Quantum Computation and Quantum Information

Dhanush Sanjay Nidamanuri

July 2025

Abstract

This report provides my detailed study of the first three chapters of Nielsen and Chuang's *Quantum Computation and Quantum Information* [1]. I explored the historical background, conceptual foundations, and mathematical formalism of quantum mechanics and computer science that underlie the field of Quantum Computing.

Contents

Chapter 1

Introduction and Overview

1.1 Global Perspectives

Quantum computation and quantum information unite physics, computer science, and information theory. The fundamental idea is to exploit quantum mechanical systems for information processing tasks.

1.1.1 History of Quantum Computation and Information

- **Early Quantum Mechanics:** Crisis in classical physics (ultraviolet catastrophe, electron instability) led to quantum mechanics.
- **Computation Theory:** Turing (1936) introduced the universal Turing machine. Church–Turing thesis equated computability with Turing-computable functions.
- **Information Theory:** Shannon (1948) introduced entropy and channel capacity.
- **Cryptography:** Development of public-key cryptography motivated interest in factoring and discrete logarithms.

1.2 Quantum Bits

A qubit is a two-level system:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \alpha, \beta \in \mathbb{C},\ |\alpha|^2 + |\beta|^2 = 1. \tag{1.1}$$

Multiple qubits live in tensor product Hilbert spaces, leading to entangled states such as Bell states:

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \tag{1.2}$$

1.3 Quantum Computation

1.3.1 Single Qubit Gates

Unitary gates manipulate qubits. Examples:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \qquad H = \tfrac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{1.3}$$

1.3.2 Multi-Qubit Gates

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{1.4}$$

1.3.3 Teleportation Protocol

1. Alice and Bob share $|\Phi^+\rangle$.
2. Alice entangles unknown state $|\psi\rangle$ with her half.
3. Alice measures and sends 2 classical bits.
4. Bob applies $X^a Z^b$ to recover $|\psi\rangle$.

1.3.4 Deutsch's Algorithm

The simplest quantum algorithm, proposed by David Deutsch (1985), illustrates the concept of **quantum parallelism**.

Problem Statement: We are given a Boolean function $f : \{0,1\} \to \{0,1\}$. The task is to determine whether f is

- *constant*: $f(0) = f(1)$, or
- *balanced*: $f(0) \neq f(1)$.

Classical Complexity: A deterministic classical algorithm must query both $f(0)$ and $f(1)$, requiring two evaluations.
Quantum Approach: Define the oracle U_f acting as

$$U_f|x, y\rangle = |x, y \oplus f(x)\rangle, \tag{1.5}$$

where $\oplus$ denotes XOR. Start with $|0\rangle|1\rangle$, apply Hadamards, then U_f, then another Hadamard.

The state evolves as:

$$|0\rangle|1\rangle \xrightarrow{H\otimes H} \tfrac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) \tag{1.6}$$

$$\xrightarrow{U_f} \tfrac{1}{2}\big((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\big)(|0\rangle - |1\rangle). \tag{1.7}$$

Measuring the first qubit after another Hadamard gives:

- Result $|0\rangle$ if f is constant,
- Result $|1\rangle$ if f is balanced.

Thus the algorithm solves the problem with a **single query**.

—

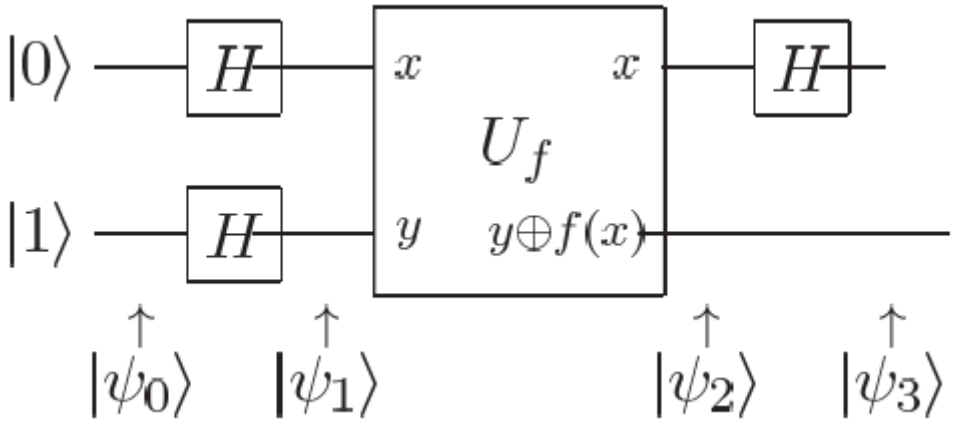

Figure 1.1: Quantum circuit for Deutsch's algorithm.

1.3.5 Deutsch–Jozsa Algorithm

Generalized by Deutsch and Jozsa (1992), this algorithm distinguishes between constant and balanced functions $f : \{0,1\}^n \to \{0,1\}$.
Problem Statement: Given either $f(x) = 0$ for all x, or exactly half the inputs give $f(x) = 0$ and the other half give $f(x) = 1$.
Classical Complexity: Any deterministic classical algorithm requires $2^{n-1} + 1$ evaluations in the worst case.
Quantum Approach: Initialize $|0\rangle^{\otimes n}|1\rangle$, apply Hadamards, then the oracle:

$$U_f|x, y\rangle = |x, y \oplus f(x)\rangle. \tag{1.8}$$

This introduces a phase factor:

$$\frac{1}{\sqrt{2^n}} \sum_x (-1)^{f(x)}|x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{1.9}$$

After Hadamards on the first n qubits, measure:

- Output $|0^n\rangle$ if f is constant.
- Any other outcome (probability 1) if f is balanced.

Result: The Deutsch–Jozsa algorithm solves the promise problem with certainty in a single quantum query, while classical deterministic algorithms require $2^{n-1} + 1$ queries.

1.4 Experimental Realizations and Quantum Information

- The Stern-Gerlach experiment is discussed as foundational experimental evidence for the existence of two-level quantum systems (spin-1/2), which can serve as physical implementations of qubits.
- The chapter acknowledges the immense experimental challenges in building a scalable quantum computer, such as maintaining coherence and controlling quantum systems with high precision.

- It introduces the core goals of **quantum information theory**: identifying quantum resources (like entanglement), understanding quantum processes (like communication and computation), and quantifying the fundamental trade-offs between them.

Key challenges:

1. **Scalability:** Current devices handle only a few qubits reliably.
2. **Decoherence:** Interaction with environment destroys quantum coherence.
3. **Error Correction:** Fault-tolerant methods are required to scale to useful computations.

Despite difficulties, experimental progress continues rapidly. Deutsch–Jozsa has been realized with trapped ions, superconducting qubits, and linear optics, serving as benchmarks for emerging quantum technologies.

1.5 Conclusion

The conceptual framework of quantum information and quantum computation is effectively laid out in Chapter 1. It identifies the quantum circuit as the computational model, the qubit as the basic building block of information, and quantum algorithms as the source of possible computational advantage. It skilfully combines elements of information theory, computer science, and physics to provide a cohesive and captivating introduction to this ground-breaking field.

Chapter 2

Introduction to Quantum Mechanics

2.1 Introduction

Chapter 2 of Nielsen and Chuang marks a shift from the broad overview in Chapter 1 to a more detailed and rigorous exploration of quantum mechanics. As I went through this chapter, I realized it forms the foundation for understanding quantum computation and information. It carefully introduces the mathematical formalism and physical principles that allow us to describe quantum systems precisely. Reading it gave me a much clearer sense of how the abstract concepts from Chapter 1 are formalized, and it really helped me grasp the rules and tools needed to work with quantum states, operators, and measurements. In this report, I will summarize the aspects of Chapter 2 that I found most essential and illuminating.

2.2 Linear Algebra: The Language of Quantum Mechanics

Quantum mechanics is formulated in the mathematical language of linear algebra over complex vector spaces. This section reviews the core concepts and introduces the standard notation used in the field.

2.2.1 Hilbert Spaces and Dirac Notation

The arena for quantum mechanics is a **Hilbert space**, which for our purposes is a complex vector space equipped with an inner product. The state of a quantum system is represented by a vector in this space.

- **Kets:** A column vector is denoted by a "ket", $|\psi\rangle$. For a d-dimensional space $\mathbb{C}^d$, this is a $d \times 1$ matrix of complex numbers.
- **Bras:** The Hermitian conjugate (conjugate transpose) of a ket is a "bra", $\langle\psi| = (|\psi\rangle)^\dagger$. This is a $1 \times d$ row vector.
- **Inner Product:** The inner product between two states $|\phi\rangle$ and $|\psi\rangle$ is written as $\langle\phi|\psi\rangle$. It is a complex number satisfying:
  1. $\langle\phi|\psi\rangle = (\langle\psi|\phi\rangle)^*$

2. Linearity in the second argument: $\langle\phi|a\psi_1 + b\psi_2\rangle = a\langle\phi|\psi_1\rangle + b\langle\phi|\psi_2\rangle$
3. $\langle\psi|\psi\rangle \geq 0$, with equality if and only if $|\psi\rangle$ is the zero vector. The norm of a vector is $\| |\psi\rangle \| = \sqrt{\langle\psi|\psi\rangle}$.

- **Orthonormal Basis:** A set of vectors $\{|i\rangle\}$ is an orthonormal basis if $\langle i|j\rangle = \delta_{ij}$. Any vector $|\psi\rangle$ can be expanded as $|\psi\rangle = \sum_i c_i |i\rangle$, where $c_i = \langle i|\psi\rangle$. The completeness relation is $\sum_i |i\rangle\langle i| = I$.

2.2.2 Operators and Matrices

Physical processes and observables are represented by linear operators.

- **Operators:** A linear operator A maps vectors to vectors, $A|\psi\rangle = |\phi\rangle$. In a basis $\{|i\rangle\}$, an operator has a matrix representation with elements $A_{ij} = \langle i|A|j\rangle$.
- **Outer Product:** The outer product of two vectors, $|\psi\rangle\langle\phi|$, is an operator. Its action on a vector $|v\rangle$ is $|\psi\rangle\langle\phi|v\rangle$.
- **Pauli Matrices:** The Pauli matrices are a crucial set of operators for single qubits:

$$\sigma_0 = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_1 = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- **Adjoint:** The adjoint or Hermitian conjugate of an operator A is denoted $A^\dagger$. It is defined such that for any states, $\langle\phi|A\psi\rangle = \langle A^\dagger\phi|\psi\rangle$.

2.2.3 Important Operator Types

- **Hermitian Operators:** An operator A is Hermitian if $A = A^\dagger$. Hermitian operators correspond to physical observables (like energy or momentum) and have real eigenvalues.
- **Unitary Operators:** An operator U is unitary if $U^\dagger U = I$. Unitary operators preserve inner products ($\langle U\phi|U\psi\rangle = \langle\phi|\psi\rangle$) and describe the evolution of closed quantum systems. Their eigenvalues are complex numbers of modulus 1.
- **Projectors:** A projector P is a Hermitian operator satisfying $P^2 = P$. It projects a state vector onto a subspace.

The **spectral decomposition theorem** states that any normal operator ($AA^\dagger = A^\dagger A$), which includes Hermitian and unitary operators, can be diagonalized in an orthonormal basis of its eigenvectors. For a Hermitian operator A, this means $A = \sum_i \lambda_i |i\rangle\langle i|$, where $|i\rangle$ are orthonormal eigenvectors with corresponding real eigenvalues λ_i.

2.2.4 The Tensor Product

The tensor product is the mathematical tool for describing composite quantum systems. The state space of a system composed of subsystems A and B is the tensor product of their individual Hilbert spaces, $H_{AB} = H_A \otimes H_B$.

- If $\{|i_A\rangle\}$ and $\{|j_B\rangle\}$ are bases for H_A and H_B, then $\{|i_A\rangle \otimes |j_B\rangle\}$ is a basis for H_{AB}. This is often written as $|i_A j_B\rangle$ or $|ij\rangle$.
- If system A is in state $|\psi_A\rangle$ and B is in $|\psi_B\rangle$, the composite system is in the product state $|\psi_A\rangle \otimes |\psi_B\rangle$.
- States that cannot be written as a product state, such as the Bell state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, are called **entangled**.

2.3 The Postulates of Quantum Mechanics

With the mathematical language established, the chapter presents the four fundamental postulates that connect the formalism to physical reality.

2.3.1 Postulate 1: State Space

Associated to any isolated physical system is a complex vector space with inner product (that is, a Hilbert space) known as the state space of the system. The system is completely described by its state vector, which is a unit vector in the system's state space.

For a single qubit, the state space is the two-dimensional Hilbert space $\mathbb{C}^2$. A state vector $|\psi\rangle$ is a linear combination of basis states $|0\rangle$ and $|1\rangle$:

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

2.3.2 Postulate 2: Evolution

The evolution of a closed quantum system is described by a unitary transformation. That is, the state $|\psi\rangle$ of the system at time t_1 is related to the state $|\psi'\rangle$ of the system at time t_2 by a unitary operator U which depends only on the times t_1 and t_2, $|\psi'\rangle = U\,|\psi\rangle$.

This evolution is more fundamentally described by the **Schrödinger equation**:

$$i\hbar \frac{d\,|\psi(t)\rangle}{dt} = H\,|\psi(t)\rangle$$

where H is a fixed Hermitian operator known as the **Hamiltonian** of the system. For a time-independent Hamiltonian, the solution is $|\psi(t)\rangle = e^{-iHt/\hbar}\,|\psi(0)\rangle$, so the unitary operator is $U(t) = e^{-iHt/\hbar}$.

2.3.3 Postulate 3: Quantum Measurement

Quantum measurements are described by a collection $\{M_m\}$ of measurement operators. These are operators acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur. If the state of the system is $|\psi\rangle$ immediately before the measurement, then the probability that result m occurs is given by

$$p(m) = \langle\psi|\,M_m^\dagger M_m\,|\psi\rangle$$

and the state of the system after the measurement is

$$\frac{M_m\,|\psi\rangle}{\sqrt{\langle\psi|\,M_m^\dagger M_m\,|\psi\rangle}}$$

The measurement operators satisfy the completeness equation, $\sum_m M_m^\dagger M_m = I$.

- **Projective Measurements:** A common special case is a projective measurement, where the measurement operators are orthogonal projectors $\{P_m\}$ such that $\sum_m P_m = I$. In this case, $p(m) = \langle\psi| P_m |\psi\rangle$.
- **POVMs:** When only the measurement probabilities are of interest, the set of positive operators $E_m = M_m^\dagger M_m$ is sufficient. This set is called a Positive Operator-Valued Measure (POVM).

2.3.4 Postulate 4: Composite Systems

The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. If we have systems $1, \ldots, n$*, and system* i *is prepared in the state* $|\psi_i\rangle$*, then the joint state of the total system is* $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$.

This postulate explains how to describe multi-particle systems and is the foundation for entanglement.

2.4 The Density Operator

The density operator (or density matrix) formalism provides a way to describe quantum systems whose state is not completely known (**mixed states**), or to describe the state of a subsystem of a larger entangled system.

2.4.1 Ensembles and Mixed States

If a quantum system is in one of a number of states $|\psi_i\rangle$ with respective probabilities p_i, this is an **ensemble** of pure states. The density operator for this system is defined as:

$$\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i|$$

- A state is **pure** if it can be described by a single state vector $|\psi\rangle$, in which case $\rho = |\psi\rangle \langle\psi|$.
- A state is **mixed** if it is not pure.
- A key property is that $\mathrm{tr}(\rho^2) \leq 1$, with equality if and only if the state is pure.

The quantum postulates can be rephrased in terms of density operators:

- **State:** A system's state is a density operator ρ satisfying $\rho \geq 0$ and $\mathrm{tr}(\rho) = 1$.
- **Evolution:** A closed system evolves as $\rho' = U\rho U^\dagger$.
- **Measurement:** The probability of outcome m is $p(m) = \mathrm{tr}(M_m^\dagger M_m \rho)$, and the post-measurement state is $\rho'_m = \frac{M_m \rho M_m^\dagger}{\mathrm{tr}(M_m^\dagger M_m \rho)}$.
- **Composite Systems:** The state of a composite system of uncorrelated subsystems is $\rho_{AB} = \rho_A \otimes \rho_B$.

2.4.2 The Reduced Density Operator

For a composite system AB in state ρ_{AB}, the state of subsystem A alone is given by the **reduced density operator** ρ_A, obtained by taking the **partial trace** over system B:

$$\rho_A = \mathrm{tr}_B(\rho_{AB})$$

This is a crucial concept, as it shows how a subsystem of a pure entangled state can be in a mixed state. For example, for the pure Bell state $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, the reduced density operator for either qubit is $\rho_A = \rho_B = I/2$, the maximally mixed state.

2.5 Advanced Tools for Composite Systems

2.5.1 The Schmidt Decomposition

This is a powerful theorem for analyzing pure states of a bipartite system AB. It states that any pure state $|\psi\rangle_{AB}$ can be written in a special basis:

$$|\psi\rangle_{AB} = \sum_i \lambda_i |i_A\rangle |i_B\rangle$$

where $\{|i_A\rangle\}$ and $\{|i_B\rangle\}$ are orthonormal bases for systems A and B respectively, and the λ_i are non-negative real numbers called the **Schmidt coefficients** satisfying $\sum_i \lambda_i^2 = 1$.

- The number of non-zero λ_i is the **Schmidt number**.
- A state is a product state if and only if its Schmidt number is 1. Otherwise, it is entangled.
- The eigenvalues of the reduced density operators ρ_A and ρ_B are precisely $\{\lambda_i^2\}$.

2.5.2 Purifications

Any mixed state ρ_A of a system A can be viewed as the reduced state of a pure state $|\psi\rangle_{AR}$ on a larger system AR, where R is a reference system. The state $|\psi\rangle_{AR}$ is called a **purification** of ρ_A. This is a mathematical tool that allows one to apply theorems about pure states to problems involving mixed states.

2.6 The EPR Paradox and Bell's Inequality

This final section delves into the foundational nature of quantum mechanics and what makes it so different from classical physics.

2.6.1 The EPR Argument

In 1935, Einstein, Podolsky, and Rosen (EPR) argued that quantum mechanics is an incomplete theory. They considered an entangled state (an EPR pair) shared between two spatially separated observers, Alice and Bob. They argued that by measuring her particle, Alice could predict with certainty the outcome of a corresponding measurement

on Bob's particle, without disturbing it. According to their criterion for physical reality-If, without in any way disturbing a system, we can predict with certainty...the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity—this implied that properties like position and momentum must have definite, pre-existing values. Since quantum mechanics does not assign such values, they concluded it was incomplete.

2.6.2 Bell's Theorem

For nearly 30 years, the EPR argument was considered a philosophical point. In 1964, John Bell showed it could be put to an experimental test. He proved that any theory based on the principles of **local realism**—the combination of locality (no faster-than-light influence) and realism (properties have definite values independent of measurement)—must satisfy certain statistical constraints, known as **Bell inequalities**.

A common form is the CHSH inequality, which considers correlations between measurement outcomes for four observables Q, R (measured by Alice) and S, T (measured by Bob), each with outcomes ± 1:

$$|E(QS) + E(RS) + E(RT) - E(QT)| \leq 2$$

Quantum mechanics, however, predicts that for a judicious choice of measurements on an entangled state like a Bell pair, this inequality can be violated. The quantum prediction is:

$$|E(QS) + E(RS) + E(RT) - E(QT)| \leq 2\sqrt{2}$$

Numerous experiments have confirmed the quantum mechanical prediction and demonstrated a clear violation of Bell's inequality.

2.6.3 Implications

The violation of Bell's inequality is a profound result. It proves that the world cannot be described by a local realistic theory. At least one of the intuitive classical assumptions of locality or realism (or both) must be abandoned. This demonstrates that entanglement is a genuinely non-classical phenomenon and a resource that cannot be simulated by any classical system sharing hidden information.

2.7 Conclusion

When I read Chapter 2, I felt that it gives a complete and formal introduction to the framework of quantum mechanics. It clearly lays out the rules—how quantum states are defined, how they evolve, and how measurements work—which really helped me understand the foundation for quantum information processing. I also found the introduction of tools like the density operator and the Schmidt decomposition particularly enlightening. Additionally, the discussions around EPR and Bell helped me appreciate not only how quantum mechanics works, but also why it behaves in such counterintuitive ways. Overall, the chapter gave me a solid understanding of both the mechanics and the deeper reasoning behind quantum theory.

Chapter 3

Introduction to computer science

3.1 Introduction

While reading Chapter 3, I realized it provides a solid introduction to classical computation theory, which is essential for understanding quantum computation in context. The chapter made me think about the fundamental questions of computation: What exactly is an algorithm? How can we design effective algorithms? And what are the minimal resources needed to solve a problem? Going through this chapter helped me see how classical computation is rigorously structured, and it gave me a clear framework to compare classical and quantum models. I could also appreciate where quantum computers might provide significant advantages over their classical counterparts.

3.2 Models for Computation

To formally define an "algorithm," computer science relies on abstract models of computation. The chapter focuses on two primary, equivalent models: the Turing machine and the circuit model.

3.2.1 Turing Machines

The Turing machine is a mathematical model of a general-purpose computer, proposed by Alan Turing in 1936. Despite its simplicity, it is believed to be capable of performing any computation that can be described by an algorithm.

- **Components:** A Turing machine consists of a program, a finite state control (a simple processor), an infinite one-dimensional tape (memory), and a read-write head that moves along the tape. The machine operates in discrete steps, reading a symbol from the tape, consulting its program based on its current internal state, writing a new symbol, changing its internal state, and moving the head left or right.
- **The Church-Turing Thesis:** This foundational thesis states that any function that is intuitively considered "computable by an algorithm" can be computed by a Turing machine. This thesis equates the physical notion of computation with a formal mathematical model. No counterexample has ever been found, though the discovery of a natural process that violates it would revolutionize science.

- **Universal Turing Machine (UTM):** Turing also showed the existence of a UTM, a single, fixed machine that can simulate any other Turing machine. A description of the machine to be simulated (M) and its input (x) are written on the UTM's tape, and the UTM then simulates M's execution on x. This is the theoretical basis for modern programmable computers, where software (the program) is distinct from hardware (the fixed machine).

- **Undecidability and the Halting Problem:** Not all problems are solvable by algorithms. Turing proved the existence of undecidable problems, the most famous being the **Halting Problem**: Does a given Turing machine M halt on a given input x? There is no general algorithm that can solve this problem for all possible M and x. This establishes a fundamental limit to the power of computation.

3.2.2 The Circuit Model

While the Turing machine is excellent for theoretical computer science, the **circuit model** is often more practical for designing and analyzing specific algorithms, and it serves as a more direct analogue for quantum circuits.

- **Components:** A circuit is composed of wires, which carry bits, and logic gates, which perform operations on those bits. The circuit must be acyclic (contain no feedback loops).

- **Universal Gates:** A small set of gates is sufficient to build a circuit for any computable function. For example, the NAND gate is universal for classical computation. The AND, OR, and NOT gates together also form a universal set.

- **Uniform Circuit Families:** A single circuit can only handle inputs of a fixed size. To compute a function on inputs of any length (like a Turing machine can), we use a **uniform circuit family** $\{C_n\}$, where C_n is a circuit for n-bit inputs. The "uniformity" condition requires that there must be an efficient classical algorithm (a Turing machine) that, given n, outputs a description of the circuit C_n. This condition prevents "hard-coding" non-computable information into the circuit design and establishes the equivalence between the circuit model and the Turing machine model.

3.3 The Analysis of Computational Problems

This section explores how to classify the difficulty of problems based on the resources required to solve them. The primary resources considered are time (number of computational steps) and space (amount of memory).

3.3.1 Computational Complexity

Computational complexity theory aims to classify problems into **complexity classes** based on their resource requirements.

- **Asymptotic Notation:** To analyze resource usage in a model-independent way, we use asymptotic notation. For an input of size n:

- $O(f(n))$ ("Big O"): The resource usage grows no faster than $f(n)$.
- $\Omega(f(n))$ ("Big Omega"): The resource usage grows at least as fast as $f(n)$.
- $\Theta(f(n))$ ("Big Theta"): The resource usage grows at the same rate as $f(n)$.

- **Efficient vs. Intractable:** A problem is considered **efficiently solvable** or **tractable** if an algorithm exists that solves it using resources (time or space) that are polynomial in the input size n, i.e., $O(n^k)$ for some constant k. If the best possible algorithm requires super-polynomial (e.g., exponential, $O(2^n)$) resources, the problem is considered **intractable**. The **strong Church-Turing thesis** conjectures that any reasonable model of classical computation can be simulated on a probabilistic Turing machine with at most a polynomial slowdown, suggesting that this polynomial/exponential dichotomy is a fundamental feature of computation.

3.3.2 Key Complexity Classes

The theory is most elegantly formulated in terms of **decision problems** (problems with a yes/no answer).

- **P (Polynomial Time):** The class of decision problems that can be solved by a deterministic Turing machine in polynomial time. These are the problems considered "efficiently solvable" classically.

- **NP (Nondeterministic Polynomial Time):** The class of decision problems for which a "yes" answer can be *verified* in polynomial time if a suitable piece of evidence, called a **witness**, is provided. For example, for the factoring decision problem ("Does number N have a factor less than k?"), a factor is a witness that can be quickly checked.

- **P vs. NP Problem:** It is clear that P $\subseteq$ NP. Whether P = NP is the most famous open question in computer science. Most researchers believe P $\neq$ NP, meaning there are problems whose solutions are easy to check but hard to find.

- **NP-Completeness:** The "hardest" problems in NP are called NP-complete. If a polynomial-time algorithm were found for any single NP-complete problem, it would imply that P = NP. The satisfiability problem (SAT) is a canonical NP-complete problem.

- **PSPACE:** The class of decision problems solvable by a Turing machine using a polynomial amount of space. It is known that P $\subseteq$ NP $\subseteq$ PSPACE, but it is not known if these inclusions are strict.

3.3.3 Energy and Computation

A physical consideration for computation is energy consumption.

- **Landauer's Principle:** Rolf Landauer showed that the only fundamental physical requirement for energy dissipation in computation is the erasure of information. The erasure of one bit of information in an environment at temperature T must dissipate at least $k_B T \ln 2$ of energy.

- **Reversible Computation:** This principle implies that if a computation is performed **reversibly**—without erasing information—it can, in principle, be done without dissipating any energy. An operation is reversible if its inputs can be uniquely determined from its outputs.

- **Reversible Gates:** While standard gates like AND and NAND are irreversible, it is possible to build universal reversible gates. The **Toffoli gate** (a 3-bit controlled-controlled-NOT) and the **Fredkin gate** (a 3-bit controlled-SWAP) are both universal for classical reversible computation. Any irreversible circuit can be simulated by a reversible one by adding extra "ancilla" bits to store information that would otherwise be erased, and then "uncomputing" this information at the end to restore the ancilla bits to their original state. This is a critical prerequisite for quantum computation, as all quantum evolution (except measurement) is unitary and thus reversible.

3.4 Conclusion

1. The power of quantum computers is not in computing the uncomputable but in changing the complexity of problems.

2. Quantum algorithms are analyzed using the same language of complexity theory (P, NP, etc.), allowing for direct comparisons. The quantum complexity class BQP (Bounded-error Quantum Polynomial time) is the quantum analogue of P, and it is known that $P \subseteq BQP \subseteq PSPACE$. Shor's algorithm suggests that BQP may be strictly larger than P.

3. The requirement for reversibility in quantum mechanics makes the study of classical reversible computation not just a theoretical curiosity but a necessary precursor.

Bibliography

[1] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. 10th Anniversary Edition. Cambridge University Press, 2010.