \frac{|0\rangle^{\otimes n} + |1\rangle^{\otimes n}}{\sqrt{2}}$$

3.2.6 Efficiency

Algorithm	Classical Queries	Quantum Queries
Simon's	$\Omega(\sqrt{2^n})$	$\mathcal{O}(n)$

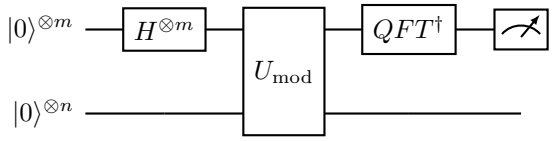
Table 3.2: Query complexity comparison (n-bit hidden string)

3.3 Shor's Factoring Algorithm

3.3.1 Key Insight

Factoring reduces to finding period of $f(x) = a^x \mod N$.

3.3.2 Quantum Circuit



where $m = 2\lceil \log_2 N \rceil$, $n = \lceil \log_2 N \rceil$.

3.3.3 Complexity

Runs in $O((\log N)^3)$ time vs. classical sub-exponential time.

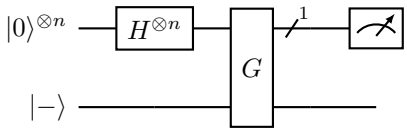
Will dive deeper in this algorithm after mid-term

3.4 Grover's Search Algorithm

3.4.1 Problem

Find x such that $f(x) = 1$ in unstructured database of size N.

3.4.2 Circuit



where G is the Grover iterate.

3.4.3 Analysis

Amplifies solution probability with $O(\sqrt{N})$ queries vs. classical $O(N)$.

Will dive deeper in this algorithm after mid-term

Chapter 4

Implementation and Applications

4.1 Quantum Hardware

- **Superconducting qubits** (IBM, Google): Microwave circuits
- **Trapped ions** (IonQ): Atomic qubits manipulated by lasers
- **Topological qubits** (Microsoft): Protected quantum states

4.2 IBM Quantum Experience

Implementation of Deutsch-Jozsa algorithm:

Results show probability distribution confirming constant/balanced function.

4.3 Applications

- Cryptanalysis (RSA, ECC)
- Quantum simulation (materials, chemistry)
- Optimization problems
- Machine learning acceleration

Conclusion

Quantum computing leverages quantum mechanics to solve problems intractable for classical computers. While current devices face challenges in error correction and qubit coherence, rapid advancements suggest practical quantum advantage is imminent. Key algorithms like Shor's and Grover's demonstrate exponential and quadratic speedups respectively. As hardware matures, quantum computing will revolutionize fields from cryptography to drug discovery.

Bibliography

[1] Nielsen, M. A., & Chuang, I. L. (2010). *Quantum Computation and Quantum Information*. Cambridge University Press. (10th Anniversary Edition)

[2] Sakurai, J. J., & Napolitano, J. (2017). *Modern Quantum Mechanics*. Cambridge University Press. (2nd Edition)

[3] Portugal, R. (2023). *Basic Quantum Algorithms*. Springer Nature.