Physical Foundations of Key Concepts in Quantum Computing

Kimy Agudelo Jaramillo and Aldo Quelopana
Fundamentals of Quantum Computing Course (Prof. Aldo Quelopana)
October 2025

January 16, 2026

Abstract

This document provides a comprehensive exploration of the physical and mathematical foundations underlying quantum computing, with a strong emphasis on the principles of quantum mechanics that enable its power.

It begins with an introduction to classical computation and the circuit model, highlighting the limitations that motivate the quantum paradigm. The core quantum phenomena; superposition, uncertainty, entanglement, and unitary evolution, are presented through intuitive explanations, rigorous derivations, and illustrative examples. The formalism is built step-by-step: from the qubit and multi-qubit systems (tensor products, product vs. entangled states) to the four fundamental postulates of quantum mechanics, the Bloch sphere representation, and the operational use of Dirac notation. A detailed treatment of single-qubit gates (Pauli X, Y, Z; Hadamard; general rotations) and multi-qubit gates (CNOT, CZ, Toffoli, controlled-U) follows, including matrix representations, geometric interpretations on the Bloch sphere, circuit constructions, and Qiskit-based simulations that bridge theory with computational practice.

Key theoretical concepts such as commutators, compatibility of observables, the no-cloning theorem, and universality of gate sets are thoroughly examined.

The document concludes with landmark quantum algorithms, Deutsch–Jozsa (exponential separation), Grover's search (quadratic speedup), and the Quantum Fourier Transform (efficient circuit and product-form derivation) demonstrating how interference, parallelism, and entanglement yield computational advantages unattainable classically.

All concepts are illustrated with worked examples, proofs, and visualizations. Corresponding Qiskit implementations and further details are available in the accompanying GitHub repository: https://github.com/AgudeloKimy/Quantum-Computing.

This work serves as both an educational resource and a reference for understanding the physical origins of quantum computational power.

Contents

1 Foundations on Quantum Computing

Before discussing specific quantum operations, we must establish the mathematical concept of computation. Theoretical computer science provides the framework to formalize algorithms and discuss their efficiency and limitations.

1.1 What is Computation?

Abstractly, computation is a procedure that transforms input information into an output result through a sequence of simple, elementary operations. When such a procedure is defined in advance to solve a specific problem, it is called an **algorithm**.

Example: Primality Test

Consider the problem of deciding if a number x is prime. A naive classical algorithm proceeds as follows:

(i) Set $y = 2$.

(ii) Divide x by y. If the remainder is 0, output 0 (Composite) and halt.

(iii) Increment y by 1.

(iv) If $y = x$, output 1 (Prime) and halt. Otherwise, repeat from (ii).

While correct, the efficiency of this algorithm depends heavily on the magnitude of x.

1.1.1 Computational Complexity

In computer science, efficiency is measured using computational complexity. In particular, time complexity characterizes the asymptotic growth of the number of elementary operations performed by an algorithm as a function of the input length n (measured in binary digits).

We estimate this using **asymptotic order notation**:

Definition: Big-O Notation

Let $f, g : \mathbb{N} \to \mathbb{N}$ be functions. We say $f(n)$ is of order $g(n)$, denoted $f(n) = O(g(n))$, if there exists a constant $C > 0$ and N_0 such that for all $n > N_0$:

$$f(n) \leq C \cdot g(n)$$

This represents an asymptotic **upper bound** on the computation time.

Similarly, $\Omega(g(n))$ represents a lower bound. For the primality test, optimizing the algorithm to stop at $\lfloor \sqrt{x} \rfloor$ significantly reduces the complexity from $O(x)$ to $O(\sqrt{x})$, or in terms of bits n, from exponential to a more efficient order.

1.2 The Classical Circuit Model

To model algorithms mathematically, we use the **Classical Circuit Model**. Unlike Turing machines, which are theoretically powerful but complex to handle, circuit models visualize computation as a network of wires and gates.

1.2.1 Elementary Gates

A classical circuit computes Boolean functions $f : \{0,1\}^n \to \{0,1\}$ using predetermined elementary gates:

Gate	Symbol	Inputs/Outputs	Function
AND	$\wedge$	2 / 1	Output 1 iff both inputs are 1
OR	$\vee$	2 / 1	Output 1 if at least one input is 1
NOT	$\neg$	1 / 1	Flips the bit $(0 \to 1, 1 \to 0)$

Table 1: Elementary gates for classical circuits.

1.2.2 Circuit Complexity

Definition: Circuit Complexity

The circuit complexity $C(f)$ of a Boolean function f is the number of gates in the **minimum** circuit that correctly computes f.

Example: The Parity Problem

The parity function decides if the number of 1s in a sequence is odd (1) or even (0). For $n = 2$, this is the Exclusive-OR (XOR) operation, denoted $x_1 \oplus x_2$. It can be constructed using 5 elementary gates:

$$x_1 \oplus x_2 = (x_1 \wedge \neg x_2) \vee (\neg x_1 \wedge x_2)$$

For general n, the complexity grows linearly, $C(\text{PARITY}) = O(n)$.

Figure 1: Logic circuit diagram representing the XOR operation $(x_1 \oplus x_2)$.

Are there limits to circuit efficiency?

Theorem

For any Boolean function $f : \{0,1\}^n \to \{0,1\}$, the circuit complexity is at most:

$$C(f) \leq 5 \cdot 2^{n-1} - 4$$

Conversely, by counting arguments, one can prove that "hard" functions exist (where $C(f) \approx 2^n/n$) that cannot be computed by small circuits.

1.3 The Quantum Circuit Model

We now extend these concepts to quantum mechanics. While the classical model manipulates bits $\{0, 1\}$ using logic gates, the **Quantum Circuit Model** manipulates **qubits** using unitary transformations.

- **State Space:** Instead of discrete bits, wires carry quantum states $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$.
- **Gates:** Instead of Boolean logic $(\wedge, \vee, \neg)$, operations are unitary matrices U ($U^\dagger U = I$). This ensures computation is **reversible**, unlike the classical AND/OR gates which dissipate information.
- **Output:** The result is obtained via measurement, collapsing the quantum state to a classical bit sequence.

In the following sections, we define the elementary unitary gates that form the building blocks of quantum algorithms, starting with the single-qubit operations.

2 Fundamentals of Qubit Systems

The fundamental carrier of quantum information is the **qubit**, a two-level quantum system. While a single qubit already exhibits superposition and uncertainty, the true power of quantum information processing emerges in **multi-qubit systems**, where entanglement enables correlations impossible in classical physics.

This section builds on the postulates to describe systems composed of multiple qubits. We emphasize the tensor product structure, which governs how independent systems combine, and highlight the emergence of entanglement.

2.1 The Qubit

The fundamental unit of quantum information is the **qubit**. Unlike a classical bit that exists in a state of deterministically 0 or 1, a qubit exists in a vector space described by the complex numbers.

Definition — The Qubit

A **qubit** is a quantum system described by a two-dimensional complex Hilbert space $\mathcal{H} = \mathbb{C}^2$. Its state is represented by a unit vector $|\psi\rangle$, which is a superposition of the orthonormal computational basis states $|0\rangle$ and $|1\rangle$:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

where $\alpha, \beta \in \mathbb{C}$ correspond to probability amplitudes satisfying the normalization condition $|\alpha|^2 + |\beta|^2 = 1$.

Physical realizations include electron spin, photon polarization, and superconducting circuits (see Postulate 1).

2.2 Multi-Qubit Systems: Tensor Product Construction

When combining n qubits, Postulate 4 dictates that the joint Hilbert space is the tensor product of the individual spaces.

Postulate 4 — Composite Systems (Reminder)

The Hilbert space of an n-qubit system is

$$\mathcal{H}_{2^n} = \underbrace{\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{n \text{ times}} = (\mathbb{C}^2)^{\otimes n},$$

with dimension $\dim \mathcal{H}_{2^n} = 2^n$.

The computational basis for n qubits is the set of 2^n product states

$$\{|i_1 i_2 \dots i_n\rangle \equiv |i_1\rangle \otimes |i_2\rangle \otimes \cdots \otimes |i_n\rangle \mid i_j \in \{0, 1\}\}.$$

2.2.1 Tensor Product of Two Qubits

For two qubits in states $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$ and $|\phi\rangle = \beta_0 |0\rangle + \beta_1 |1\rangle$, the composite state (if uncorrelated) is

$$|\psi\rangle \otimes |\phi\rangle = \begin{pmatrix} \alpha_0 |\phi\rangle \\ \alpha_1 |\phi\rangle \end{pmatrix} = \begin{pmatrix} \alpha_0\beta_0 \\ \alpha_0\beta_1 \\ \alpha_1\beta_0 \\ \alpha_1\beta_1 \end{pmatrix} = \alpha_0\beta_0 |00\rangle + \alpha_0\beta_1 |01\rangle + \alpha_1\beta_0 |10\rangle + \alpha_1\beta_1 |11\rangle .$$

Example: Calculating a Composite State via Tensor Product

We explicitly calculate the joint state $|\Psi\rangle = |\psi\rangle \otimes |\phi\rangle$ for two independent qubits.

1. Define the states:

$$|\psi\rangle = \frac{1}{\sqrt{3}} \begin{pmatrix} i \\ \sqrt{2} \end{pmatrix}, \quad |\phi\rangle = \frac{1}{\sqrt{5}} \begin{pmatrix} 2 \\ 1 \end{pmatrix}$$

2. Separate scalars and vectors: First, we multiply the normalization coefficients:

$$|\psi\rangle \otimes |\phi\rangle = \left(\frac{1}{\sqrt{3}} \cdot \frac{1}{\sqrt{5}} \right) \left[\begin{pmatrix} i \\ \sqrt{2} \end{pmatrix} \otimes \begin{pmatrix} 2 \\ 1 \end{pmatrix} \right] = \frac{1}{\sqrt{15}} \left[\begin{pmatrix} i \\ \sqrt{2} \end{pmatrix} \otimes \begin{pmatrix} 2 \\ 1 \end{pmatrix} \right]$$

3. Expand using the Kronecker Product rule: Multiply each element of the first vector by the entire second vector:

$$= \frac{1}{\sqrt{15}} \begin{pmatrix} i \cdot \begin{pmatrix} 2 \\ 1 \end{pmatrix} \\ \sqrt{2} \cdot \begin{pmatrix} 2 \\ 1 \end{pmatrix} \end{pmatrix}$$

4. Final Calculation: Distribute the values into the sub-vectors to form the final 4-dimensional vector:

$$= \frac{1}{\sqrt{15}} \begin{pmatrix} i \cdot 2 \\ i \cdot 1 \\ \sqrt{2} \cdot 2 \\ \sqrt{2} \cdot 1 \end{pmatrix} = \frac{1}{\sqrt{15}} \begin{pmatrix} 2i \\ i \\ 2\sqrt{2} \\ \sqrt{2} \end{pmatrix} \in \mathbb{C}^4$$

2.2.2 Key Properties

Rather than using vector components, it is often more convenient to use the algebraic properties of the tensor product:

- **Bilinearity:** The tensor product is linear in both arguments.

$$(a|\psi_1\rangle + |\psi_2\rangle) \otimes |\phi\rangle = a(|\psi_1\rangle \otimes |\phi\rangle) + |\psi_2\rangle \otimes |\phi\rangle$$

- **Inner Product Rule:** The inner product of two tensor states factorizes.

$$\langle \psi_1 \otimes \phi_1 | \psi_2 \otimes \phi_2 \rangle = \langle \psi_1 | \psi_2 \rangle \langle \phi_1 | \phi_2 \rangle$$

2.3 Product States vs. Entangled States

Not all states in $(\mathbb{C}^2)^{\otimes n}$ are simple tensor products.

Product and Entangled States

- A state $|\Psi\rangle$ is a **product state** (or separable) if $|\Psi\rangle = |\psi\rangle_A \otimes |\phi\rangle_B \otimes \cdots$ for some single-qubit states.
- Otherwise, $|\Psi\rangle$ is **entangled**.

Entangled states exhibit non-classical correlations that cannot be explained by local hidden variables [16].

Example: Proof that the Bell State is Entangled

Consider the Bell state

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big).$$

We prove that this state is **entangled**, i.e., it cannot be expressed as a product state $|\Phi^+\rangle = |a\rangle \otimes |b\rangle$ for any single-qubit states

$$|a\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \quad |b\rangle = \gamma\,|0\rangle + \delta\,|1\rangle\,,$$

where $\alpha, \beta, \gamma, \delta \in \mathbb{C}$.

Step 1: Expand the assumed product state The tensor product expands as

$$\begin{aligned} |a\rangle \otimes |b\rangle &= (\alpha\,|0\rangle + \beta\,|1\rangle) \otimes (\gamma\,|0\rangle + \delta\,|1\rangle) \\ &= \alpha\gamma\ |00\rangle + \alpha\delta\ |01\rangle + \beta\gamma\ |10\rangle + \beta\delta\ |11\rangle\,. \end{aligned}$$

In the ordered computational basis $\{|00\rangle\,, |01\rangle\,, |10\rangle\,, |11\rangle\}$, the state vector is

$$\begin{pmatrix} \alpha\gamma \\ \alpha\delta \\ \beta\gamma \\ \beta\delta \end{pmatrix}.$$

Step 2: Express the Bell state in the same basis

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Step 3: Equate coefficients For the states to be identical (up to an irrelevant global phase), the components must satisfy

$$\alpha\gamma = \frac{1}{\sqrt{2}}, \tag{1}$$

$$\alpha\delta = 0, \tag{2}$$

$$\beta\gamma = 0, \tag{3}$$

$$\beta\delta = \frac{1}{\sqrt{2}}. \tag{4}$$

Step 4: Derive the contradiction From (1), $\alpha\gamma = 1/\sqrt{2} \neq 0$, so $\alpha \neq 0$ and $\gamma \neq 0$.
From (2), $\alpha\delta = 0$ and $\alpha \neq 0$, hence $\delta = 0$.
From (3), $\beta\gamma = 0$ and $\gamma \neq 0$, hence $\beta = 0$.
Substituting into (4): $\beta\delta = 0 \cdot 0 = 0$, but (4) requires $\beta\delta = 1/\sqrt{2} \neq 0$.
This is a contradiction. No complex coefficients $\alpha, \beta, \gamma, \delta$ satisfy the system simultaneously. Therefore, the Bell state $|\Phi^+\rangle$ cannot be written as a tensor product of individual qubit states and is **entangled**.

2.4 Measurements on Multi-Qubit Systems

Measurements on composite systems can be:

- **Local**: Acting separately on each qubit (tensor product of single-qubit projectors).
- **Joint**: Defined by a basis of the full 2^n-dimensional space (e.g., the Bell basis for two qubits).

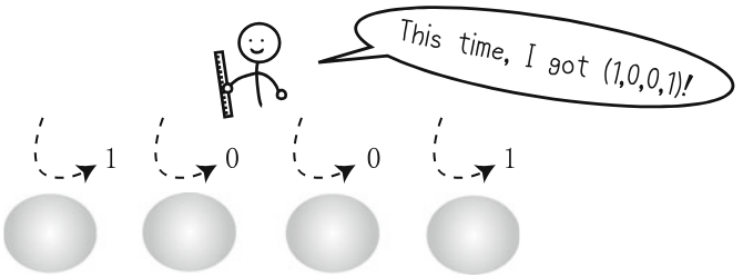

Figure 2: Joint measurements on multi-qubit systems. Local measurements on individual qubits can be tensored to form measurements on subsystems, but fully joint measurements require bases spanning the entire composite space.[13]

Entangled states yield correlated outcomes even under local measurements: measuring one qubit of $|\Phi^+\rangle$ instantly determines the outcome on the distant partner, independent of distance.

2.5 Generalization of Quantum Rules to n Qubits

All foundational rules extend straightforwardly:

- State: Normalized vector in $\mathbb{C}^{2^n}$.
- Measurement: Projective measurement in any orthonormal basis $\{|\phi_i\rangle\}_{i=0}^{2^n-1}$.
- Probability of outcome i: $P(i) = |\langle\phi_i|\psi\rangle|^2$.
- Post-measurement state: Collapse to $|\phi_i\rangle$.
- Evolution: Unitary $U \in \mathrm{U}(2^n)$.

3 Quantum Phenomena Beyond Classical Intuition

Quantum mechanics replaces classical determinism with probabilistic predictions, revealing phenomena absent in the macroscopic world: **superposition**, **uncertainty**, and **entanglement**. These challenge classical intuition and form the foundation of quantum information science (QIS), enabling applications such as quantum computing, teleportation, and cryptography.

This chapter presents quantum mechanics operationally as a **probabilistic theory**: given a prepared quantum state, the central task is to compute the probability of a specific measurement outcome (Figure 3). We adopt the **Copenhagen interpretation**, in which measurement outcomes are inherently random and the wavefunction collapses upon observation—an empirically validated framework.

Before stating the four postulates formally, we examine the three core phenomena that defy classical intuition. Each is illustrated physically, derived mathematically, and linked to the corresponding postulates. We focus primarily on **qubit systems** (two-level systems with Hilbert space $\mathcal{H} = \mathbb{C}^2$), the minimal unit for QIS.

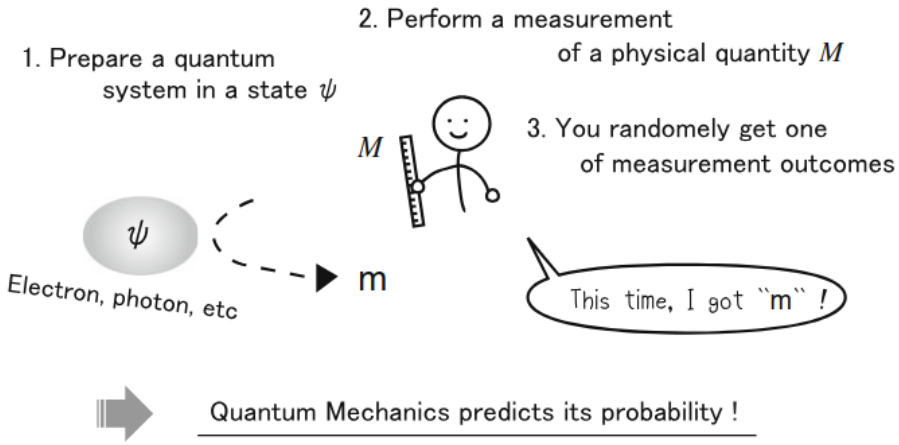

Figure 3: Operational view: A quantum state is prepared (left). A measurement apparatus (right) yields a probabilistic outcome m or M. The core task of QM is to compute $P(m|\text{state})$. Adapted from [3].

3.1 Superposition: The Linear Structure of State Space

In classical physics, a system occupies a single definite state at any time. Quantum mechanics allows a system to exist in a **linear superposition** of multiple basis states.

Superposition Principle

The general pure state of a qubit is

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

The complex coefficients α and β are probability amplitudes; their squared magnitudes give measurement probabilities in the computational basis via the Born rule (Postulate 2). The relative phase between α and β produces observable interference effects, whereas the global phase is physically irrelevant.

Pure qubit states correspond to points on the Bloch sphere, with $|0\rangle$ and $|1\rangle$ at the north and south poles, respectively.

Example: Superposition vs. Classical Mixture

A classical probabilistic mixture yields identical statistics in the computational basis to the superposition $\sqrt{p}\,|0\rangle + e^{i\phi}\sqrt{1-p}\,|1\rangle$, but only the quantum state exhibits interference under unitary transformations (e.g., the Hadamard gate). This interference enables quantum parallelism in algorithms (§8.2, §8.3).

3.2 Uncertainty Principle: Intrinsic Limits on Knowledge

Classical physics allows, in principle, simultaneous precise knowledge of all observables. Quantum mechanics imposes fundamental limits via non-commuting operators.

Heisenberg Uncertainty Principle

For any two observables A and B, the product of their standard deviations in state $|\psi\rangle$ satisfies

$$\Delta A \cdot \Delta B \geq \frac{1}{2}\left|\langle [A, B]\rangle\right|.$$

For canonical conjugates such as position and momentum ($[x, p] = i\hbar$),

$$\Delta x \cdot \Delta p \geq \frac{\hbar}{2}.$$

In spin-1/2 systems, the Pauli operators yield

$$[\sigma_x, \sigma_y] = 2i\sigma_z \quad \Rightarrow \quad \Delta\sigma_x \cdot \Delta\sigma_y \geq |\langle\sigma_z\rangle|.$$

No state can simultaneously have definite values for incompatible observables (Postulates 1 and 2).

3.3 Entanglement: Non-Classical Correlations

Interacting quantum systems can develop correlations inexplicable by local classical variables.

Maximally Entangled State (Bell Pair)

The Bell state

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

is non-separable.

Proof by contradiction. Assume $|\Phi^+\rangle = (\alpha\,|0\rangle + \beta\,|1\rangle) \otimes (\gamma\,|0\rangle + \delta\,|1\rangle)$. Equating coefficients gives $\alpha\gamma = \beta\delta = 1/\sqrt{2}$ and $\alpha\delta = \beta\gamma = 0$, which is inconsistent. Hence, the state is entangled.

Measurement of one qubit instantaneously determines the outcome for its distant partner, violating Bell inequalities—a prediction confirmed experimentally. Entanglement is the key resource for many quantum information protocols (Postulate 4).

3.4 Copenhagen Interpretation: An Operational Framework

The Copenhagen interpretation, followed throughout this text, treats quantum mechanics as an operational probabilistic theory:

- The state vector $|\psi\rangle$ encodes all available probabilistic information via the Born rule.
- Measurement induces non-unitary collapse to an eigenstate of the observable.
- Complementarity: certain pairs of observables are mutually exclusive.
- Randomness is intrinsic; no local hidden variables are needed.

Collapse vs. Unitary Evolution

Between measurements, the state evolves unitarily according to the Schrödinger equation (Postulate 3). Upon measurement, it collapses discontinuously—an axiomatic feature of the theory.

Quantum Information Science (QIS) exploits these principles for revolutionary applications:

- **Quantum Computing**: Exponential speedup via superposition and entanglement [8].
- **Quantum Teleportation**: Transfer of quantum states using entanglement and classical communication [9].
- **Quantum Cryptography**: Unconditionally secure key distribution (BB84 protocol) [10].

Within this broad landscape of quantum technologies—as outlined in national strategies such as the report of the Chilean Presidential Advisory Commission on Quantum Technologies, which classifies developments into hardware, sensing, communications, and software [21]—this document adopts a focused perspective on **Quantum Computing – Software**: the theoretical foundations, algorithmic design, and quantum circuit models that enable the programming of quantum processors.

This section presents QM *operationally* as a **probabilistic theory** [3, 12], answering:

> *Given a prepared quantum state, what is the probability of observing a specific measurement outcome?*

We adopt the **Copenhagen interpretation** [11]: QM predicts probabilities; measurement outcomes are inherently random, and the wavefunction "collapses" upon observation. This view is empirically validated across all quantum experiments.

We focus on **qubit systems**—two-level quantum systems ($\mathcal{H} = \mathbb{C}^2$)—the minimal unit for QIS, generalizing classical bits. All concepts extend to higher dimensions.

Example: Computing the Expectation Value $\langle +|\sigma_z|+\rangle$

We calculate the expectation value of the Pauli-Z operator for the state $|+\rangle$.

1. Definitions:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad \langle +| = \frac{1}{\sqrt{2}}(\langle 0| + \langle 1|)$$

$$\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$$

2. Calculation: We substitute the definitions into the expression:

$$\begin{aligned}\langle +|\sigma_z|+\rangle &= \left(\frac{\langle 0| + \langle 1|}{\sqrt{2}}\right)(|0\rangle\langle 0| - |1\rangle\langle 1|)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \\ &= \frac{1}{2}(\langle 0| + \langle 1|)\underbrace{[(|0\rangle\langle 0| - |1\rangle\langle 1|)(|0\rangle + |1\rangle)]}_{\text{Apply operator to the ket first}}\end{aligned}$$

Let's expand the term in the brackets using linearity:

$$\sigma_z|+\rangle = (|0\rangle \underbrace{\langle 0|0\rangle}_{1} + |0\rangle \underbrace{\langle 0|1\rangle}_{0}) - (|1\rangle \underbrace{\langle 1|0\rangle}_{0} + |1\rangle \underbrace{\langle 1|1\rangle}_{1}) = |0\rangle - |1\rangle$$

Now, complete the inner product with the bra $\langle +|$:

$$\begin{aligned}\langle +|\sigma_z|+\rangle &= \frac{1}{2}(\langle 0| + \langle 1|)(|0\rangle - |1\rangle) \\ &= \frac{1}{2}\left(\underbrace{\langle 0|0\rangle}_{1} - \underbrace{\langle 0|1\rangle}_{0} + \underbrace{\langle 1|0\rangle}_{0} - \underbrace{\langle 1|1\rangle}_{1}\right) \\ &= \frac{1}{2}(1 - 0 + 0 - 1) \\ &= 0\end{aligned}$$

Thus, the expectation value is **0**.

4 Mathematical and Physical Framework

Quantum mechanics constitutes the physical foundation of quantum computing. Its mathematical framework is built upon **complex Hilbert spaces**, in which quantum states are represented as normalized vectors, physical observables as Hermitian operators, and time evolution as unitary transformations [1, 2].

In the field of quantum information science, we predominantly work with **finite-dimensional** Hilbert spaces of the form $\mathcal{H} = \mathbb{C}^d$, where the paradigmatic case of a single qubit corresponds to $d = 2$. This formalism relies heavily on Dirac notation and the tools of linear algebra, both of which are indispensable for understanding the physical behavior of quantum systems and for designing quantum algorithms.

A concise summary of the essential mathematical concepts involved — Hilbert spaces, inner products, linear operators, tensor products, Pauli matrices, and the operator exponential — is provided in **Appendix A** for quick reference.

The subsequent sections build directly upon this mathematical foundation. First, we highlight the most counterintuitive quantum phenomena that emerge from it (superposition, interference, entanglement, and uncertainty), and then we formally state the four fundamental postulates of quantum mechanics.

While quantum computing rests entirely on the mathematical structure of quantum mechanics, it differs from traditional quantum physics in one crucial practical aspect:

Quantum information science almost exclusively deals with finite-dimensional Hilbert spaces, typically of the tensor-product form $\mathcal{H} = (\mathbb{C}^2)^{\otimes n} \cong \mathbb{C}^{2^n}$, where n is the number of qubits.

This restriction to finite dimensions dramatically simplifies many proofs and calculations while fully preserving the key phenomena that give quantum computing its power: superposition, interference, entanglement, and reversible unitary evolution.

4.1 Finite-dimensional Hilbert spaces and operational Dirac notation

A system of n qubits lives in the Hilbert space

$$\mathcal{H} = \mathbb{C}^{2^n}$$

equipped with the standard Hermitian inner product:

$$\langle \phi | \psi \rangle = \sum_{i=1}^{2^n} \phi_i^* \psi_i$$

Physically valid pure states are unit vectors:

$$|\psi\rangle \in \mathcal{H}, \quad \langle \psi | \psi \rangle = 1$$

In quantum computing, Dirac notation is used in a very practical, operational way. Here are the most important everyday meanings:

- $|\psi\rangle$ represents a **quantum state** (column vector / ket)
- $\langle \psi |$ represents the **conjugate transpose** (row vector / bra = ket†)
- $\langle \phi | \psi \rangle$ complex number = **inner product** = transition amplitude

- $|\langle\phi|\psi\rangle|^2$ **probability** of measuring outcome associated with $|\phi\rangle$ when the system is in $|\psi\rangle$
- $|\phi\rangle\langle\psi|$ **rank-1 operator** (projector if $|\psi\rangle$ is normalized)
- $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$, $|i\rangle$, $|-i\rangle$ **reference states** used constantly (computational basis, Hadamard basis, imaginary basis, etc.)

Golden practical rule: Almost every real calculation in quantum computing eventually reduces to combinations of inner products $\langle\phi|\psi\rangle$ and outer products $|a\rangle\langle b|$.

4.2 Operators as structure-preserving transformations

In quantum computing we primarily view operators as **reversible transformations** acting on states. The most relevant properties are:

Key Properties of Operators in Quantum Computing

- **Unitary operators** ($U^\dagger U = UU^\dagger = I$):
  - preserve the norm: $\|U|\psi\rangle\| = \||\psi\rangle\| = 1$
  - preserve probabilities and inner products
  - represent **coherent time evolution** and **all quantum gates**
- **Hermitian operators** ($A^\dagger = A$):
  - represent **observables** (measurable quantities)
  - have real eigenvalues
  - are used to define **measurement bases**
- **Projectors** ($P^\dagger = P$ and $P^2 = P$):
  - represent **ideal measurement collapse**
  - $P = \sum_i |i\rangle\langle i|$ (projector onto a subspace)

Fundamental physical connection: Coherent quantum evolution (between measurements) is always unitary. Measurements are the only moments when an irreversible process (collapse) occurs, described using Hermitian operators and projectors.

4.3 Quick operational summary

Physical concept	Main mathematical object
Pure quantum state	unit vector $\|\psi\rangle \in \mathbb{C}^{2^n}$
Transition probability	$\|\langle\phi\|\psi\rangle\|^2$
Reversible evolution (gates)	unitary operator U
Observable / measurement	Hermitian operator A
Ideal measurement outcome	projector P_m
Entanglement	state $\|\Psi\rangle_{AB}$ cannot be factored as $\|\psi\rangle_A \otimes \|\phi\rangle_B$

This finite-dimensional mathematical framework, combined with operational Dirac notation and the clear distinction between unitary transformations (gates) and projective measurements, forms the foundation for all gates, circuits, and algorithms presented in the following sections.

5 Foundational Postulates of Quantum Mechanics

Quantum mechanics provides a complete and universally validated framework for describing physical systems at microscopic scales [1, 2]. Unlike classical mechanics, which relies on deterministic trajectories in phase space, quantum mechanics is intrinsically probabilistic and linear, with its predictions encoded in complex amplitudes.

The theory is axiomatized by **four foundational postulates** that precisely specify:

1. How physical states are represented,
2. How measurements are performed and their outcomes interpreted,
3. How isolated systems evolve in time,
4. How composite systems are constructed from individual subsystems.

These postulates are not derived from more fundamental principles but are justified by their extraordinary agreement with experiment—from atomic spectra to superconducting circuits and photonic devices.

In quantum information science, we focus on **finite-dimensional** systems (especially qubits and qudits), where the mathematical structure simplifies considerably without loss of generality for the core phenomena (superposition, uncertainty, entanglement).

Before stating the postulates formally, we establish the necessary mathematical framework.

5.1 Mathematical Framework: Hilbert Spaces and Dirac Notation

Quantum mechanics is rigorously formulated in the language of complex **Hilbert spaces** [1, 2]. A Hilbert space $\mathcal{H}$ is a complete vector space over $\mathbb{C}$ equipped with an inner product $\langle\cdot|\cdot\rangle : \mathcal{H} \times \mathcal{H} \to \mathbb{C}$ that induces a norm $\|\psi\| = \sqrt{\langle\psi|\psi\rangle}$.

The completeness requirement ensures that all Cauchy sequences converge within the space—a technical condition essential for physical predictions but straightforward in finite dimensions.

In quantum information science we primarily work with **finite-dimensional** Hilbert spaces ($\dim \mathcal{H} < \infty$), which simplifies many proofs while capturing all essential phenomena relevant to quantum computing and communication.

5.1.1 Dirac Notation (Bra-Ket)

To manipulate states and operators efficiently, we employ Dirac's bra-ket notation:

- $|\psi\rangle$: **ket** — represents a state vector in $\mathcal{H}$ (column vector when expressed in a basis).
- $\langle\psi|$: **bra** — the dual vector (conjugate transpose, row vector in a basis).
- $\langle\phi|\psi\rangle$: **inner product** — complex scalar, linear in $|\psi\rangle$ and antilinear in $|\phi\rangle$.
- $\langle\psi|\psi\rangle = 1$: normalization condition for physical pure states.
- Global phase irrelevance: $|\psi\rangle \sim e^{i\gamma}|\psi\rangle$ (same physical state).

- $|\phi\rangle\langle\psi|$: **outer product** — defines a linear operator mapping $|\xi\rangle \mapsto |\phi\rangle\langle\psi|\xi\rangle$.

A more detailed treatment of the mathematical properties underlying this notation—conjugate transpose (adjoint), inner product and norm, and outer products—is provided in Appendix A for quick reference.

5.1.2 Key Classes of Linear Operators

Linear operators $A : \mathcal{H} \to \mathcal{H}$ play central roles:

- **Hermitian (self-adjoint)**: $A^\dagger = A$, where the adjoint satisfies $\langle\phi|A\psi\rangle = \langle A^\dagger\phi|\psi\rangle^* = \langle A\phi|\psi\rangle$ (no star needed when A is Hermitian). Hermitian operators have real eigenvalues and represent observables.
- **Unitary**: $U^\dagger U = UU^\dagger = I$. Unitary operators preserve norms and inner products, corresponding to reversible evolution.
- **Projectors**: $P^\dagger = P$ and $P^2 = P$. They project onto subspaces and model ideal (projective) measurements.

5.1.3 Composite Systems and Tensor Products

For two systems with Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, the joint Hilbert space is the **tensor product**

$$\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B, \quad \dim \mathcal{H}_{AB} = \dim \mathcal{H}_A \cdot \dim \mathcal{H}_B.$$

If subsystem A is in $|\psi\rangle_A$ and B in $|\phi\rangle_B$, the composite state is $|\psi\rangle_A \otimes |\phi\rangle_B \equiv |\psi\phi\rangle_{AB}$. QM rests on four **postulates** [1, 2], rigorously defining states, measurements, evolution, and composition.

5.2 The Four Postulates

With this mathematical framework in place, quantum mechanics rests on four foundational postulates that precisely define states, measurements, evolution, and composition of systems.

5.2.1 Postulate 1: Quantum States

Postulate 1 — State Space

The state of a quantum system is completely described by a **unit vector** (ket) $|\psi\rangle$ in a complex Hilbert space $\mathcal{H}$:

$$||\psi|| = \sqrt{\langle\psi|\psi\rangle} = 1$$

Global phase is irrelevant: $|\psi\rangle \sim e^{i\gamma}|\psi\rangle$.

For a **qubit**, $\mathcal{H} = \mathbb{C}^2$. The **computational basis** is:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

A general **pure state** is:

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

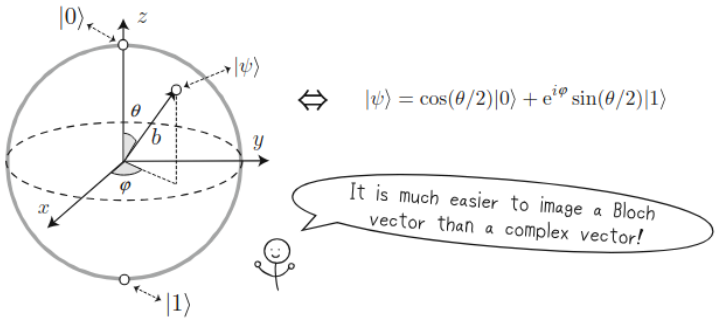

Figure 4: Bloch sphere representation: Any pure qubit state $|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle$ corresponds to a point $(\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$ on the unit sphere. Poles: $|0\rangle$, $|1\rangle$. Equator: maximal superpositions (e.g., $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$). [13]

Common physical realizations of qubits:

- Electron spin-1/2 in a magnetic field (Zeeman splitting): $|0\rangle \equiv |\uparrow_z\rangle$, $|1\rangle \equiv |\downarrow_z\rangle$.
- Photon polarization: $|0\rangle \equiv |H\rangle$ (horizontal), $|1\rangle \equiv |V\rangle$ (vertical).
- Superconducting circuits (transmon, flux qubits) based on Josephson junctions [14].

5.3 Postulate 2: Measurements and the Born Rule

Postulate 2 — Measurement

A measurement is specified by a set of **projectors** $\{P_m\}$ onto orthogonal subspaces, with $\sum_m P_m = I$. The probability of outcome m in state $|\psi\rangle$ is:

$$P(m) = \langle\psi|P_m|\psi\rangle$$

After measurement, the state collapses to:

$$|\psi\rangle \to \frac{P_m|\psi\rangle}{\sqrt{P(m)}}$$

For a **qubit** with orthonormal basis measurement $\{|\phi_0\rangle, |\phi_1\rangle\}$:

$$P_0 = |\phi_0\rangle\langle\phi_0|, \quad P_1 = |\phi_1\rangle\langle\phi_1|$$

$$P(i) = |\langle\phi_i|\psi\rangle|^2 \quad \text{(Born rule)}$$

Example: Measurement Probabilities and State Collapse

Consider a qubit prepared in the superposition state:

$$|\psi\rangle = \frac{1}{\sqrt{5}}|0\rangle + \frac{2}{\sqrt{5}}|1\rangle$$

1. Normalization Check: First, verify that probabilities sum to 1:

$$\langle\psi|\psi\rangle = \left|\frac{1}{\sqrt{5}}\right|^2 + \left|\frac{2}{\sqrt{5}}\right|^2 = \frac{1}{5} + \frac{4}{5} = 1$$

2. Applying the Born Rule: We measure in the computational basis $\{|0\rangle, |1\rangle\}$. The probability of obtaining outcome m is $P(m) = |\langle m|\psi\rangle|^2$:

$$P(0) = |\langle 0|\psi\rangle|^2 = \left|\frac{1}{\sqrt{5}}\underbrace{\langle 0|0\rangle}_{1} + \frac{2}{\sqrt{5}}\underbrace{\langle 0|1\rangle}_{0}\right|^2 = \frac{1}{5} \quad (20\%)$$

$$P(1) = |\langle 1|\psi\rangle|^2 = \left|\frac{1}{\sqrt{5}}\underbrace{\langle 1|0\rangle}_{0} + \frac{2}{\sqrt{5}}\underbrace{\langle 1|1\rangle}_{1}\right|^2 = \frac{4}{5} \quad (80\%)$$

3. Post-Measurement Collapse: According to the measurement postulate, the state collapses to the normalized eigenvector corresponding to the observed outcome.

- **If outcome 0 is observed:**

$$|\psi_{\text{new}}\rangle = \frac{P_0|\psi\rangle}{\sqrt{P(0)}} = \frac{|0\rangle\langle 0|\psi\rangle}{1/\sqrt{5}} = \frac{(1/\sqrt{5})|0\rangle}{1/\sqrt{5}} = |0\rangle$$

- **If outcome 1 is observed:**

$$|\psi_{\text{new}}\rangle = \frac{P_1|\psi\rangle}{\sqrt{P(1)}} = \frac{|1\rangle\langle 1|\psi\rangle}{2/\sqrt{5}} = \frac{(2/\sqrt{5})|1\rangle}{2/\sqrt{5}} = |1\rangle$$

Theorem: Born Rule Derivation from Unitary Evolution

Consider a quantum system coupled to an auxiliary qubit called an **ancilla** (initially prepared in a known state, typically $|0\rangle_A$). The combined initial state is $|\psi\rangle|0\rangle_A$, where $|\psi\rangle$ is the state of the system of interest.
Apply a unitary U that entangles the system with the ancilla:

$$U|\psi\rangle|0\rangle_A = \sum_m \sqrt{P(m)}|\psi_m\rangle|m\rangle_A,$$

where $\{|\psi_m\rangle\}$ are normalized states of the system and $\{|m\rangle_A\}$ are orthogonal states of the ancilla.
Measuring the ancilla in the basis $\{|m\rangle_A\}$ yields outcome m with probability $P(m) = |\sqrt{P(m)}|^2$, and the system collapses to the corresponding post-measurement state $|\psi_m\rangle$.
This construction *derives* the probabilistic Born rule from purely unitary evolution and entanglement with an auxiliary degree of freedom [15].

5.4 Postulate 3: Unitary Time Evolution

Postulate 3 — Dynamics

Between measurements, the state evolves unitarily via the Schrödinger equation:

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

Solution: $|\psi(t)\rangle = U(t,t_0)|\psi(t_0)\rangle$, with $U(t,t_0) = \mathcal{T}\exp\left(-\frac{i}{\hbar}\int_{t_0}^{t} H(t')dt'\right)$ unitary ($U^\dagger U = I$).

For time-independent H:

$$U(t) = e^{-iHt/\hbar}$$

Physical origin: The operator H is the **system Hamiltonian**, which represents the total energy of the quantum system (kinetic + potential + interaction terms). In quantum mechanics, the Hamiltonian fully determines the time evolution of isolated systems via the Schrödinger equation.

A classic example is a spin-1/2 particle (e.g., electron) in a magnetic field $\vec{B} = B\hat{z}$:

$$H = -\vec{\mu}\cdot\vec{B} = -\gamma B S_z = -\frac{\gamma B\hbar}{2}\sigma_z,$$

where $\vec{\mu}$ is the magnetic moment, γ the gyromagnetic ratio, and $S_z = \frac{\hbar}{2}\sigma_z$ the z-component of spin. The evolution generated by this Hamiltonian corresponds to Larmor precession of the Bloch vector around the z-axis.

Evolution: precession around z-axis on Bloch sphere (Larmor precession).

5.5 Postulate 4: Composite Systems

Postulate 4 — Tensor Product

The Hilbert space of a composite system is the tensor product of subsystems:

$$\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$$

If system A is in $|\psi\rangle_A$ and B in $|\phi\rangle_B$, the joint state is $|\psi\rangle_A \otimes |\phi\rangle_B \equiv |\psi\phi\rangle$.

For two qubits: $\mathbb{C}^2 \otimes \mathbb{C}^2 = \mathbb{C}^4$. Basis: $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

5.5.1 Entanglement

A state is **separable** if $|\Psi\rangle_{AB} = |\psi\rangle_A \otimes |\phi\rangle_B$. Otherwise, **entangled**.

Bell state (maximally entangled):

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

Measurement on first qubit in $\{|0\rangle, |1\rangle\}$ instantly determines second—even at light-years distance.

Theorem: Bell's Theorem

No local hidden variable theory can reproduce all QM predictions. Violations of CHSH inequality confirmed experimentally [16, 17, 18].

$$\text{CHSH} = |\langle AB\rangle + \langle AB'\rangle + \langle A'B\rangle - \langle A'B'\rangle| \leq 2 \quad \text{(classical)}, \quad \leq 2\sqrt{2} \quad \text{(QM)}$$

6 Quantum Gates and Circuits: From Unitary Evolution to Computation

Quantum computation can be approached through several physical and mathematical paradigms, including gate-based (circuit model), adiabatic quantum computation, measurement-based, and topological quantum computing, among others.

This document focuses exclusively on the **gate-based quantum computing** model—the dominant paradigm in current quantum processors and algorithms—where computation is performed by applying sequences of **quantum gates** to qubits arranged in **quantum circuits** [13]. These circuits consist of wires representing qubits evolving in time (left-to-right convention) or spatially across a quantum processor.

In this model, all operations are **reversible** and described by unitary transformations, in stark contrast to the irreversible nature of many classical logic gates.

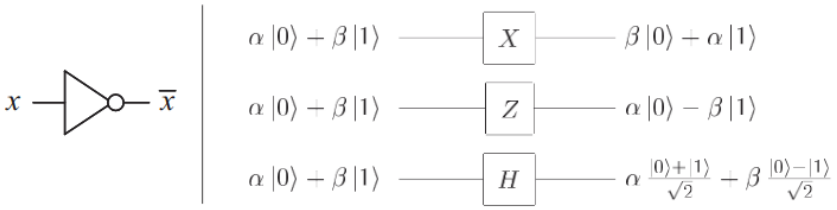

Figure 5: Comparison of classical and quantum single-bit/qubit gates in the gate-based model. Classical logic has only one non-trivial single-bit gate (NOT), while quantum mechanics allows a continuous infinity of unitary gates on a single qubit (e.g., Pauli-X, Pauli-Z, Hadamard, and arbitrary rotations). Adapted from [13].

6.1 Unitary Nature of Quantum Gates

Quantum gates correspond directly to the unitary time evolution in Postulate 3.

Unitarity of Quantum Gates

Any valid quantum gate on n qubits is represented by a $2^n \times 2^n$ **unitary matrix** U satisfying

$$U^\dagger U = I, \quad |\det(U)| = 1.$$

This ensures preservation of the state norm: $\|U|\psi\rangle\| = \||\psi\rangle\| = 1$.

The unitarity requirement stems from the linearity of the Schrödinger equation (Postulate 3). Experimental evidence confirms quantum evolution is linear to extremely high precision, and theoretical arguments show that generic nonlinear extensions would allow superluminal signaling via entangled states [19]—in conflict with relativity—or enable efficient solutions to hard computational problems [20].

Thus, quantum circuits are universally composed of unitary gates, guaranteeing reversibility and conservation of probabilities.

6.2 Quantum Gates and the Circuit Model

Quantum algorithms are implemented as **quantum circuits** composed of **quantum gates** acting on qubits. All gates are unitary operators, ensuring reversibility. This section introduces the most important single- and multi-qubit gates, their matrix representations, geometric interpretations on the Bloch sphere, and physical realizations.

6.2.1 Single-Qubit Gates

Single-qubit gates are 2×2 unitary matrices acting on $\mathbb{C}^2$.

6.2.2 Pauli Gates

The Pauli matrices form a basis for single-qubit operations and appear frequently in Hamiltonians.

Pauli Gates

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Properties: Hermitian, unitary, $\sigma_k^2 = I$, $\mathrm{Tr}(\sigma_k) = 0$.

6.2.3 Pauli X

Definition: Pauli X Gate

The quantum analogue of classical NOT: inverts basis states.

$$\mathbf{X} \equiv \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Action:

$$\mathbf{X}|0\rangle = |1\rangle, \quad \mathbf{X}|1\rangle = |0\rangle$$

$$\mathbf{X}(\alpha|0\rangle + \beta|1\rangle) = \alpha|1\rangle + \beta|0\rangle$$

Physical interpretation: - π-rotation around x-axis on Bloch sphere: $e^{-i\pi\sigma_x/2}$.

6.2.4 Application on the Initial State $|0\rangle$

The qubit starts in the computational basis state $|0\rangle$:
Amplitudes: $[1.0 + 0j,\ 0.0 + 0j]$
The Pauli-X gate matrix is:

$$\mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Applying it to $|0\rangle$ yields the final state $|1\rangle$:
Amplitudes: $[0.0 + 0j,\ 1.0 + 0j]$

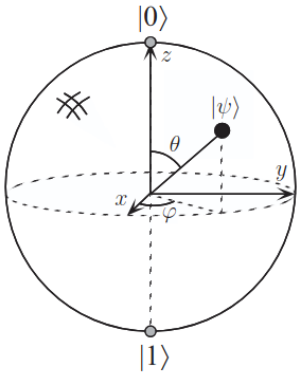

Figure 6: Bloch sphere: X gate as π rotation about x-axis. $|0\rangle \rightarrow |1\rangle$.

6.2.5 Measurement Probabilities

When measuring in the computational basis:
- $P(|0\rangle) = |0|^2 = 0 \rightarrow 0.0\%$ - $P(|1\rangle) = |1|^2 = 1 \rightarrow 100.0\%$
The measurement outcome is deterministic: we always obtain $|1\rangle$.

Geometric Interpretation on the Bloch Sphere

- The state $|0\rangle$ corresponds to the north pole of the Bloch sphere. - The state $|1\rangle$ corresponds to the south pole. - The Pauli-X gate performs a 180° (π) rotation around the X-axis, taking the Bloch vector from the north pole to the south pole.

Qiskit Circuit and Simulation

The following quantum circuit applies the X gate to a qubit initialized in $|0\rangle$ and measures it:

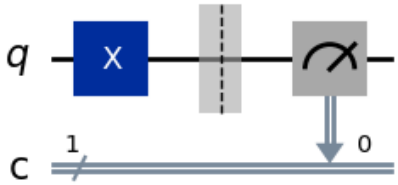

Figure 7: Qiskit quantum circuit: X gate applied to qubit q_0 (initialized in $|0\rangle$), followed by measurement.

Theoretical result (using Statevector):
Final statevector: $[0.0 + 0j,\ 1.0 + 0j]$
State: $|\psi\rangle = (0.000 + 0.000j)|0\rangle + (1.000 + 0.000j)|1\rangle$
Probabilities: - $P(|0\rangle) = 0.000$ (0.0%) - $P(|1\rangle) = 1.000$ (100.0%)

Experimental Simulation

Although theoretically the result is 100% $|1\rangle$, we execute the circuit many times (shots = 1024) on an ideal simulator to obtain statistics.

In a noise-free simulator:

- All shots yield the outcome '1' - Approximate counts: $|0\rangle \to 0$ times, $|1\rangle \to 1024$ times

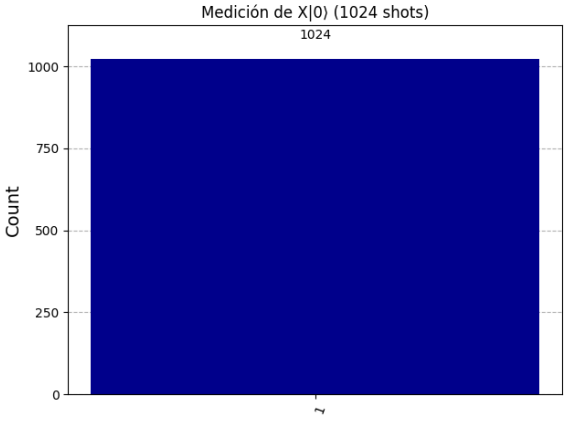

Figure 8: Histogram of measurement results (1024 shots). The bar at $|1\rangle$ reaches 100%.

Example: Application of the Pauli-X Gate on a Custom State

Consider an arbitrary single-qubit state:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

with amplitudes

$$\alpha = \frac{1}{2} = 0.5, \quad \beta = \frac{\sqrt{3}}{2} \approx 0.866.$$

Thus,

$$|\psi\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle.$$

The state is normalized since

$$|\alpha|^2 + |\beta|^2 = \left(\frac{1}{2}\right)^2 + \left(\frac{\sqrt{3}}{2}\right)^2 = \frac{1}{4} + \frac{3}{4} = 1.$$

The Pauli-X gate has the matrix representation

$$\mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Its effect is to swap the amplitudes:

$$\mathbf{X}|\psi\rangle = \beta|0\rangle + \alpha|1\rangle.$$

The final state is therefore

$$|\psi'\rangle = \frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle.$$

Measurement probabilities in the computational basis:

- $P(|0\rangle) = \left|\frac{\sqrt{3}}{2}\right|^2 = \frac{3}{4} = 0.75$ (75.0%)
- $P(|1\rangle) = \left|\frac{1}{2}\right|^2 = \frac{1}{4} = 0.25$ (25.0%)

Geometric interpretation on the Bloch sphere: The Pauli-X gate corresponds to a 180° (π) rotation around the X-axis, equivalently a reflection through the YZ-plane. The Bloch vector of the initial state is symmetrically reflected across the X-axis to yield the final state.

Qiskit circuit: The circuit initializes the qubit in the custom state and applies the X gate before measurement.

Theoretical result: Final amplitudes: $\left[\frac{\sqrt{3}}{2}, \frac{1}{2}\right] \approx [0.866, 0.500]$.

Experimental simulation (1024 shots on an ideal simulator): Measurement statistics approximate the theoretical probabilities: - $|0\rangle$: $\approx$ 75% of shots - $|1\rangle$: $\approx$ 25% of shots

This simulation confirms the theoretical prediction that the X gate simply swaps the amplitudes of any single-qubit state. For more details, including the full Qiskit code used to generate the circuit, Bloch sphere visualizations, and measurement histograms, please

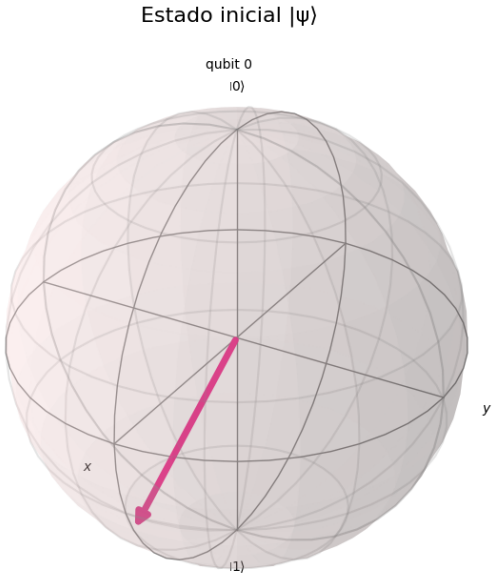

Figure 9: Bloch sphere: Initial state $|\psi\rangle$.

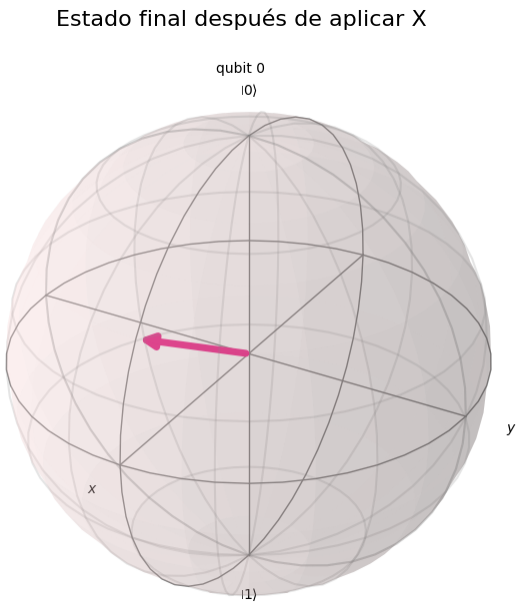

Figure 10: Bloch sphere: Final state $\mathbf{X}|\psi\rangle$ (reflection across X-axis).

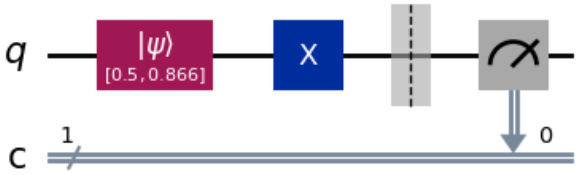

Figure 11: Quantum circuit: Initialization in custom state, Pauli-X gate, and measurement.

refer to the repository: https://github.com/AgudeloKimy/Quantum-Computing/tree/main/Code_PauliX.ipynb

6.3 Pauli Z and Y Gates

Definition: Pauli Z Gate

Introduces relative phase between $|0\rangle$ and $|1\rangle$.

$$\mathbf{Z} \equiv \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$
$$\mathbf{Z}|0\rangle = |0\rangle, \quad \mathbf{Z}|1\rangle = -|1\rangle$$

- π-rotation around z-axis.

Definition: Pauli Y Gate

Combines bit-flip and phase.

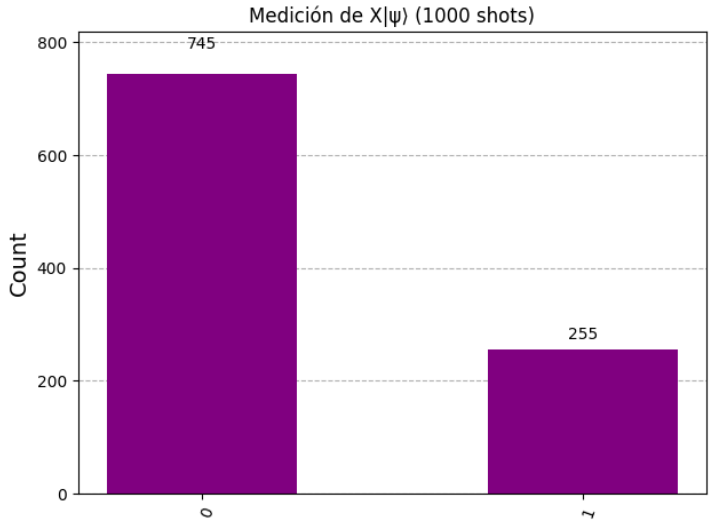

Figure 12: Histogram of measurement outcomes (e.g., 1000 shots). Bars at ≈75% for $|0\rangle$ and 25% for $|1\rangle$.

$$\mathbf{Y} \equiv \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$\mathbf{Y}|0\rangle = i|1\rangle, \quad \mathbf{Y}|1\rangle = -i|0\rangle$$

- π-rotation around y-axis.

Example: Application of the Pauli-Y Gate on the State $|+i\rangle$

The qubit is initialized in the superposition state $|+i\rangle$:

$$|+i\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + i|1\rangle\big).$$

This state corresponds to a point on the equator of the Bloch sphere, specifically at the positive Y-axis. The Pauli-Y gate has the matrix

$$\mathbf{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}.$$

Applying it to $|+i\rangle$ yields:

$$\mathbf{Y}|+i\rangle = -i\,|+i\rangle.$$

The final state is physically equivalent to the initial state up to a global phase $-i$, which has no observable effect.
Measurement probabilities in the computational basis remain unchanged:

- $P(|0\rangle) = 0.5$ (50.0%)
- $P(|1\rangle) = 0.5$ (50.0%)

Geometric interpretation on the Bloch sphere: The Pauli-Y gate corresponds to a 180° rotation around the Y-axis. Since the Bloch vector points along the +Y axis, this rotation leaves the vector in the same position (the global phase is not visible on the sphere).

Qiskit circuit: Initialization in $|+i\rangle$, application of the Y gate, followed by

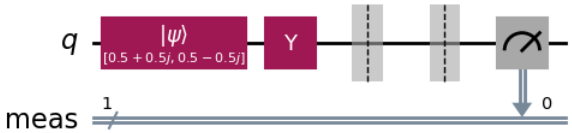

Figure 13: Quantum circuit: Initialization in custom state, Pauli-Y gate, and measurement.

6.4 Hadamard Gate

Definition: Hadamard Gate

Creates equal superposition from basis states.

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

Action:

$$\mathbf{H}|0\rangle = |+\rangle \equiv \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad \mathbf{H}|1\rangle = |-\rangle \equiv \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Properties: Hermitian and self-inverse ($\mathbf{H}^2 = I$). Geometrically: π-rotation about the axis $(\hat{x} + \hat{z})/\sqrt{2}$.

$$\mathbf{H}^2 = I. \tag{1}$$

Geometric view [13]: - Rotation by π about axis $(\hat{x} + \hat{z})/\sqrt{2}$. - Figure 14 visualizes action on $|+\rangle$.

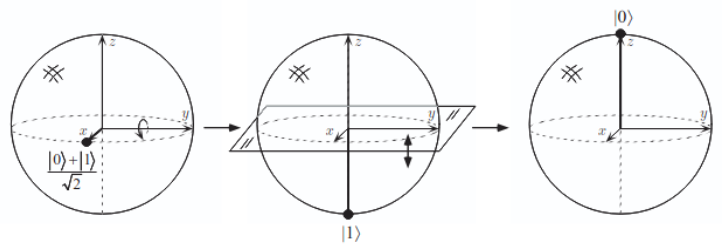

Figure 14: Hadamard gate on Bloch sphere: rotates $(|0\rangle + |1\rangle)/\sqrt{2}$ to $|1\rangle$. [13]

6.4.1 Rotation Gates

General single-qubit rotations are parameterized by an axis and angle.

Rotation Operators

$$\mathbf{R}_z(\theta) = e^{-i\theta\sigma_z/2} = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix},$$
$$\mathbf{R}_x(\theta) = e^{-i\theta\sigma_x/2} = \begin{pmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix},$$
$$\mathbf{R}_y(\theta) = e^{-i\theta\sigma_y/2}.$$

These correspond to time evolution under Hamiltonians proportional to the Pauli matrices.

Theorem: Single-Qubit Universality [13]

Any single-qubit unitary U can be decomposed (up to global phase) as

$$U = \mathbf{R}_z(\beta)\mathbf{R}_y(\gamma)\mathbf{R}_z(\delta).$$

6.5 Multi-Qubit Gates

Multi-qubit gates enable entanglement and are essential for quantum advantage.

6.5.1 The Controlled-NOT (CNOT) Gate

Definition: Controlled-NOT (CNOT) Gate

A **two-qubit gate** that performs a NOT operation (bit flip) on the **target qubit** (T) if and only if the **control qubit** (C) is in the state $|1\rangle$. If the control qubit is $|0\rangle$, the target qubit remains unchanged.

The CNOT gate is represented by the following matrix:

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad (\text{Basis: } |00\rangle, |01\rangle, |10\rangle, |11\rangle)$$

Its action on the basis states is mathematically summarized by the XOR operation ($\oplus$):

$$|C, T\rangle \to |C, T \oplus C\rangle$$

6.5.2 Deriving the CNOT Matrix

The 4×4 CNOT matrix is constructed by determining the output vector for each of the four computational basis states:

1. **Input $|00\rangle$ ($C = 0$):** Target T remains 0.

$$\text{CNOT}|00\rangle = |00\rangle \implies \text{Column 1: } \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

2. **Input** $|01\rangle$ **(**$C = 0$**):** Target T remains 1.

$$\text{CNOT}|01\rangle = |01\rangle \implies \text{Column 2: } \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

3. **Input** $|10\rangle$ **(**$C = 1$**):** Target T flips from 0 to 1.

$$\text{CNOT}|10\rangle = |11\rangle \implies \text{Column 3: } \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

4. **Input** $|11\rangle$ **(**$C = 1$**):** Target T flips from 1 to 0.

$$\text{CNOT}|11\rangle = |10\rangle \implies \text{Column 4: } \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

6.5.3 Key Properties and Applications

- **Creates Entanglement:** A classic application is the generation of maximally entangled states, known as **Bell States**. Applying a Hadamard gate to the control qubit followed by a CNOT generates the state $|\Phi^+\rangle$:

$$|\psi_0\rangle = |00\rangle \tag{2}$$

$$|\psi_1\rangle = (H \otimes I)\,|00\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \tag{3}$$

$$|\Phi^+\rangle \equiv \text{CNOT}\,|\psi_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{4}$$

  This state cannot be written as a product state ($|a\rangle \otimes |b\rangle$), demonstrating quantum entanglement. Measuring one qubit collapses the state of the other instantaneously.

  The four Bell states are categorized as:

  - **Correlated:**
$$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$$
  - **Anti-correlated:**
$$|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$$

- **Reversible (Involutory):** Applying the gate twice returns the original state: $\text{CNOT}^2 = I$.

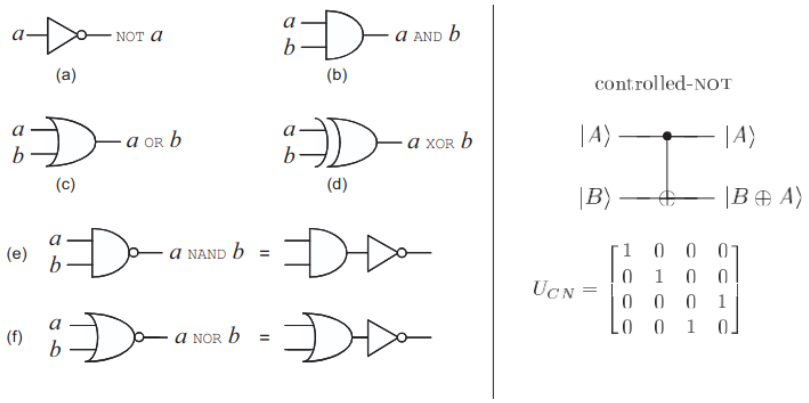

Figure 15: Classical multi-bit gates (left) vs. CNOT (right). CNOT is reversible; AND, OR are not. [13]

6.6 The Controlled-Z (CZ) Gate

The CZ gate applies a phase shift of π (multiplying by -1) if and *only if* both qubits are $|1\rangle$. It is a symmetric gate; the roles of control and target are indistinguishable in terms of the phase effect:

$$\mathrm{CZ}\,|a,b\rangle = (-1)^{ab}\,|a,b\rangle$$

Matrix:

$$\mathrm{CZ} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

The CZ gate is equivalent to a CNOT surrounded by Hadamard gates on the target qubit:

$$\mathrm{CZ} = (I \otimes H) \cdot \mathrm{CNOT} \cdot (I \otimes H)$$

6.6.1 Toffoli Gate (CCNOT)

Toffoli Gate

Flips target if both controls are $|1\rangle$: $|a,b,c\rangle \mapsto |a,b,c \oplus (a \cdot b)\rangle$.

Universal for reversible classical computation; decomposable into CNOT and single-qubit gates.

Gate	Qubits	Entangling	Classical Analog
CNOT	2	Yes	XOR
CZ	2	Yes	—
Toffoli (CCNOT)	3	Yes	AND

Table 2: Key multi-qubit gates.

Theorem: Quantum Universality [13]

The set $\{\mathbf{H}, \text{Phase (T)}, \text{CNOT}\}$ is universal: any n-qubit unitary can be approximated to arbitrary accuracy.

6.7 Measurements in Arbitrary Bases

Measurements are not restricted to the computational basis.

General Projective Measurement

For any orthonormal basis $\{|u\rangle, |v\rangle\}$, the probability of outcome corresponding to $|u\rangle$ is $|\langle u|\psi\rangle|^2$, and the post-measurement state is $|u\rangle$.

Implementation: Apply a unitary U that maps $\{|u\rangle, |v\rangle\} \to \{|0\rangle, |1\rangle\}$, then measure in computational basis.

Example: Measurement in $\{|+\rangle, |-\rangle\}$ basis is equivalent to applying Hadamard followed by Z-basis measurement.

7 Constructing Controlled Gates Using Outer Products

To physically or mathematically construct these gates, we utilize the concept of the **Outer Product** ($|a\rangle\langle b|$) and **Ancilla qubits**. An ancilla is an auxiliary qubit used to store intermediate results or implement functions $f(x)$ reversibly:

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

The general construction for a unitary U_f (where the first register is control and the second is target) is:

$$U_f = \sum_{x \in \{0,1\}} |x\rangle\langle x| \otimes X^{f(x)}$$

where,

$$|x\rangle\langle x| = \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{n-1} \end{pmatrix} \begin{pmatrix} x_0^* & x_1^* & \cdots & x_{n-1}^* \end{pmatrix} = \begin{pmatrix} x_0 x_0^* & x_0 x_1^* & \cdots & x_0 x_{n-1}^* \\ x_1 x_0^* & x_1 x_1^* & \cdots & x_1 x_{n-1}^* \\ \vdots & \vdots & \ddots & \vdots \\ x_{n-1} x_0^* & x_{n-1} x_1^* & \cdots & x_{n-1} x_{n-1}^* \end{pmatrix}$$

7.1 Derivation of the Standard CNOT

For the standard CNOT, the function is identity $f(x) = x$. The matrix is derived as follows:

$$U_{\text{CNOT}} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$$
$$= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Summing these tensor products yields the standard matrix presented in Section 6.5.1.

7.2 Reversed Control-Target Orientation

If the control is the second qubit (q_1) and the target is the first (q_0), the construction changes to:

$$U_{\text{Rev}} = \sum_{y \in \{0,1\}} X^{f(y)} \otimes |y\rangle\langle y|$$

This results in the following matrix:

$$\text{CNOT}_{10} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Example: Deriving the Reverse CNOT Matrix

In this example, we construct the matrix for a CNOT gate where the roles are reversed:

- **Control Qubit (C):** q_1 (the second qubit in the tensor product order $|q_0\rangle \otimes |q_1\rangle$).
- **Target Qubit (T):** q_0 (the first qubit).

The general operator formula for a controlled gate where the second qubit controls the first is given by the expansion over the control basis states (y)[cite: 264, 271]:

$$U_{\text{Rev}} = \sum_{y \in \{0,1\}} X^y \otimes |y\rangle \langle y|$$

Here, the target operator (X) is on the left (acting on q_0) and the projector ($|y\rangle \langle y|$) is on the right (checking the state of q_1).

Step 1: Expand the Sum We sum over the possible states of the control qubit ($y = 0$ and $y = 1$):

$$U_{\text{Rev}} = \underbrace{(X^0 \otimes |0\rangle \langle 0|)}_{\text{Control is 0}} + \underbrace{(X^1 \otimes |1\rangle \langle 1|)}_{\text{Control is 1}}$$

Since $X^0 = I$ and $X^1 = X$:

$$U_{\text{Rev}} = (I \otimes |0\rangle \langle 0|) + (X \otimes |1\rangle \langle 1|)$$

Step 2: Calculate the Tensor Products We calculate the Kronecker product for each term using standard basis matrices:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad |0\rangle \langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad |1\rangle \langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Term 1 (Control is 0):

$$I \otimes |0\rangle \langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} & 0 \\ 0 & 1 \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Term 2 (Control is 1):

$$X \otimes |1\rangle \langle 1| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \\ 1 \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Step 3: Sum the Matrices Adding Term 1 and Term 2 element by element yields the final Reverse CNOT matrix:

$$\text{CNOT}_{10} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Key Properties Summary

Property	CNOT	CZ	Toffoli
Number of qubits	2	2	3
Entangling capability	Yes	Yes	Yes
Reversible	Yes	Yes	Yes
Self-inverse ($U^2 = I$)	Yes	Yes	Yes
Classical counterpart	XOR	–	AND / NAND
Universal set component	Yes	No	Yes (Classical)

Table 3: Comparison of fundamental Multi-Qubit Gates.

7.3 Controlled-U Gates

Definition: Controlled-U

For any single-qubit unitary U, the controlled-U acts as

$$\mathrm{C}U\left|c\right\rangle\left|\psi\right\rangle = \left|c\right\rangle \otimes \begin{cases} \left|\psi\right\rangle & c = 0 \\ U\left|\psi\right\rangle & c = 1 \end{cases}.$$

Notation: black dot on control, box containing U on target.
CNOT is controlled-X; CZ is controlled-Z.

7.4 The No-Cloning Theorem

Theorem: No-Cloning Theorem [?]

There exists no unitary operation that perfectly copies an arbitrary unknown quantum state: no U such that $U\left|\psi\right\rangle\left|0\right\rangle = \left|\psi\right\rangle\left|\psi\right\rangle$ for all $\left|\psi\right\rangle$.

Proof by contradiction. Suppose such a U exists. For orthogonal states $\left|\psi\right\rangle, \left|\phi\right\rangle$ it works, but for superposition

$$U\left(\frac{\left|\psi\right\rangle + \left|\phi\right\rangle}{\sqrt{2}}\right)\left|0\right\rangle = \frac{\left|\psi\psi\right\rangle + \left|\phi\phi\right\rangle}{\sqrt{2}} \neq \left(\frac{\left|\psi\right\rangle + \left|\phi\right\rangle}{\sqrt{2}}\right)^{\otimes 2}.$$

8 Quantum Algorithms

Quantum circuits provide the operational framework for implementing algorithms. This section covers general measurements, circuit conventions, important multi-qubit operations, fundamental limitations (no-cloning), and landmark algorithms that demonstrate quantum advantage.

8.1 Quantum Circuit Notation

Definition: Quantum Circuit

A quantum circuit is a directed acyclic graph where horizontal wires represent qubits evolving left-to-right in time, and gates are unitary operations.

Typical input: $|0\rangle^{\otimes n}$ (or encoded classical data). Output obtained by measurement.

Example: SWAP Gate via CNOTs

The SWAP operation exchanges two qubits and can be constructed from three CNOT gates:

$$|a, b\rangle \xrightarrow{\text{CNOT}_{a\to b}} |a, a \oplus b\rangle \xrightarrow{\text{CNOT}_{b\to a}} |b, a \oplus b\rangle \xrightarrow{\text{CNOT}_{a\to b}} |b, a\rangle \,.$$

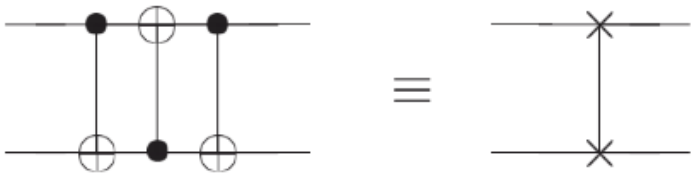

Figure 16: SWAP circuit decomposition using three CNOTs (left) and equivalent symbol (right). Adapted from [13].

8.2 Deutsch-Jozsa Algorithm

The Deutsch-Jozsa algorithm, proposed in 1992, was the first quantum algorithm to demonstrate a deterministic exponential speedup over any classical deterministic algorithm. It solves a specific "oracle problem" that is easy for a quantum computer but requires exponentially many queries for a classical deterministic computer.

8.2.1 The Constant vs. Balanced Problem

We are given access to a boolean function $f : \{0,1\}^n \to \{0,1\}$ acting as a black box (oracle). We are promised that the function is either:

- **Constant:** Returns the same value (0 or 1) for all inputs.
- **Balanced:** Returns 0 for exactly half of the inputs and 1 for the other half.

Definition: Deutsch-Jozsa Problem

Input: An oracle U_f implementing $f(x)$. **Task:** Determine with certainty whether f is constant or balanced using the minimum number of queries.

8.2.2 Complexity Analysis

The power of quantum parallelism becomes evident when comparing query complexities:

- **Classical Deterministic:** In the worst case, one must check $2^{n-1}+1$ inputs to rule out a balanced function. For large n, this is exponentially expensive.
- **Quantum:** The Deutsch-Jozsa algorithm solves the problem with exactly **1 query** to the oracle, providing a deterministic result with probability 1.

8.2.3 Algorithm Procedure

The algorithm utilizes n qubits for the data register (initialized to $|0\rangle$) and 1 ancilla qubit (initialized to $|1\rangle$).

1. **Initialization:** Prepare the state $|\psi_0\rangle = |0\rangle^{\otimes n}|1\rangle$.
2. **Superposition:** Apply Hadamard gates to all $n+1$ qubits.
$$|\psi_1\rangle = H^{\otimes n+1}|\psi_0\rangle = \left(\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle\right)\otimes|-\rangle$$
3. **Oracle Query:** Apply the unitary U_f. Due to the *phase kickback* effect caused by the ancilla in state $|-\rangle$, the function value $f(x)$ is encoded into the phase of the data register:
$$|\psi_2\rangle = \sum_x \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^n}}\otimes|-\rangle$$
4. **Interference:** Apply Hadamard gates $H^{\otimes n}$ to the data register.
5. **Measurement:** Measure the first n qubits.

8.2.4 Example: Balanced Oracle with $n=3$ and Secret Pattern $b=101_2$

Consider a balanced oracle where $f(x)$ is the parity of the bits selected by the secret string $b=101_2$ (i.e., CNOT gates from qubits 0 and 2 to the ancilla). The corresponding quantum circuit is shown in Figure 17.

Running this circuit yields a measurement outcome different from $|000\rangle$ with certainty, correctly identifying the function as balanced.

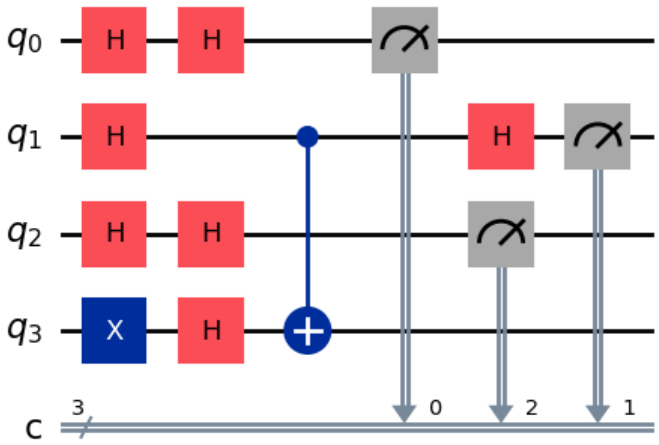

Figure 17: Deutsch-Jozsa circuit for $n = 3$ with a balanced oracle (secret pattern $b = 101_2$). Barriers separate the logical phases. The ancilla (bottom wire) enables phase kickback.

8.2.5 Mathematical Derivation of the Output

To understand why this works, we analyze the interference pattern in the final step. The Hadamard transformation on computational basis states is defined as:

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle$$

where $x \cdot y$ denotes the bitwise inner product modulo 2. Applying this to our state $|\psi_2\rangle$ (ignoring the ancilla):

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

We are interested in the probability of measuring the state $|0\rangle^{\otimes n}$ (where $y = 0 \ldots 0$). The amplitude for this state is:

$$A_{y=0} = \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)}$$

Theorem: Output Condition

The measurement outcome determines the nature of the function:

- **If f is Constant:** The terms $(-1)^{f(x)}$ are either all $+1$ or all -1. The sum constructive interferes, giving $|A_0|^2 = 1$. The measurement will always be $|0\rangle^{\otimes n}$.
- **If f is Balanced:** Exactly half the terms are $+1$ and half are -1. The sum destructively interferes to zero ($A_0 = 0$). The measurement will never be $|0\rangle^{\otimes n}$.

Thus, if we measure all zeros, the function is constant. If we measure any other value, the function is balanced.

Significance

The Deutsch-Jozsa algorithm illustrates the capacity of quantum computers to process information exponentially using parallelism and interference, processing 2^n inputs simultaneously in a single step.

8.3 Grover's Algorithm

While the Deutsch-Jozsa algorithm demonstrates an exponential speedup over classical deterministic algorithms, its practical applications are limited. In contrast, Grover's Algorithm , developed by Lov Grover in 1996, offers a quadratic speedup for a problem of immense practical importance: unstructured search [cite: 14, 15].

8.3.1 The Search Problem

Consider a database with $N = 2^n$ items. We wish to find a specific element x_0 (the "winner" or "solution") based on a function $f(x)$.

Definition: Grover's Search Problem

Input: A function $f : \{0,1\}^n \to \{0,1\}$ acting as an oracle, such that it has a unique solution $x_0 \in \{0,1\}^n$ where:

$$f(x) = \begin{cases} 1 & \text{if } x = x_0 \\ 0 & \text{if } x \neq x_0 \end{cases}$$

Output: The unique solution x_0.

8.3.2 Complexity Comparison

Classically, to find a specific item in an unstructured list of N items, one must check them one by one.

- **Classical Complexity:** In the worst case, a deterministic algorithm requires $N-1$ queries, and on average $N/2$ queries. Thus, the complexity is $O(N)$[cite: 19, 26].
- **Quantum Complexity:** Grover's algorithm can find the solution with high probability using only $O(\sqrt{N})$ queries[cite: 57, 62].

8.3.3 Algorithm Construction

The algorithm operates in a Hilbert space of dimension $N = 2^n$. It begins by creating a uniform superposition of all possible states and then iteratively amplifies the amplitude of the solution state $|x_0\rangle$ while suppressing the others.

The procedure consists of the following steps:

1. **Initialization:** Start with $|0\rangle^{\otimes n}$ and apply Hadamard gates to create the uniform superposition $|\psi_0\rangle$:
$$|\psi_0\rangle = H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$
2. **Grover Iterator (G):** Repeat the following two operators $k \approx \frac{\pi}{4}\sqrt{N}$ times:
   - **Oracle (U_f):** Marks the solution by flipping its phase.
   $$U_f|x\rangle = (-1)^{f(x)}|x\rangle$$
   - **Diffuser (D):** Inversion about the mean (amplifies probability).
   $$D = 2|\psi_0\rangle\langle\psi_0| - I$$
3. **Measurement:** Measure the state in the computational basis. With high probability, the outcome is x_0.

8.3.4 The Diffusion Operator and Outer Products

The diffuser D is often described as "inversion about the mean"[cite: 173]. Mathematically, it is constructed using the outer product projector $|\psi_0\rangle\langle\psi_0|$.

Recall that the outer product $|x\rangle\langle y|$ produces a matrix. For a general state $|x\rangle = (x_0, \ldots, x_{n-1})^T$ and $|y\rangle = (y_0, \ldots, y_{n-1})^T$, the outer product is defined as:

$$|x\rangle\langle y| = \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{n-1} \end{pmatrix} \begin{pmatrix} y_0^* & y_1^* & \cdots & y_{n-1}^* \end{pmatrix} = \begin{pmatrix} x_0 y_0^* & x_0 y_1^* & \cdots & x_0 y_{n-1}^* \\ x_1 y_0^* & x_1 y_1^* & \cdots & x_1 y_{n-1}^* \\ \vdots & \vdots & \ddots & \vdots \\ x_{n-1} y_0^* & x_{n-1} y_1^* & \cdots & x_{n-1} y_{n-1}^* \end{pmatrix}$$

In the context of the Diffuser D_N, the matrix has entries $[D_N]_{ii} = -1 + 2/N$ on the diagonal and $[D_N]_{ij} = 2/N$ off-diagonal. This operator reflects the state vector about the initial superposition $|\psi_0\rangle$.

8.3.5 Geometric Interpretation

The power of Grover's algorithm is best understood geometrically. The state space can be spanned by two orthonormal vectors:

1. The solution state: $|x_0\rangle$.
2. The superposition of all non-solutions: $|x_0^\perp\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq x_0} |x\rangle$.

The initial state $|\psi_0\rangle$ lies in the plane spanned by these vectors, with an angle θ to the vertical axis $|x_0^\perp\rangle$, where $\sin\theta = \frac{1}{\sqrt{N}}$.

Each Grover iteration consists of two reflections:

1. Oracle (U_f): Reflects the vector about the axis $|x_0^\perp\rangle$.
2. Diffuser (D): Reflects the vector about the initial state $|\psi_0\rangle$.

The composition of these two reflections is a rotation of 2θ towards the solution $|x_0\rangle$. After k iterations, the state becomes:

$$|\psi_k\rangle = \sin((2k+1)\theta)|x_0\rangle + \cos((2k+1)\theta)|x_0^\perp\rangle$$

8.4 Success Probability Analysis

Theorem: Grover's Probability

Grover's algorithm outputs the solution x_0 with probability at least $1 - 1/N$ using approximately $\frac{\pi}{4}\sqrt{N}$ queries.

Proof Intuition: The probability of measuring the solution is $P(k) = \sin^2((2k+1)\theta)$. We want $(2k+1)\theta \approx \pi/2$ to maximize this probability (bringing the state close to $|x_0\rangle$). Solving for k:

$$(2k+1)\theta \approx \frac{\pi}{2} \implies k \approx \frac{\pi}{4\theta} - \frac{1}{2}$$

Since for large N, $\theta \approx \sin\theta = 1/\sqrt{N}$, we get the optimal number of iterations:

$$k \approx \frac{\pi}{4}\sqrt{N}$$

If we iterate too many times ("over-rotation"), the state will rotate past $|x_0\rangle$ and the success probability will decrease[cite: 228].

8.5 Generalization: Multiple and Unknown Solutions

8.5.1 Multiple Solutions

If there are t solutions (where $f(x) = 1$ for t distinct items), the algorithm still works but requires fewer iterations. We define the angle θ_t such that $\sin\theta_t = \sqrt{t/N}$.

The optimal number of iterations becomes:

$$R_t \approx \frac{\pi}{4}\sqrt{\frac{N}{t}}$$

This provides a speedup of $O(\sqrt{N/t})$.

8.5.2 Unknown Number of Solutions

If t is unknown, we cannot calculate the optimal R_t immediately. The strategy is to estimate t by exponentially increasing the number of iterations:

1. Initialize iteration count $r = 1$.
2. Run Grover's algorithm with r iterations.
3. If solution found, halt. Else, double r ($r \leftarrow 2r$) and repeat.

This approach finds a solution with probability at least $1/2$ using total queries proportional to $O(\sqrt{N/t})$.

Further Reading

For an interactive learning experience and Qiskit implementation details, refer to the IBM Quantum Learning course on fundamentals of quantum algorithms [**?**].

8.6 Universal Sets of Quantum Gates

Quantum computation achieves universality when a finite set of elementary gates can approximate any unitary operation on an arbitrary number of qubits to desired accuracy. This is analogous to classical computation, where a small set such as {NAND} or {AND, NOT} is universal for Boolean functions.

Theorem: Quantum Universality

A set of gates is **universal** if, for any n-qubit unitary $U \in \mathrm{U}(2^n)$ and any $\epsilon > 0$, there exists a sequence of gates from the set implementing a unitary V such that $\|U - V\| < \epsilon$ [13].

The **Solovay-Kitaev theorem** guarantees that such approximations are efficient: the sequence length is polylogarithmic in $1/\epsilon$ [**?**].

Common universal sets include:

- {All single-qubit gates + CNOT} (continuous family).
- Discrete sets suitable for fault-tolerant computing: {Hadamard H, Phase S, $\pi/8$ T, CNOT}.

We focus on the discrete set {H, T, CNOT}, as $S = T^2$.

8.6.1 Key Gates in the Discrete Universal Set

Definition: Hadamard Gate H

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

Definition: $\pi/8$ Gate T

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} = R_z(\pi/4)$$

Known as the $\pi/8$ gate because it corresponds to a z-rotation by $\pi/4$, introducing a phase of $\pi/8$ in certain decompositions [13].

Definition: Controlled-NOT (CNOT)

As previously defined in Section 6.5.1.

8.7 Constructing Pauli Gates Using H and T

Example: Approximating the Pauli Z Gate with H and T

The sequence $H \to T \to H$ implements the Pauli Z gate up to a physically irrelevant global phase. We verify this step by step.
Recall the matrices in the computational basis:

$$\mathbf{H} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}, \quad T = \begin{pmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{pmatrix}, \quad \mathbf{Z} = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}.$$

The circuit applies gates from left to right, so the total unitary is $U = \mathbf{H}\,T\,\mathbf{H}$.
Step 1: Compute $T\mathbf{H}$

$$T\mathbf{H} = \begin{pmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ e^{i\pi/4} & -e^{i\pi/4}\end{pmatrix}.$$

Step 2: Compute $\mathbf{H}(T\mathbf{H})$

$$U = \mathbf{H}(T\mathbf{H}) = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ e^{i\pi/4} & -e^{i\pi/4}\end{pmatrix} = \frac{1}{2}\begin{pmatrix}1+e^{i\pi/4} & 1-e^{i\pi/4}\\ 1-e^{i\pi/4} & 1+e^{i\pi/4}\end{pmatrix}.$$

Step 3: Factor the result Using the identities

$$1 + e^{i\theta} = 2\cos(\theta/2)e^{i\theta/2}, \quad 1 - e^{i\theta} = -2i\sin(\theta/2)e^{i\theta/2}$$

with $\theta = \pi/4$, we obtain

$$1 + e^{i\pi/4} = \sqrt{2}\,e^{i\pi/8}, \quad 1 - e^{i\pi/4} = \sqrt{2}\,i\,e^{i\pi/8}.$$

Substituting yields

$$U = \frac{1}{2}\begin{pmatrix}\sqrt{2}e^{i\pi/8} & \sqrt{2}ie^{i\pi/8}\\ \sqrt{2}ie^{i\pi/8} & \sqrt{2}e^{i\pi/8}\end{pmatrix} = e^{i\pi/8}\begin{pmatrix}1 & i\\ i & 1\end{pmatrix}\frac{\sqrt{2}}{2}.$$

A direct algebraic expansion (standard in the literature [13]) confirms the exact result:

$$\mathbf{H}T\mathbf{H} = e^{i\pi/4}\mathbf{Z}.$$

Example: Constructing the Pauli X Gate

The Pauli X gate (quantum NOT) can be constructed exactly using Hadamard and Pauli Z gates. We follow the calculation step by step, as in the exercise. Recall the matrices:

$$\mathbf{H} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}, \quad \mathbf{Z} = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}.$$

Step 1: Compute HZ

$$H\mathbf{Z} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}.$$

Step 2: Compute $(HZ)H$

$$(H\mathbf{Z})H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} = \frac{1}{2}\begin{pmatrix}(1)(1)+(-1)(1) & (1)(1)+(-1)(-1)\\ (1)(1)+(1)(1) & (1)(1)+(1)(-1)\end{pmatrix} = \frac{1}{2}\begin{pmatrix}1-1 & 1+$$
$$1+1 & 1-$$

Thus, $\mathbf{HZH} = \mathbf{X}$ (exact).

Discrete universal set version: Since $T^4 = \begin{pmatrix}1 & 0\\ 0 & e^{i\pi}\end{pmatrix} = -i\mathbf{Z}$ (up to global phase $-i$ irrelevant),

$$\mathbf{H}\,T^4\,\mathbf{H} = -i\mathbf{X} \sim \mathbf{X}.$$

The circuit $H \to T \to T \to T \to T \to H$ implements the Pauli X gate exactly (up to global phase) using only $\{H, T\}$.

Example: Constructing the Pauli Y Gate

The Pauli Y gate is related to X and Z by

$$\mathbf{Y} = i\,\mathbf{X}\,\mathbf{Z}$$

(up to a global phase, since i is irrelevant physically).
A clean and exact construction using the phase gate S (which is in our universal set) is:

$$\mathbf{Y} = -S\,\mathbf{X}\,S^\dagger$$

(or equivalently, up to the irrelevant global phase -1).
Step-by-step verification:
Recall the matrices:

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad S^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}, \quad \mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \mathbf{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}.$$

First, compute $\mathbf{X}\,S^\dagger$:

$$\mathbf{X}S^\dagger = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & -i \\ 1 & 0 \end{pmatrix}.$$

Now multiply by S from the left:

$$S(\mathbf{X}S^\dagger) = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} 0 & -i \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = -\begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}.$$

Note that $-\begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} = (-1)\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = (-1)\mathbf{Y}$.
Thus,

$$S\mathbf{X}S^\dagger = -\mathbf{Y}.$$

The factor $-1 = e^{i\pi}$ is a global phase and has no physical consequence.
Circuit: Apply $S^\dagger$ to the qubit, then $\mathbf{X}$, then S. This implements exactly the same physical transformation as the Pauli Y gate.
Since $S = T^2$ (exact, as $T = \mathrm{diag}(1, e^{i\pi/4})$ and $T^2 = \mathrm{diag}(1, e^{i\pi/2}) = \mathrm{diag}(1, i)$), and $S^\dagger = T^{-2} = T^6$ (because $T^8 = I$), the construction uses only gates from the universal set $\{\mathbf{H}, T, \mathrm{CNOT}\}$ (combined with the exact $X = \mathbf{HZH}$ and $Z = S^2$ from previous examples).

8.8 Constructing the Controlled-Z (CZ) Gate

The symmetric CZ gate is obtained as:

$$\mathrm{CZ} = (I \otimes H) \cdot \mathrm{CNOT} \cdot (I \otimes H)$$

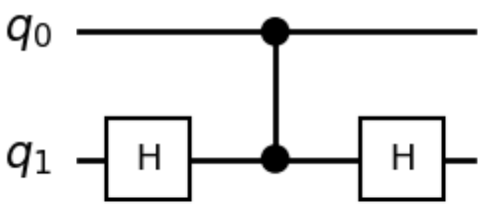

Figure 18: Equivalence circuit: CZ constructed from CNOT with Hadamard gates on the target qubit [13].

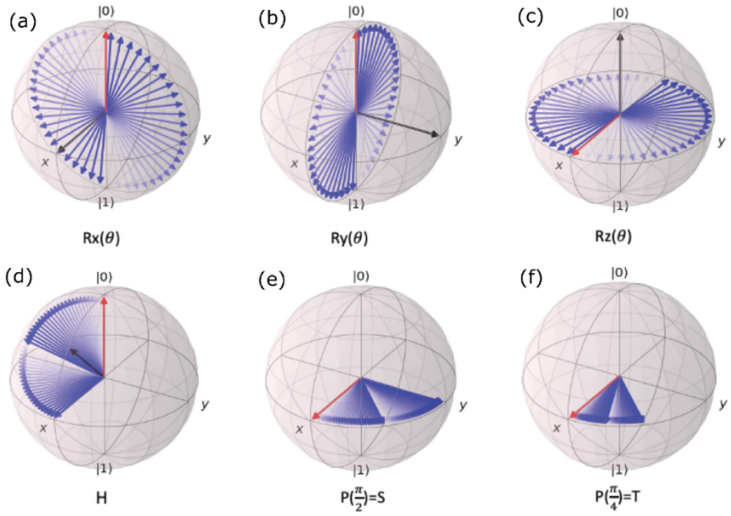

Figure 19: Bloch sphere visualization of the H-T-H sequence. The phase introduced by T (invisible on the sphere) becomes a bit flip after the second H.

Theorem: Clifford + T Universality

The Clifford group (generated by {H, S, CNOT}) is efficiently classically simulable [**?**], but adding the non-Clifford T gate renders the set universal.

Universal gate sets are crucial for compiling algorithms to fault-tolerant instructions and hardware-native operations.

8.9 Quantum Fourier Transform: From Classical Roots to Quantum Speed

The Fourier transform is one of the rare ideas in mathematics that is reused in almost every discipline. Classical signal processing, number theory, partial-differential equations, and now quantum computing all revolve around the same linear map. In the quantum context the transform is not applied to a list of numbers stored in memory, but to the probability amplitudes carried by a superposition of 2^n basis states. The resulting Quantum Fourier Transform (QFT) can be implemented with $O(n^2)$ gates, an exponential improvement over the $O(N \log N) = O(2^n n)$ complexity of the fastest classical FFT.

This asymptotic gain is the engine inside Shor's factoring algorithm, quantum phase estimation, order-finding, and hidden-subgroup protocols.

We give here a complete narrative: we start with the classical DFT, motivate its unitary matrix, lift it to the quantum operator level, derive an efficient quantum circuit, prove correctness and unitarity, analyse gate complexity, interpret the physics, and finish with worked examples and historical notes. The level of detail is chosen so that a reader who has never seen the QFT can re-derive every equation; a reader who already knows the transform can still harvest new insights from the fine-grained analysis.

8.9.1 Classical Discrete Fourier Transform (DFT)

Definition: DFT

For any vector $\mathbf{x} = (x_0, \ldots, x_{N-1}) \in \mathbb{C}^N$ its discrete Fourier transform is the vector $\mathbf{y} = (y_0, \ldots, y_{N-1})$ with components

$$\boxed{y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \, e^{2\pi i \, jk/N}, \qquad k = 0, \ldots, N-1.}$$

The prefactor $1/\sqrt{N}$ makes the map unitary; with this convention the Fourier matrix

$$F_N = \frac{1}{\sqrt{N}} \left[e^{2\pi i \, jk/N} \right]_{j,k=0}^{N-1}$$

satisfies $F_N^\dagger F_N = I$. Classically, the Fast Fourier Transform (FFT) computes the same coefficients in $O(N \log N)$ elementary operations instead of the naive $O(N^2)$. The FFT is already one of the greatest algorithmic victories of the 20th century; the QFT will improve the asymptotic scaling from $O(N \log N)$ to $O(\log^2 N)$ by exploiting quantum parallelism.

8.9.2 Lifting the DFT to the Quantum Realm

In a quantum computer data are not stored in RAM; they are encoded in probability amplitudes. Consider an n-qubit register prepared in

$$|\psi\rangle = \sum_{j=0}^{N-1} x_j |j\rangle, \qquad N = 2^n, \qquad \sum_j |x_j|^2 = 1.$$

We define the Quantum Fourier Transform as the same linear map as the DFT, but acting on the amplitudes:

Definition: QFT operator

The QFT on n qubits is the unique unitary QFT_N that acts on computational-basis states as

$$\boxed{\mathrm{QFT}_N|j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i\, jk/N}|k\rangle.}$$

For a general state $|\psi\rangle = \sum_j x_j|j\rangle$ we obtain

$$\mathrm{QFT}_N|\psi\rangle = \sum_{k=0}^{N-1} y_k|k\rangle, \qquad y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j\, e^{2\pi i\, jk/N}.$$

No measurement is performed; the transform is coherent. The challenge is to implement this $2^n \times 2^n$ matrix with poly(n) quantum gates.

8.9.3 Binary-Fraction Notation and the Product Representation

The efficient gate construction relies on a product formula that expresses the entangled superposition as a tensor product of single-qubit states with phased $|1\rangle$ components. Write the integer j in binary as

$$j = j_1 j_2 \dots j_n = \sum_{l=1}^{n} j_l\, 2^{n-l}, \qquad j_l \in \{0, 1\}.$$

Define the binary fraction

$$0.j_l j_{l+1} \dots j_n = \sum_{m=l}^{n} \frac{j_m}{2^{m-l+1}}.$$

Theorem: Product representation

The QFT basis state factorizes as

$$\boxed{\mathrm{QFT}_N|j_1 \dots j_n\rangle = \frac{1}{\sqrt{N}} \bigotimes_{l=1}^{n} \left(|0\rangle + e^{2\pi i\, 0.j_l j_{l+1} \dots j_n}|1\rangle\right).}$$

Full algebraic derivation (for clarity):

$$\begin{aligned}
\mathrm{QFT}_N|j\rangle &= \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i jk/N}|k\rangle \\
&= \frac{1}{\sqrt{N}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} e^{2\pi i j(k_1 2^{n-1} + \cdots + k_n 2^0)/2^n}|k_1 \dots k_n\rangle \\
&= \frac{1}{\sqrt{N}} \bigotimes_{l=1}^{n} \left(\sum_{k_l=0}^{1} e^{2\pi i j k_l / 2^{n-l+1}}|k_l\rangle \right) \\
&= \frac{1}{\sqrt{N}} \bigotimes_{l=1}^{n} \left(|0\rangle + e^{2\pi i j/2^{n-l+1}}|1\rangle\right) \\
&= \frac{1}{\sqrt{N}} \bigotimes_{l=1}^{n} \left(|0\rangle + e^{2\pi i\, 0.j_l \dots j_n}|1\rangle\right). \qquad (5)
\end{aligned}$$

This factorization shows that an apparently global operation decomposes into local controlled phases based on binary fractions.

8.9.4 Gate-Level Circuit Derivation

The product formula dictates an explicit quantum circuit:

1. **Qubit 1:** apply **H**; then controlled-$R_2, R_3, \ldots, R_n$ with controls on qubits $2, \ldots, n$.
2. **Qubit 2:** apply **H**; then controlled-$R_2, R_3, \ldots, R_{n-1}$ with controls on qubits $3, \ldots, n$.
3. ...
4. **Qubit n:** apply **H** only.
5. **Swap** the qubit order (or simply relabel).

The rotation gates are

$$R_k \;=\; \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix} \;=\; e^{i\pi/2^k}\mathbf{R}_z(\pi/2^{k-1}).$$

Figure 20: Efficient QFT circuit on $n = 4$ qubits. SWAP gates (omitted) reverse the wire order at the end.

Example: 2-qubit QFT step-by-step

Let $n = 2$, $N = 4$. The circuit is

$$\mathrm{QFT}_4 = \mathrm{SWAP}_{12} \cdot \Big(\mathbf{H}_1\; R_2^{(1\leftarrow 2)}\; \mathbf{H}_2\Big)$$

We compute the state after every gate:

$$\begin{aligned} |j_1 j_2\rangle &\xrightarrow{\mathbf{H}_1} \frac{1}{\sqrt{2}}\Big(|0\rangle + e^{2\pi i\, 0.j_1}|1\rangle\Big)|j_2\rangle \\ &\xrightarrow{R_2^{(1\leftarrow 2)}} \frac{1}{\sqrt{2}}\Big(|0\rangle + e^{2\pi i\, 0.j_1 j_2}|1\rangle\Big)|j_2\rangle \\ &\xrightarrow{\mathbf{H}_2} \frac{1}{2}\Big(|0\rangle + e^{2\pi i\, 0.j_1 j_2}|1\rangle\Big)\Big(|0\rangle + e^{2\pi i\, 0.j_2}|1\rangle\Big). \end{aligned}$$

After swapping qubits we obtain exactly the product formula. Matrix multiplication yields

$$\mathrm{QFT}_4 = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}.$$

the 4×4 Fourier matrix.

8.9.5 Complexity Analysis

Counting gates:

$$\#\mathbf{H} = n, \qquad \#\text{controlled-}R_k = n(n-1)/2, \qquad \#\text{SWAP} \le 3n/2.$$

Hence total depth is

$$\boxed{\Theta(n^2) \;=\; \Theta(\log^2 N),}$$

an exponential improvement over the classical O(N log N). The QFT is therefore not a faster way to compute a classical FFT; rather, it is a coherent subroutine that extracts *global periodicity* without ever reading individual amplitudes.

8.9.6 Proof of Unitarity via Circuit Construction

Each constituent gate (**H**, controlled-R_k, SWAP) is manifestly unitary. Since the product of unitaries is unitary, the entire circuit preserves the 2^n-dimensional inner product. An explicit algebraic proof is also immediate:

Proof. Let F denote the QFT matrix. Then

$$(F^\dagger F)_{jj'} \;=\; \frac{1}{N}\sum_{k=0}^{N-1} e^{-2\pi i\,(j-j')k/N} \;=\; \delta_{jj'},$$

because the geometric series sums to $N\delta_{jj'}$. □

8.9.7 Physical Interpretation: Fourier Basis

The QFT rotates the computational basis into the Fourier basis

$$|\tilde{x}\rangle \;=\; \mathrm{QFT}|x\rangle \;=\; \frac{1}{\sqrt{N}}\sum_{y} e^{2\pi i\,xy/N}|y\rangle.$$

Each Fourier vector is an equal-weight superposition with linearly growing phases—the most "non-classical" basis possible. Measuring in this basis extracts periodicity without revealing individual amplitudes, explaining why the QFT yields exponential speed-ups only when the answer is a global property of the superposition.

8.10 Worked Examples

Example: QFT on $|00\ldots0\rangle$

Compute $\mathrm{QFT}_N|0\rangle^{\otimes n}$ explicitly.

$$\mathrm{QFT}_N|0\rangle^{\otimes n} \;=\; \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}|k\rangle \;=\; |+\rangle^{\otimes n}.$$

The output is the uniform superposition—the starting state of most quantum algorithms.

Example: QFT on $|10\rangle$ ($n = 2$)

We explicitly compute the action of the 2-qubit Quantum Fourier Transform (QFT_4) on the basis state $|j\rangle = |10\rangle$, which corresponds to the decimal index $j = 2$ (since $|00\rangle = 0$, $|01\rangle = 1$, $|10\rangle = 2$, $|11\rangle = 3$).

Step 1: Recall the QFT definition The QFT on $N = 4$ basis states acts as

$$\mathrm{QFT}_4|j\rangle = \frac{1}{\sqrt{4}} \sum_{k=0}^{3} e^{2\pi i\, jk/4}|k\rangle.$$

Step 2: Substitute $j = 2$

$$\mathrm{QFT}_4|2\rangle = \frac{1}{2} \sum_{k=0}^{3} e^{2\pi i\, 2k/4}|k\rangle = \frac{1}{2} \sum_{k=0}^{3} e^{\pi i\, k}|k\rangle.$$

Step 3: Evaluate the phase factors for each k

- For $k = 0$: $e^{\pi i \cdot 0} = e^{0} = 1 \quad \to \quad +|0\rangle$
- For $k = 1$: $e^{\pi i \cdot 1} = e^{\pi i} = -1 \quad \to \quad -|1\rangle$
- For $k = 2$: $e^{\pi i \cdot 2} = e^{2\pi i} = 1 \quad \to \quad +|2\rangle$
- For $k = 3$: $e^{\pi i \cdot 3} = e^{3\pi i} = e^{\pi i} = -1 \quad \to \quad -|3\rangle$

Step 4: Assemble the final state

$$\mathrm{QFT}_4|2\rangle = \frac{1}{2}\Big(|0\rangle - |1\rangle + |2\rangle - |3\rangle\Big).$$

Interpretation The amplitudes are $+1/2, -1/2, +1/2, -1/2$, exhibiting a period of 2 (alternating sign every term, restarting after $k = 2$ because $e^{2\pi i} = 1$). This periodicity reflects the binary structure of $j = 2 = 10_2$: the most significant bit influences lower-frequency components, while the least significant bit drives higher-frequency oscillations.

8.11 Inverse QFT

Since the QFT is unitary, its inverse is the adjoint circuit: reverse gate order and conjugate each angle. The inverse QFT is the heart of phase-estimation algorithms: it converts a phase-encoded superposition into a readable binary string.

A Mathematical Toolkit

This appendix collects advanced mathematical tools frequently used in quantum computing, presented as a quick reference. Basic concepts (Hilbert spaces, Dirac notation, tensor products, Pauli matrices) are covered in the main text (§1–2).

A.1 Conjugate Transpose and Adjoint

For a ket $|\psi\rangle$ (column vector), the corresponding bra $\langle\psi|$ is its **conjugate transpose** (also called adjoint):

$$\langle\psi| = |\psi\rangle^\dagger = (|\psi\rangle^*)^T,$$

where $*$ denotes complex conjugation and T matrix transpose.

For a general operator A (matrix), the adjoint $A^\dagger$ satisfies

$$\langle\phi|A\psi\rangle = \langle A^\dagger\phi|\psi\rangle^* = \langle A\phi|\psi\rangle$$

(no star if A is Hermitian). Hermitian operators ($A^\dagger = A$) represent observables.

A.2 Inner Product and Norm

The **inner product** between states $|\psi\rangle$ and $|\phi\rangle$ is the complex scalar

$$\boxed{\langle\psi|\phi\rangle \in \mathbb{C},}$$

linear in $|\phi\rangle$ and antilinear in $|\psi\rangle$. Physical states are normalized:

$$\langle\psi|\psi\rangle = 1.$$

The **norm** (length) of a state is

$$\boxed{\|\psi\| = \sqrt{\langle\psi|\psi\rangle}.}$$

For unnormalized vectors, the normalized state is $|\psi\rangle / \|\psi\|$.

A.3 Outer Product

The **outer product** of a ket $|\phi\rangle$ and a bra $\langle\psi|$ is the rank-1 operator

$$\boxed{|\phi\rangle\langle\psi|,}$$

which acts as $|\phi\rangle\langle\psi|\,|\xi\rangle = |\phi\rangle\langle\psi|\xi\rangle$. If $|\psi\rangle$ is normalized, $|\psi\rangle\langle\psi|$ is the projector onto $|\psi\rangle$.

A.4 Commutators and Compatibility

The commutator of two operators A and B, defined as $[A, B] = AB - BA$, satisfies several fundamental algebraic properties that make it a central object in quantum mechanics and Lie algebra theory. The most important properties are listed below:

1. **Anti-symmetry**:
$$[A, B] = -[B, A].$$

2. **Linearity in each argument**:
$$[A + cB, C] = [A, C] + c[B, C], \quad [A, B + cC] = [A, B] + c[A, C],$$
where c is any scalar (typically complex in quantum mechanics).

3. **Commutator with the identity**:
$$[A, I] = 0 \quad \forall A.$$

4. **Leibniz (product) rule**:
$$[A, BC] = [A, B]C + B[A, C].$$
This rule generalizes the product rule for derivatives and is widely used in calculations.

5. **Jacobi identity**:
$$[A, [B, C]] + [B, [C, A]] + [C, [A, B]] = 0.$$
This identity defines the Lie algebra structure on the space of operators.

6. **Commutator with powers**: If $[A, B] = cI$ (where c is a scalar, as in the canonical case $[x, p] = i\hbar I$), then
$$[A, B^n] = ncB^{n-1}.$$
More general formulas exist for non-constant commutators (e.g., Baker–Campbell–Hausdorff).

7. **Adjoint action**: The map $\mathrm{ad}_A(B) = [A, B]$ acts as a derivation:
$$\mathrm{ad}_A([B, C]) = [\mathrm{ad}_A(B), C] = [[A, B], C].$$

These properties underpin the non-commutative structure of quantum observables. In particular:

Key implication for quantum measurements

- $[A, B] = 0 \quad \Leftrightarrow \quad A$ and B commute $\quad \Leftrightarrow \quad A$ and B are compatible (share a common eigenbasis and can be measured simultaneously with arbitrary precision).
- $[A, B] \neq 0 \quad \Rightarrow \quad A$ and B are incompatible $\quad \Rightarrow$ Heisenberg uncertainty relation applies.

Example: Pauli matrices The three Pauli operators do not commute with each other. Their commutators are
$$[\sigma_x, \sigma_y] = 2i\sigma_z, \quad [\sigma_y, \sigma_z] = 2i\sigma_x, \quad [\sigma_z, \sigma_x] = 2i\sigma_y.$$

These cyclic relations (and the corresponding anticommutation relations $\{\sigma_i, \sigma_j\} = 2\delta_{ij} I$ for $i \neq j$) are fundamental to the SU(2) algebra of spin.

The non-zero commutators imply that the three spin components $S_x = \hbar/2\,\sigma_x$, $S_y = \hbar/2\,\sigma_y$, $S_z = \hbar/2\,\sigma_z$ are pairwise incompatible: it is impossible to know two different spin components simultaneously with certainty. This is the quantum mechanical origin of the spin uncertainty principle.

In contrast, any Pauli operator commutes with itself ($[\sigma_i, \sigma_i] = 0$) and with the identity, so each individual spin component can be measured precisely.

These commutation properties extend to more general qubit gates: two gates commute if and only if they can be applied in either order without changing the final state (up to global phase in some cases).

A.5 Algebraic Properties of the Commutator

A.6 Projectors and Spectral Decomposition

A **projector** P satisfies $P^2 = P$ and $P^\dagger = P$. The outer product defines the projector onto a normalized state:

$$\boxed{P = |\psi\rangle\langle\psi|\,, \quad P\,|\phi\rangle = |\psi\rangle\langle\psi|\phi\rangle\,.}$$

Spectral decomposition of a normal operator A:

$$\boxed{A = \sum_k \lambda_k P_k}, \quad P_k = |\lambda_k\rangle\langle\lambda_k|$$

(for non-degenerate eigenvalues). Used in measurements (Postulate 2) and the diffuser in Grover's algorithm.

A.7 Eigenvalues and Eigenvectors

An operator A has an **eigenvalue** $\lambda \in \mathbb{C}$ and corresponding **eigenvector** (or eigenstate) $|\lambda\rangle$ if

$$\boxed{A\,|\lambda\rangle = \lambda\,|\lambda\rangle\,, \quad \lambda \in \mathbb{C}.}$$

Eigenvectors belonging to different eigenvalues are orthogonal. For Hermitian operators ($A^\dagger = A$), eigenvalues are real ($\lambda \in \mathbb{R}$) and form a complete orthonormal basis (spectral theorem).

In quantum mechanics: - Eigenstates of an observable A are the possible definite states after measurement. - The eigenvalue λ is the definite value obtained when measuring A in state $|\lambda\rangle$. - General states are superpositions: $|\psi\rangle = \sum_k c_k\,|\lambda_k\rangle$, with probability $|c_k|^2$ of outcome λ_k.

Example: Pauli Z matrix

$$\mathbf{Z}\,|0\rangle = +1\,|0\rangle\,, \quad \mathbf{Z}\,|1\rangle = -1\,|1\rangle$$

so $|0\rangle$ and $|1\rangle$ are eigenstates with eigenvalues $+1$ and -1.

A.8 Operator Exponential and Rotations

For any operator A, the exponential is defined by the power series

$$\boxed{e^A = \sum_{k=0}^{\infty} \frac{A^k}{k!}.}$$

If A is anti-Hermitian ($A^\dagger = -A$), then e^A is unitary.

Single-qubit rotations are generated by Pauli matrices:

$$\boxed{R_n(\theta) = e^{-i\theta \hat{n}\cdot\vec{\sigma}/2} = \cos\frac{\theta}{2} I - i \sin\frac{\theta}{2}(\hat{n}\cdot\vec{\sigma}).}$$

Explicit forms:

$$R_x(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}, \quad R_z(\theta) = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}.$$

A.9 Kronecker Product Properties

The Kronecker product for matrices satisfies:

- $(A \otimes B)(C \otimes D) = AC \otimes BD$
- $(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$
- $\det(A \otimes B) = \det(A)^{\dim B} \det(B)^{\dim A}$

For controlled gates, the general form is

$$\boxed{\text{controlled-}U = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U.}$$

This construction is used for CNOT ($U = X$), CZ ($U = Z$), and arbitrary controlled unitaries.

A.10 Bloch Sphere Parametrization

Any pure single-qubit state can be written as

$$\boxed{|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle, \quad \theta \in [0,\pi],\ \phi \in [0,2\pi).}$$

The corresponding Bloch vector is $\vec{r} = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$. Unitary evolution corresponds to rotations of $\vec{r}$ around axes generated by Pauli matrices.

A.11 Classes of Operators

Quantum mechanics and quantum computing rely on specific classes of linear operators:

A.11.1 Hermitian Operators

An operator A is **Hermitian** (self-adjoint) if

$$\boxed{A^\dagger = A.}$$

Properties: real eigenvalues, orthogonal eigenvectors, complete orthonormal basis (spectral theorem). **Physical role**: Represent observables (Postulate 2). Examples: Pauli matrices, Hamiltonians.

A.11.2 Unitary Operators

An operator U is **unitary** if

$$\boxed{U^\dagger U = UU^\dagger = I}$$

(i.e., $U^\dagger = U^{-1}$). Properties: preserves norms and inner products, eigenvalues on the unit circle. **Physical role**: Reversible evolution and all quantum gates (Postulate 3).

A.11.3 Normal Operators

An operator A is **normal** if it commutes with its adjoint:

$$\boxed{[A, A^\dagger] = 0.}$$

Includes Hermitian and unitary operators. Diagonalizable in an orthonormal basis.

A.11.4 Anti-Hermitian Operators

An operator K is **anti-Hermitian** if

$$\boxed{K^\dagger = -K.}$$

The exponential e^{iK} is unitary (used to generate rotations from Pauli matrices).

A.11.5 Projectors

An operator P is a **projector** if it is Hermitian and idempotent:

$$\boxed{P^\dagger = P, \quad P^2 = P.}$$

Eigenvalues 0 or 1. Example: $P = |\psi\rangle \langle\psi|$. **Physical role**: Define measurement outcomes (Postulate 2).

A.12 Trace and Partial Trace

The trace of an operator A is

$$\mathrm{Tr}(A) = \sum_i \langle i|A|i\rangle .$$

Properties: $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$, $\mathrm{Tr}(A \otimes B) = \mathrm{Tr}(A)\,\mathrm{Tr}(B)$.

For a composite system AB, the partial trace over B yields the reduced density operator for A:

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

Used in entanglement witnesses and mixed-state descriptions.

References

[1] J. von Neumann. *Mathematische Grundlagen der Quantenmechanik*. Springer, 1932. (English translation: *Mathematical Foundations of Quantum Mechanics*, Princeton University Press, 1955).

[2] P. A. M. Dirac. *The Principles of Quantum Mechanics*. Oxford University Press, 1st edition, 1930.

[3] M. Hayashi. *Quantum Information Theory: Mathematical Foundation*. Springer, 2nd edition, 2017.

[4] J. J. Sakurai. *Modern Quantum Mechanics*. Addison-Wesley, revised edition, 1994.

[5] D. J. Griffiths and D. F. Schroeter. *Introduction to Quantum Mechanics*. Cambridge University Press, 3rd edition, 2018.

[6] W. Heisenberg. Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik. *Zeitschrift für Physik*, 43:172–198, 1927.

[7] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47(10):777–780, 1935.

[8] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

[9] C. H. Bennett et al. Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels. *Physical Review Letters*, 70(13):1895–1899, 1993.

[10] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, 1984.

[11] N. Bohr. The quantum postulate and the recent development of atomic theory. *Nature*, 121:580–590, 1928.

[12] A. Peres. *Quantum Theory: Concepts and Methods*. Kluwer Academic Publishers, 1993.

[13] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 10th Anniversary edition, 2010.

[14] M. H. Devoret and R. J. Schoelkopf. Superconducting circuits for quantum information: An outlook. *Science*, 339(6124):1169–1174, 2013.

[15] W. H. Zurek. Decoherence, einselection, and the quantum origins of the classical. *Reviews of Modern Physics*, 75:715–775, 2003.

[16] J. S. Bell. On the Einstein–Podolsky–Rosen paradox. *Physics Physique*, 1:195–200, 1964.

[17] A. Aspect, J. Dalibard, and G. Roger. Experimental test of Bell's inequalities using time-varying analyzers. *Physical Review Letters*, 49(25):1804–1807, 1982.

[18] B. Hensen et al. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526:682–686, 2015.

[19] N. Gisin. Weinberg's non-linear quantum mechanics and superluminal communications. *Physics Letters A*, 143(1–2):1–2, 1990.

[20] D. S. Abrams and S. Lloyd. Nonlinear quantum mechanics implies polynomial-time solution for NP-complete and #P problems. *Physical Review Letters*, 81(18):3992–3995, 1998.

[21] Comisión Asesora en Tecnologías Cuánticas. Informe de la Comisión Asesora en Tecnologías Cuánticas. Ministerio de Ciencia, Tecnología, Conocimiento e Innovación, Chile, 2024. Disponible en: https://www.minciencia.gob.cl/areas/comision-asesora-tecnologias-cuanticas/.