Quantum Computing
An introduction

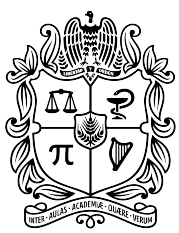
Mathematical foundations • Quantum mechanics • Information in QM
Quantum gates Programming • Quantum Entanglement • Quantum Protocols
Quantum Algorithms • Hybrid Quantum-classical algorithms • Hardware

Quantum Computing
An introduction

Mathematical foundations • Quantum mechanics • Information in QM
Quantum gates Programming • Quantum Entanglement • Quantum Protocols
Quantum Algorithms • Hybrid Quantum-classical algorithms • Hardware

Alcides Montoya Cañola

Associate Professor, Department of Physics,
Faculty of Sciences, Universidad Nacional de Colombia,
Sede Medellín



UNIVERSIDAD
NACIONAL
DE COLOMBIA

Medellín, Colombia, 2026

004.1
M79 Montoya Cañola, Alcides
Quantum Computing: An introduction /
Montoya. – First edition. – Medellín, Colombia : Universidad Nacional
de Colombia. Faculty of Sciences, 2026.
1 online resource (XXX pages) : illustrations, diagrams

ISBN: XXXXX

1. QUANTUM COMPUTING 2. QUANTUM MECHANICS
3. QUANTUM ALGORITHMS 4. QUANTUM INFORMATION
I. Montoya Cañola, Alcides
II. Title.

Cataloging-in-Publication Data, Universidad Nacional de Colombia. Sede Medellín

Quantum Computing: An introduction

Editorial Center of the Faculty of Sciences

Digital ISBN: XXXXX
Medellín, Colombia
First edition: August 2026

Cover design: XXXXX

Printed and made in Medellín, Colombia.

To all the women who made science
in laboratories where no chair awaited them,
who persevered against closed doors,
unsigned papers and unspoken names,
and built, step by step,
the luminous path we walk today.

To Marie Curie and Lise Meitner;
to Emmy Noether, who revealed that symmetry
is the deepest grammar of the universe;
to Grete Hermann, who dared to question
a proof that no one else questioned;
to Maria Goeppert Mayer and Chien-Shiung Wu;
to Ada Lovelace and Grace Hopper,
who first imagined that a machine could think.

And to those who are writing the present:
Dorit Aharonov, Barbara Terhal,
Michelle Simmons, Stephanie Wehner,
Eleanor Rieffel, Krysta Svore, Maria Schuld,
and Ana María Rey, who carried the light
of these same mountains to the coldest atoms.

Acknowledgments

My gratitude goes first to the Universidad Nacional de Colombia, Sede Medellín, for providing the academic space where these ideas could germinate and grow. This institution has been the garden where the seed of this project found fertile soil to flourish.

I am especially grateful to the **Centro de Excelencia en Computación Cuántica e Inteligencia Artificial** of the Universidad Nacional de Colombia, a space where quantum computing and artificial intelligence meet, and where the conviction that these two fields must be taught together has taken shape. Much of what appears in these pages was first discussed, questioned, and refined there.

To Professor Mario Trujillo Vargas, whose teaching has transformed the lives of his students. He taught us that physics is not a collection of formulas to be memorized but a way of looking at the world, and that a teacher's true measure is not what he knows, but what he awakens in others. His vision continues to shape those of us who had the fortune of learning from him.

To the young minds of Engineering Physics, who with their genuine questions and tireless curiosity have shaped every page of this text. Their doubts became clarities, their difficulties became opportunities to explain things better. This book is, in reality, an extended dialogue with all those restless souls seeking to understand.

Finally, to the students of the quantum computing course, who read these pages with a critical eye and helped correct the errors that inevitably inhabit a work of this length, and to all those who have helped and will help to improve it: you are a fundamental part of this collective process of building knowledge. In every correction, in every suggestion, lives the spirit of collaboration that makes the advancement of science possible.

Contents

Chapter 1

Information in Quantum Mechanics

In classical information theory, we store data in the form of zeros and ones, following binary logic. For example, when flipping a coin in the air, it can land showing heads or tails. We assign the value 0 to one side and 1 to the other, thus storing information in bits. Using Dirac notation, we can represent this type of information analogously: we assign $|0\rangle$ to represent "heads" and $|1\rangle$ for "tails". If we flip six coins and obtain the sequence heads, heads, tails, heads, tails, tails, we can store this information as 001011 in classical notation, and as $|001011\rangle$ in Dirac notation.

A crucial aspect we must consider is the number of possible states of the system. For one coin, there are two possible outcomes: heads or tails. If we flip two coins, the number of possible combinations is four. Generalizing, for a number of coins n, the number of possible combinations is 2^n. This relationship is the same as that used to describe the number of possible states in a system of n bits of information.

Table 1.1: Possible states of a bit system

Number of bits	**Number of possible states**
1	2
2	4
3	8
4	16
n	2^n

We denote by N_s the number of possible states of the system. According to the previous table, this quantity is given by:

$$N_s = 2^n \tag{1.1}$$

where n is the number of bits. Taking the base-2 logarithm of the previous expression, we obtain the explicit definition of the number of bits of information

available in the system:

$$\log_2 N_s = n \tag{1.2}$$

These equations are very useful because they allow us to represent any physical quantity in terms of bits. For example, the temperature in a room, the electric field in a region of space, the magnetic field, or the brightness of a star can be modeled using these bits of information. The reason physics uses digital computers is precisely because they allow modeling these relationships between physical quantities, describing both the state of a system and its configuration at a given instant, and how these evolve over time.

In the context of a system's configuration space, we can encounter reversible and non-reversible systems. A reversible system, like a switch that turns on and off, can return to its initial state. However, some systems do not return to their initial state; we call them singular systems. But what happens when we consider complex systems composed of millions of atoms or molecules, like a living being? Do we lose information about the system? The answer is no. The information is still present, but our ability to access all the details of the system may be limited. This does not imply that information is lost, but rather that our ability to distinguish between different system states is reduced due to the limitations of our measurement and modeling tools.

Definitions

Classical state: A classical state refers to the complete description of a physical object in terms of its observable properties such as position, velocity, acceleration, etc. By knowing these values at a given moment, it is possible to predict the future or past behavior of the system using known laws of motion. For example, if we know the velocity and direction of a ball in the air, we can accurately predict when and where it will land. This determinism is an essential characteristic of classical systems.

Quantum state: In contrast, a quantum state describes a generally microscopic physical system, such as atoms, electrons, photons, or any particle or set of few particles. In these systems, we must consider quantum effects such as superposition or entanglement. In addition to classical observable properties, new magnitudes such as spin or polarization emerge in quantum mechanics, which are fundamental for making predictions in the microworld. One of the most significant differences between classical and quantum systems is the impossibility of predicting with certainty the future state of a quantum system. In quantum mechanics, even if we know the current state of the system, we can only predict probabilities for future states, which reflects the intrinsically probabilistic and non-deterministic nature of the quantum world.

Quantum states are modeled physically and mathematically using Dirac notation, along with graphical representations that facilitate their visualization. For example, in the case of a photon, we can define its possible polarization states as follows:

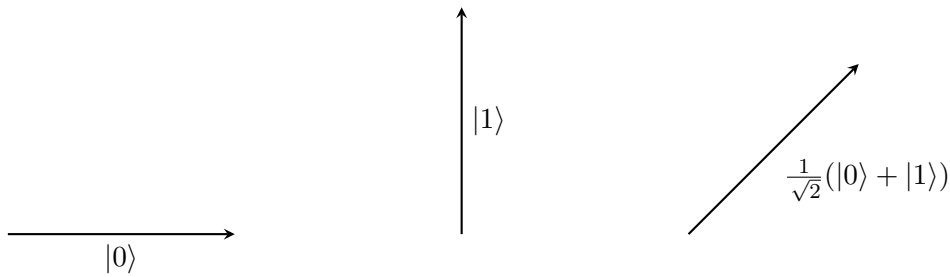


Figure 1.1: Representation of photon polarization in quantum states. The horizontal arrow represents state $|0\rangle$, the vertical arrow represents state $|1\rangle$, and the diagonal arrow corresponds to the superposition state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

Superposition: Unlike macroscopic systems, which are always in a defined state, quantum systems can exist in a superposition of states. This means that a photon can be in a combination of several different polarization states simultaneously. However, when the system is measured, it "collapses" to one of the specific states in the superposition. Before measurement, it is only possible to know the probabilities that the system is in each particular state.

The Transition to the Macroscopic World

Even though quantum mechanics successfully describes the behavior of matter at atomic and subatomic scales, its apparent contrast with classical physics—which governs the phenomena of our everyday environment—raises a fundamental question: why do effects such as superposition, entanglement, and the probabilistic nature of quantum states seem to vanish as the scale of systems increases?

The answer lies in the phenomenon of *quantum decoherence*, which explains how quantum systems lose their *purely quantum* character when interacting with the environment. Just as a wave disperses when it encounters obstacles in a pond, superposition states "dephase" due to multiple collisions and interactions with other particles [18].

Factors Contributing to Decoherence:

- **Interaction with the environment:** In practice, a quantum system is not isolated, but rather suffers collisions with other particles, absorbs or emits radiation, and experiences various types of "involuntary" measurements. These interactions promote the collapse of superposition and entanglement.
- **System size:** As the number of particles increases, so does the probability of interactions with the environment. Consequently, decoherence occurs more quickly and intensely in larger systems.

Schrödinger's "Cat" and Decoherence:

The famous thought experiment of Schrödinger's cat illustrates the fragility of quantum superposition. In theory, a cat confined in a box with a device that could cause its death would be in a superposition of "alive" and "dead" until we open the box. However, in reality, the cat continuously interacts with its environment—for example, exchanging heat with the air—so that its state "settles" into one of the two outcomes long before the box is opened.

Decoherence Time Scales

Decoherence is not a binary phenomenon but occurs gradually on characteristic time scales T_2 (decoherence time). For a modern superconducting qubit:

- T_1 (relaxation time): $\sim 50 - 100\ \mu s$
- T_2 (decoherence time): $\sim 50 - 200\ \mu s$
- Gate operation time: $\sim 20 - 100\ ns$

This allows approximately 10^3 to 10^4 operations before quantum information is lost, establishing the current practical limit for quantum circuits without error correction.

Practical example: A quantum algorithm requiring 1000 gates at 50 ns each needs 50 μs total execution time. With $T_2 = 100\ \mu s$, this leaves only a factor of 2 margin before decoherence destroys the computation—highlighting why error correction is essential for large-scale quantum computing.

Why Are Quantum Effects Not Observed in Large Objects?

- **Time scales:** In macroscopic systems, decoherence operates in incredibly short lapses. In fractions of a second, a large object experiences so many interactions that its *non-decoherent* quantum description becomes practically indistinguishable from a classical state.
- **Average effects:** As the number of particles increases, individual quantum mechanics effects tend to cancel out or average, so that classical features dominate [13].

Is It Possible to Observe Quantum Properties at Macroscopic Scales?

Despite the challenges involved, science has demonstrated that certain macroscopic systems can exhibit characteristic quantum mechanics behaviors. Notable examples include superconductivity and superfluidity. Similarly, quantum computing seeks to exploit quantum phenomena—such as superposition and entanglement—for the development of new technologies.

In summary, *quantum decoherence* constitutes the crucial nexus between the quantum world and classical physics. Although quantum mechanics describes

processes at atomic scales with great precision, its effects become less evident when the system interacts intensely with its environment or when it reaches macroscopic dimensions. Thus, classical features emerge as a result of incessant interaction with the environment.

1.1 Mathematical Elements for Representing Quantum Information

The representation and manipulation of quantum information rests entirely on the linear algebra developed in Chapter 2: complex vectors (kets), inner products, matrices as linear operators, and their multiplication. We assume that machinery here and do not repeat it; the reader may review Chapter 2 for definitions and proofs. In this section we highlight only the specific way these tools describe *information* and its evolution, and we fix the notation used throughout the rest of the chapter.

A physical system with a finite number of distinguishable configurations is represented by assigning each configuration a basis vector, and the state of the system by a column vector over those basis states. The *evolution* of the system—its transition from one configuration to another—is represented by the action of a matrix on that vector, exactly as a linear operator acts on a ket.

Example: State Evolution as Matrix Action

Consider a system that can occupy four configurations a, b, c, d, encoded as the standard basis vectors of $\mathbb{C}^4$:

$$\text{State } a: \begin{bmatrix}1\\0\\0\\0\end{bmatrix}, \quad \text{State } b: \begin{bmatrix}0\\1\\0\\0\end{bmatrix}, \quad \text{State } c: \begin{bmatrix}0\\0\\1\\0\end{bmatrix}, \quad \text{State } d: \begin{bmatrix}0\\0\\0\\1\end{bmatrix} \tag{1.3}$$

A cyclic evolution $a \to b \to c \to d \to a$ is implemented by the transition matrix

$$\mathbf{M} = \begin{bmatrix}0&0&0&1\\1&0&0&0\\0&1&0&0\\0&0&1&0\end{bmatrix}, \qquad \mathbf{M}\begin{bmatrix}1\\0\\0\\0\end{bmatrix} = \begin{bmatrix}0\\1\\0\\0\end{bmatrix}, \tag{1.4}$$

which sends state a to state b. Applying $\mathbf{M}$ repeatedly advances the system through the cycle; the state after k steps is $\mathbf{M}^k$ acting on the initial vector. This matrix–vector picture of evolution is the classical prototype of the unitary evolution of quantum states that we develop in the following sections, where the states carry complex amplitudes and the matrices are required to be unitary.

1.1.1 Vectors in Quantum State Spaces

Traditionally, in a three-dimensional vector space $\mathbb{R}^3$, we define a vector $\mathbf{r}$ as a quantity with magnitude and direction, expressed through the linear combination of components in the directions of Cartesian axes: $\mathbf{r} = x\hat{\mathbf{i}} + y\hat{\mathbf{j}} + z\hat{\mathbf{k}}$. In the context of quantum mechanics, we use a special type of vectors defined in a complex vector space $\mathbb{C}^n$, known as *kets* and denoted as $|a\rangle$.

These quantum vectors $|a\rangle$ have particular properties that distinguish them from classical vectors. One of their fundamental properties is linearity. That is, when multiplying a ket $|a\rangle$ by a complex number C, a new ket $|a'\rangle$ is obtained:

$$C\,|a\rangle \longrightarrow |a'\rangle \tag{1.5}$$

Similarly, the sum of two vectors in this space also produces a new vector in the same complex space:

$$|a\rangle + |b\rangle = |a + b\rangle = |\phi\rangle \tag{1.6}$$

Vector $|a\rangle$ in complex space $\mathbb{C}^n$ can be represented as a column vector with its components defined as follows:

$$|a\rangle \equiv \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{bmatrix} \tag{1.7}$$

If we multiply this vector by a complex number C, we obtain:

$$C\,|a\rangle \equiv \begin{bmatrix} Ca_1 \\ Ca_2 \\ Ca_3 \\ Ca_4 \end{bmatrix} \tag{1.8}$$

Here, the symbol $\equiv$ indicates that the ket can be represented or is equivalent to a column vector with numerical components.

The sum of kets can also be expressed in matrix notation:

$$|a\rangle + |b\rangle = |a + b\rangle \equiv \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{bmatrix} + \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{bmatrix} = \begin{bmatrix} a_1 + b_1 \\ a_2 + b_2 \\ a_3 + b_3 \\ a_4 + b_4 \end{bmatrix} \tag{1.9}$$

Since we are in a complex vector space, each complex number has a complex conjugate. In this space, we can define the complex conjugate of a ket $|a\rangle$, which is called *bra* and is represented as $\langle a|$. This bra can be expressed as a row vector with the complex conjugates of the ket components:

$$\langle a| \equiv \begin{bmatrix} \overline{a_1} & \overline{a_2} & \overline{a_3} & \overline{a_4} \end{bmatrix} \tag{1.10}$$

The inner product in this vector space, also known as *braket*, is defined as $\langle a|b\rangle$ and is equivalent to the matrix operation between bra $\langle a|$ and ket $|b\rangle$, as follows:

$$\langle a|b\rangle \equiv \begin{bmatrix} \overline{a_1} & \overline{a_2} & \overline{a_3} & \overline{a_4} \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{bmatrix} = \overline{a_1}b_1 + \overline{a_2}b_2 + \overline{a_3}b_3 + \overline{a_4}b_4 \tag{1.11}$$

As a particular example, if we calculate $\langle a|a\rangle$, we obtain:

$$\langle a|a\rangle \equiv \begin{bmatrix} \overline{a_1} & \overline{a_2} & \overline{a_3} & \overline{a_4} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{bmatrix} = \overline{a_1}a_1 + \overline{a_2}a_2 + \overline{a_3}a_3 + \overline{a_4}a_4 \tag{1.12}$$

For an electron, the possible quantum states in which it can be found can be represented generally as a superposition of two base states $|0\rangle$ and $|1\rangle$:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{1.13}$$

The probability that the electron is in state $|0\rangle$ is given by $\mathbb{P}\left[[]\,0\right] = |\alpha|^2$, while the probability that it is in state $|1\rangle$ is given by $\mathbb{P}\left[[]\,1\right] = |\beta|^2$. These probabilities must sum to 1, which ensures that the physical state of the quantum system is normalized:

$$|\alpha|^2 + |\beta|^2 = 1 \tag{1.14}$$

This is a fundamental concept in quantum mechanics and has no direct equivalent in the classical world. In terms of brackets, this normalization condition is expressed as:

$$\langle\psi|\psi\rangle = 1 \tag{1.15}$$

Some important relationships that the reader can prove are:

$$\langle 0|0\rangle = 1 \tag{1.16}$$
$$\langle 1|1\rangle = 1 \tag{1.17}$$
$$\langle 0|1\rangle = 0 \tag{1.18}$$
$$\langle 1|0\rangle = 0 \tag{1.19}$$

These relationships are the basis for understanding how quantum states are constructed and how operations are performed in Hilbert space, which is fundamental for quantum mechanics and quantum computing.

Matrices as Operators

In physics, both classical and quantum, matrices play a crucial role as operators that act on vectors, allowing us to obtain observable quantities. In classical physics, matrices can represent linear transformations that act on vectors, while in quantum computing, we use a special type of matrices to operate on quantum states. We will illustrate this general idea using simple examples in a two-dimensional vector space, and then extend these concepts to the quantum domain.

Consider a plane in two dimensions and a vector $\mathbf{V}$ in that plane, represented as follows:

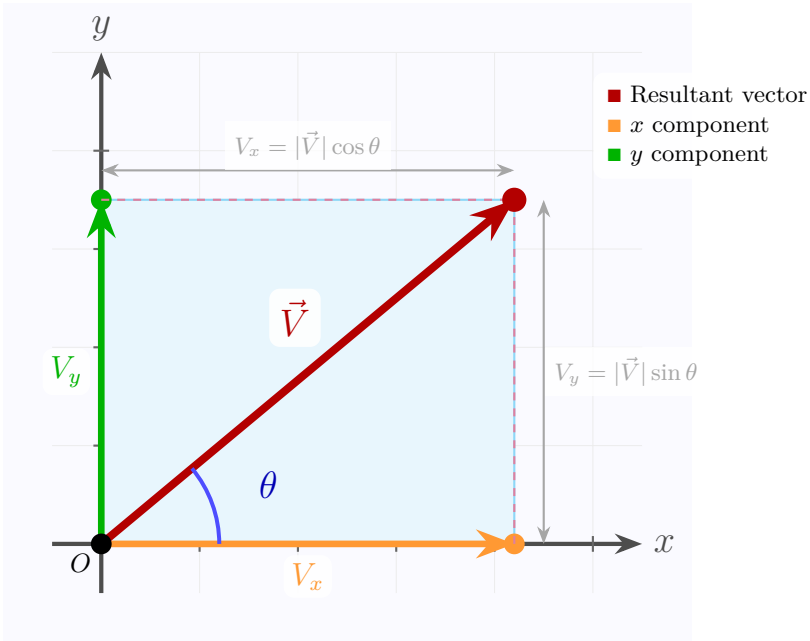


Figure 1.2: Decomposition of a vector $\vec{V}$ into its rectangular components V_x and V_y. The angle θ determines the direction of the vector with respect to the x axis.

The vector $\mathbf{V}$ can be expressed in terms of its components as:

$$\mathbf{V} = \begin{bmatrix} V_x \\ V_y \end{bmatrix} \tag{1.20}$$

Suppose we want to scale this vector $\mathbf{V}$ to double its length. We can achieve this by using a matrix that acts as an operator on the vector, multiplying its components by a factor of 2:

$$\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} V_x \\ V_y \end{bmatrix} = \begin{bmatrix} 2V_x \\ 2V_y \end{bmatrix} \tag{1.21}$$

In this case, the matrix operator has doubled the values of the vector components $\mathbf{V}$. We observe that this operator is a diagonal matrix that acts uniformly

on each component of the vector. Therefore, the operator that doubles the length of the vector is:

$$\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \tag{1.22}$$

Now, let us consider a different operation: doubling only the V_y component of the vector, while keeping V_x unchanged. The corresponding matrix operator would be:

$$\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} V_x \\ V_y \end{bmatrix} = \begin{bmatrix} V_x \\ 2V_y \end{bmatrix} \tag{1.23}$$

In this case, the matrix operator acts only on the V_y component, doubling it, while leaving the V_x component unchanged:

$$\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \tag{1.24}$$

These examples illustrate how matrices can act as operators to transform vectors in a vector space. Now, let us consider a more complex transformation: the rotation of the vector components by an angle of $\frac{\pi}{2}$ clockwise. The corresponding matrix operator would be:

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} V_x \\ V_y \end{bmatrix} = \begin{bmatrix} V_y \\ -V_x \end{bmatrix} \tag{1.25}$$

Here, the matrix operator has rotated the vector components, swapping V_x and V_y and changing the sign of V_x. This type of transformation is common in many areas of physics, including quantum computing.

The key conclusion is that matrices can be used as operators to transform vectors within vector spaces. In the context of quantum computing, we will use special matrices as operators to perform operations on quantum states. These operations will be fundamental for the manipulation and evolution of qubits in quantum systems, and we will study in detail what types of matrices are necessary for these operations.

1.1.2 Special Matrices for Operating in the Quantum World

The quantum description of a physical system begins with a Hilbert space $\mathcal{H}$ and a set of operators acting on it. Two families of matrices, introduced and studied in detail in Chapter 2, play the central roles: *Hermitian* matrices, which represent observables, and *unitary* matrices, which represent reversible operations. We recall their definitions here—in the correct form—and then focus on the property most relevant to quantum information: the expectation value.

A matrix $\mathbf{M}$ is **Hermitian** if it equals its adjoint (conjugate transpose),

$$\mathbf{M} = \mathbf{M}^\dagger, \qquad (\mathbf{M}^\dagger)_{ij} = \overline{\mathbf{M}_{ji}}, \tag{1.26}$$

that is, transposition combined with complex conjugation of every entry. Note that this is *not* the same as ordinary transposition: a real symmetric matrix satisfies $\mathbf{M} = \mathbf{M}^{\top}$, but for complex entries the conjugation is essential. For example,

$$\begin{bmatrix} 1 & i \\ -i & 1 \end{bmatrix} \tag{1.27}$$

is Hermitian (the off-diagonal entries are complex conjugates), whereas $\begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}$ is symmetric but *not* Hermitian. As shown in Chapter 2, the eigenvalues of a Hermitian matrix are real and its eigenvectors corresponding to distinct eigenvalues are orthogonal—exactly the properties required of a physical observable, whose measured values are real.

A matrix $\mathbf{U}$ is **unitary** if

$$\mathbf{U}\mathbf{U}^{\dagger} = \mathbf{U}^{\dagger}\mathbf{U} = \mathbf{I}, \tag{1.28}$$

equivalently $\mathbf{U}^{-1} = \mathbf{U}^{\dagger}$. Unitary matrices preserve the inner product and hence the norm, so they map normalized states to normalized states; this is why every quantum gate is unitary. The Hadamard matrix

$$\mathbf{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{1.29}$$

is both Hermitian and unitary, as the reader can verify using $\mathbf{H}\mathbf{H}^{\dagger} = \mathbf{I}$.

Two useful identities in Dirac notation, proved directly from the definition of the adjoint, are

$$\langle \phi | \psi \rangle = \overline{\langle \psi | \phi \rangle}, \qquad \langle \phi | \mathbf{M} \rangle \, \psi = \overline{\langle \psi | \mathbf{M}^{\dagger} \rangle \, \phi}. \tag{1.30}$$

When $\mathbf{M}$ is Hermitian, $\mathbf{M}^{\dagger} = \mathbf{M}$, and the second identity becomes $\langle \phi | \mathbf{M} \rangle \, \psi = \overline{\langle \psi | \mathbf{M} \rangle \, \phi}$.

Expectation Values

A fundamental quantity in quantum mechanics is the **expectation value** of an observable $\mathbf{M}$ in a state $|\psi\rangle$, defined as

$$\langle \mathbf{M} \rangle_{\psi} = \langle \psi | \mathbf{M} \rangle \, \psi. \tag{1.31}$$

This quantity requires careful interpretation: it is the statistical mean over an *ensemble* of identically prepared systems, not the outcome of any individual measurement. Measuring $\mathbf{M}$ on a system in state $|\psi\rangle$ yields, with certainty, one of the eigenvalues λ_i of $\mathbf{M}$, with probability $|\langle \lambda_i | \psi \rangle|^2$, where $|\lambda_i\rangle$ is the corresponding eigenvector. The expectation value is the weighted average

$$\langle \mathbf{M} \rangle_{\psi} = \sum_i \lambda_i |\langle \lambda_i | \psi \rangle|^2. \tag{1.32}$$

Consider measuring the energy of an electron in the superposition $|\psi\rangle = \frac{1}{\sqrt{2}}|E_1\rangle + \frac{1}{\sqrt{2}}|E_2\rangle$, where $|E_1\rangle$, $|E_2\rangle$ are energy eigenstates with eigenvalues $E_1 = 1$ eV and $E_2 = 3$ eV. Any single measurement yields either 1 eV or 3 eV, each with probability 1/2; but the average over a large ensemble is

$$\langle E\rangle = \tfrac{1}{2}(1\text{ eV}) + \tfrac{1}{2}(3\text{ eV}) = 2\text{ eV}. \tag{1.33}$$

This value of 2 eV is *not* an eigenvalue of the energy operator and therefore cannot result from any single measurement—illustrating the statistical character of quantum predictions.

The expectation value of a Hermitian operator is always real, as required for a measurable quantity. The proof is immediate from the adjoint identity:

$$\overline{\langle\psi|\mathbf{M}\rangle\,\psi} = \left\langle\psi\middle|\mathbf{M}^\dagger\right\rangle\psi = \langle\psi|\mathbf{M}\rangle\,\psi, \tag{1.34}$$

using $\mathbf{M}^\dagger = \mathbf{M}$. Since the expectation value equals its own complex conjugate, it must be real. This is the fundamental reason why physical observables are represented by Hermitian operators.

The Pauli Matrices

The most important observables for a single qubit are the Pauli matrices, studied in detail in Chapter 2:

$$\sigma_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_2 = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{1.35}$$

They are Hermitian, with eigenvalues ± 1 and orthogonal eigenvectors; the eigenvectors of σ_3 are the computational basis states $|0\rangle$ and $|1\rangle$, with eigenvalues $+1$ and -1 respectively. Together with the identity, the Pauli matrices form a basis for the real vector space of 2×2 Hermitian matrices. In quantum computing they serve simultaneously as observables (spin components) and as quantum gates (X, Y, Z), a dual role we exploit throughout later chapters.

1.1.3 Spin as the Basic Unit of Information in Quantum Computing

Spin is a fundamental property of electrons and other subatomic particles, and constitutes one of the basic units of information in quantum computing. To understand how spin is used in this context, it is essential to understand its quantum nature and how it is represented mathematically.

The spin of an electron can be imagined as a small magnet with a North pole and a South pole, associated with a physical quantity called *magnetic moment*. This idea, however, transcends classical intuition, as spin does not correspond to a physical object rotating, but rather to an intrinsic property of quantum particles.

The first experimental evidence of spin was provided in 1922 by Otto Stern and Walther Gerlach in an experiment that showed the quantization of angular momentum. However, the quantum theory of the time could not explain the observed atomic spectra until George Uhlenbeck and Samuel Goudsmit introduced a new quantum number, called the *spin quantum number*, to describe these phenomena. The complete understanding of spin did not arrive until 1927, with the development of relativistic quantum theory.

Spin is a physical property of elementary particles that gives them a fixed intrinsic angular momentum. Along with electric charge, which was well known since the early 19th century, spin is one of the fundamental properties of particles.

According to relativistic quantum theory, spin cannot be represented in terms of conventional spatial coordinates, which implies that, regardless of the observer, a particle will always have an intrinsic angular momentum, although the direction of this momentum may vary depending on the observer [11].

The key characteristics of the magnetic moment or spin of the electron are as follows:

- The value of spin is quantized
- The spin of a particle is always an integer multiple of $\frac{\hbar}{2}$
- When spin is measured in different directions, only certain discrete values are obtained, which correspond to its projections in that direction. The projection of the spin angular momentum of an electron, if measured in a particular direction, can result exclusively in the values $\frac{\hbar}{2}$ or $-\frac{\hbar}{2}$
- The total magnitude of spin is unique for each type of elementary particle. For electrons, protons and neutrons, this magnitude is $\hbar\sqrt{s(s+1)}$, where $s = \frac{1}{2}$
- Quantum particles are divided into two categories: fermions and bosons. Fermions, which obey Fermi-Dirac statistics, have half-integer spins, while bosons, which obey Bose-Einstein statistics, have integer spins

Spin is represented as an operator in a finite-dimensional Hilbert space $2s+1$. This vector operator is expressed as:

$$(\sigma_x \hat{x} + \sigma_y \hat{y} + \sigma_z \hat{z}) \tag{1.36}$$

Where σ_i are the Pauli matrices, which are fundamental in the description of spin in quantum mechanics. The spin measurement process is performed using the operator S as follows:

$$S\,|\phi\rangle = (S_x, S_y, S_z)\,|\phi\rangle \tag{1.37}$$

The basis commonly used to describe spin is provided by the eigenvectors of S_z. For a particle with $s = \frac{1}{2}$, in Cartesian coordinates, the basis is defined in

terms of the spin projection states in the z direction. These states are associated with specific basis vectors:

$$|\uparrow\rangle = \left|m = +\frac{1}{2}\right\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \tag{1.38}$$

and

$$|\downarrow\rangle = \left|m = -\frac{1}{2}\right\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{1.39}$$

1.2 Qubits

What is a qubit? In essence, it is a quantum bit, a two-level coherent quantum system. The possible quantum states satisfy the superposition principle, and the measurements performed on these states have a probabilistic character. How can a qubit be constructed? There are several physical ways to represent a qubit, such as photon polarization, the internal states of an atom (energy levels), the magnetic field generated by an electron in its motion, or the current in a superconducting circuit at very low temperature and without resistance. These diverse physical implementations allow storing and manipulating quantum information in qubits.

In classical computing, states are completely determined (0 or 1), with no room for probability amplitudes; measurements are completely deterministic. Classical bits are, in a sense, a particular case of qubits, which are vectors in a two-dimensional space defined in the domain of complex numbers. Qubits, unlike classical bits, are always in superposition states, making them ideal for developing algorithms that exploit quantum parallelism. However, when a qubit is measured, it collapses to a particular state probabilistically.

In this text, we will use matrix representations and tensor products to describe operations on qubits. If a system is composed of multiple qubits, then we will use tensors to represent it. A graphical way to represent qubits and the different operations is through the use of a unit sphere (Bloch sphere), which shows the complex amplitudes or phases in a three-dimensional space.

The fundamental difference between classical and quantum computing lies in the encoding of information. In the quantum world, information is encoded in a completely different way from what we are accustomed to in classical computing.

Consequences of Quantum Superposition

The superposition of states in a qubit is the foundation of **quantum parallelism**, a phenomenon radically different from classical parallelism. While in classical computing parallelism requires multiple processors working simultaneously on different data, in quantum computing a *single* qubit in superposition can simultaneously represent both values 0 and 1. This superposition, moreover, allows for **quantum interference**: probability amplitudes can add constructively or destructively, a phenomenon with no classical analog that is exploited by quantum algorithms to amplify correct answers and suppress incorrect ones.

Common Misconception About Quantum Parallelism

Warning: Although a qubit in superposition "contains" information about both states simultaneously, measurement collapses the system to a SINGLE classical result. The computational power does NOT come from "computing all answers at once," but from the ability to manipulate probability amplitudes through quantum interference to amplify correct answers and cancel incorrect ones.

Example: Consider a 3-qubit system in uniform superposition:

$$|\psi\rangle = \frac{1}{\sqrt{8}} \sum_{k=0}^{7} |k\rangle$$

This state simultaneously "explores" all 8 possible inputs to a function f, but upon measurement, we obtain only ONE output value. The quantum advantage comes from cleverly designed algorithms (like Grover's or Shor's) that use interference to extract global properties of f from this single measurement.

Mathematical Representation of the Qubit

Formally, a qubit is defined as a unit vector in a two-dimensional complex Hilbert space, $\mathcal{H} \cong \mathbb{C}^2$. In the computational basis $\{|0\rangle, |1\rangle\}$, the most general state of a qubit is:

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle \tag{1.40}$$

where $\alpha, \beta \in \mathbb{C}$ are the *probability amplitudes* that must satisfy the normalization condition:

$$|\alpha|^2 + |\beta|^2 = 1 \tag{1.41}$$

This equation has profound implications: while a classical bit can only be in states $\{0, 1\}$ (two discrete possibilities), a qubit can exist in any linear combination of these basis states, determined by infinite pairs of complex values (α, β) that satisfy normalization. Geometrically, the set of all pure states of a qubit forms the *Bloch sphere*, a two-dimensional surface in three-dimensional space.

It is crucial to understand that a qubit *does not store two bits of information*: when measuring the qubit, the state $|\psi\rangle$ irreversibly collapses to $|0\rangle$ with probability $|\alpha|^2$ or to $|1\rangle$ with probability $|\beta|^2$, obtaining a single classical bit of

information. The computational power does not come from storing more information, but from the ability to simultaneously process multiple possibilities in superposition.

Quantum Parallelism in Action

The true advantage of the qubit emerges during *processing*, before measurement. Consider a Boolean function $f : \{0, 1\} \to \{0, 1\}$ implemented as a unitary quantum operation U_f. If we apply U_f to the superposition state:

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

we simultaneously obtain information about $f(0)$ and $f(1)$ in a single computational step, something impossible classically. This is the underlying principle of the Deutsch-Jozsa algorithm, which demonstrates exponential quantum advantage for a certain artificial problem.

During quantum processing, the system evolves unitarily through **quantum gates** that manipulate the amplitudes α and β, maintaining superposition at all times. Quantum algorithms ingeniously exploit interference to design gate sequences that amplify the amplitudes associated with correct solutions while canceling incorrect ones, so that when finally measuring the system, the probability of obtaining the desired answer is high.

It is important to note that not all quantum algorithms require a unique deterministic result. Many modern algorithms operate in probabilistic regimes or extract information from the complete *probability distribution* $\{|\alpha|^2, |\beta|^2, ...\}$ through quantum tomography techniques or through multiple circuit executions.

Multiple Qubit Systems and Exponential Explosion

The true power of quantum computing emerges when considering multiple qubit systems. For n qubits, the Hilbert space has dimension 2^n, allowing superpositions over 2^n basis states simultaneously.

Consider a three-qubit system. If each qubit $j \in \{1, 2, 3\}$ is in state:

$$|\gamma_j\rangle = \alpha_j |0\rangle + \beta_j |1\rangle$$

the state of the complete system (assuming the qubits are initially separable) is the tensor product:

$$\begin{aligned} |\Psi\rangle &= |\gamma_1\rangle \otimes |\gamma_2\rangle \otimes |\gamma_3\rangle \\ &= (\alpha_1 |0\rangle + \beta_1 |1\rangle) \otimes (\alpha_2 |0\rangle + \beta_2 |1\rangle) \otimes (\alpha_3 |0\rangle + \beta_3 |1\rangle) \\ &= \sum_{i,j,k \in \{0,1\}} c_{ijk} |ijk\rangle \end{aligned} \tag{1.42}$$

where the coefficients are:

$$\begin{aligned} &c_{000} = \alpha_1\alpha_2\alpha_3, \quad c_{001} = \alpha_1\alpha_2\beta_3, \quad c_{010} = \alpha_1\beta_2\alpha_3, \quad c_{011} = \alpha_1\beta_2\beta_3 \\ &c_{100} = \beta_1\alpha_2\alpha_3, \quad c_{101} = \beta_1\alpha_2\beta_3, \quad c_{110} = \beta_1\beta_2\alpha_3, \quad c_{111} = \beta_1\beta_2\beta_3 \end{aligned} \tag{1.43}$$

This can be written more compactly as:

$$|\Psi\rangle = \sum_{k=0}^{7} c_k |k\rangle \tag{1.44}$$

where $|k\rangle$ represents the binary expansion of k (e.g., $|5\rangle = |101\rangle$) and $\sum_{k=0}^{7} |c_k|^2 = 1$.

Separability and the Structure of Multi-Qubit States

The Hilbert space $\mathcal{H}^{\otimes n}$ of an n-qubit system possesses rich internal structure beyond its 2^n dimensionality. A state $|\psi\rangle \in \mathcal{H}^{\otimes n}$ is termed *separable* (or product state) if it can be expressed as a tensor product of individual qubit states:

$$|\psi\rangle_{\text{sep}} = \bigotimes_{j=1}^{n} |\phi_j\rangle = |\phi_1\rangle \otimes |\phi_2\rangle \otimes \cdots \otimes |\phi_n\rangle \tag{1.45}$$

where each $|\phi_j\rangle = \alpha_j |0\rangle + \beta_j |1\rangle$ represents an independent single-qubit state. Such states encode no quantum correlations beyond those present in classical probability distributions.

Conversely, a state that cannot be factorized into tensor products of lower-dimensional states is *entangled*. The Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ provides the canonical example of maximal two-qubit entanglement. To verify its non-separability, suppose $|\Phi^+\rangle = (\alpha |0\rangle + \beta |1\rangle) \otimes (\gamma |0\rangle + \delta |1\rangle)$ for some complex coefficients. Expanding the right side yields:

$$\alpha\gamma |00\rangle + \alpha\delta |01\rangle + \beta\gamma |10\rangle + \beta\delta |11\rangle \tag{1.46}$$

Comparing coefficients with $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ requires $\alpha\gamma = \beta\delta = \frac{1}{\sqrt{2}}$ and $\alpha\delta = \beta\gamma = 0$. From the vanishing conditions, either $\alpha = 0$ or $\delta = 0$, and either $\beta = 0$ or $\gamma = 0$. But these constraints contradict the non-vanishing requirements, establishing that no such factorization exists.

The distinction between separable and entangled states is not merely mathematical formalism but reflects fundamentally different physical resources. Separable states can be prepared using only local operations and classical communication (LOCC), while entangled states require genuine quantum interactions. This dichotomy underlies the resource theory of entanglement, wherein entanglement serves as a consumable commodity for quantum information protocols. The four maximally entangled Bell states:

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \tag{1.47}$$

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \tag{1.48}$$

form an orthonormal basis for the two-qubit Hilbert space and exhibit perfect correlations that violate Bell inequalities—correlations achievable by no local hidden

variable theory. The generation, manipulation, and measurement of such entangled states constitute the essential operations of quantum information processing.

When measuring this system, one obtains one of the $2^3 = 8$ possible classical bit strings $\{000, 001, \ldots, 111\}$ with probability $|c_k|^2$. This exponential scaling of the state space is both the source of quantum computational power and the barrier to its classical simulation.

Consider applying a function $f : \{0,1\}^n \to \{0,1\}$ to the uniform superposition $|+\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$. While the quantum state evolves to encode $f(x)$ for all 2^n inputs simultaneously, measurement extracts only a single value. Quantum algorithms succeed by carefully orchestrating interference patterns such that measurement probabilities concentrate on desired outcomes. Grover's algorithm exemplifies this principle: through $O(\sqrt{N})$ iterations of carefully designed unitary operations, it amplifies the amplitude of the target state while suppressing others, achieving quadratic speedup over classical search despite extracting only one answer per measurement.

The classical intractability of simulating quantum systems follows directly from this exponential state space. Storing the amplitudes for a 300-qubit system requires $2^{300} \approx 10^{90}$ complex numbers—exceeding the number of atoms in the observable universe. This computational bottleneck is not merely an engineering challenge but a fundamental distinction: the information capacity of quantum systems scales exponentially with physical size, whereas classical systems scale linearly.

Exponential Scaling of the State Space

- 1 qubit: $2^1 = 2$ basis states, 2 complex amplitudes
- 10 qubits: $2^{10} = 1{,}024$ states, ∼16 KB of memory
- 50 qubits: $2^{50} \approx 10^{15}$ states, ∼16 PB of memory
- 300 qubits: $2^{300} \approx 10^{90}$ states (more than the number of atoms in the observable universe)

This exponential explosion of the state space is precisely what makes quantum computers potentially more powerful than classical ones for certain problems, and simultaneously, what makes it impossible to simulate them classically efficiently.

1.2.1 Graphical Representation of Qubits and Bases

Graphically, qubits in a Hilbert space can be represented using the Bloch sphere as can be seen in Figure 1.3, defined in three-dimensional space $\mathbb{R}^3$. Each point on the sphere can be interpreted as the three expectation values $\langle X \rangle$, $\langle Y \rangle$ and $\langle Z \rangle$ of some qubit state $|\psi\rangle$. In essence, every value of a qubit $|\psi\rangle$ in Hilbert space corresponds to a point $\hat{n} = (x, y, z)^T$ on the Bloch sphere [10].

In the graphical representation of the Bloch sphere:

- On the z axis, the basis qubits $|0\rangle$ and $|1\rangle$ are located. - On the x axis, the basis qubits $|+\rangle$ and $|-\rangle$ are found. - On the y axis, the qubits $\frac{|0\rangle - \mathrm{i}|1\rangle}{\sqrt{2}}$ and $\frac{|0\rangle + \mathrm{i}|1\rangle}{\sqrt{2}}$ are located.

To represent any point on the sphere, spherical coordinates are usually used. Then, the point $\hat{n} = (1, \theta, \phi)^T$ corresponds to the qubit $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$.

We can measure a qubit in any orthonormal basis simply by projecting $|\psi\rangle$ onto the two basis vectors $|0\rangle$ and $|1\rangle$. The new state of the system $|\psi'\rangle$ is the result of the measurement. All pure states lie on the surface of the sphere, while mixed states occupy its interior.

The representation of a qubit on the Bloch sphere can be written as:

$$|\psi\rangle = \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) \\ e^{\mathrm{i}\phi} \sin\left(\frac{\theta}{2}\right) \end{bmatrix} \tag{1.49}$$

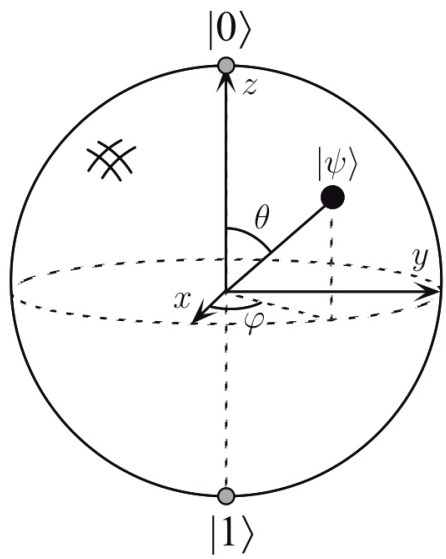


Figure 1.3: Definition of the Bloch sphere and basis states

In Figure 1.4, the basis states $|0\rangle$, $|1\rangle$, $|+\rangle$ and $|-\rangle$ represented on the Bloch sphere are shown:

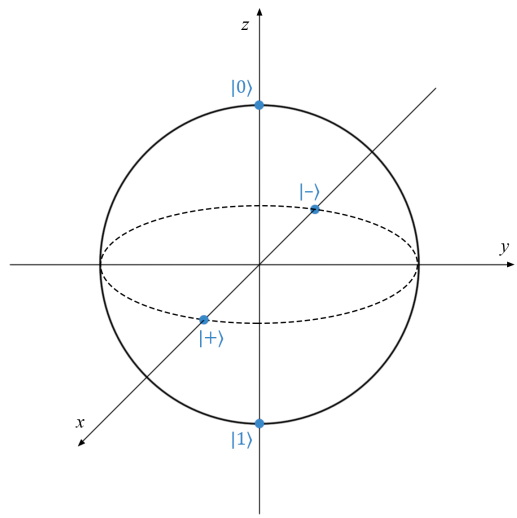


Figure 1.4: Basis states $|0\rangle$, $|1\rangle$, $|+\rangle$ and $|-\rangle$ on the Bloch sphere

The Hydrogen Atom

The hydrogen atom is the simplest atom in nature and, therefore, a good starting point for understanding quantum computing. This atom has a single electron, negatively charged, that moves around a proton, positively charged. In Bohr's model, the electron is attracted to the proton due to the Coulomb force. Since the proton is approximately 1800 times more massive than the electron, its motion in response to the Coulomb force is very small, so in this model, the proton can be considered at rest.

Consider a hydrogen atom with two energy levels. The first level, denoted as $|0\rangle$, represents the lowest energy state of the electron in the hydrogen atom. The second level, denoted as $|1\rangle$, is defined as the excited state of the electron in the same atom.

We can associate the lowest energy state with the value 0 and the excited state with the value 1. For example, if the probability of finding the electron in the lowest energy state is $\frac{1}{3}$ and in the excited state is $\frac{2}{3}$, the quantum description of the system would be given by the linear combination of these states. The hydrogen atom provides an instructive physical realization of a two-level quantum system, though we must acknowledge the simplifications inherent in this description. The Bohr model, while historically significant and pedagogically valuable for introducing quantized energy levels, represents a semiclassical approximation to the full quantum mechanical treatment. In the rigorous formulation, solving the time-independent Schrödinger equation for the Coulomb

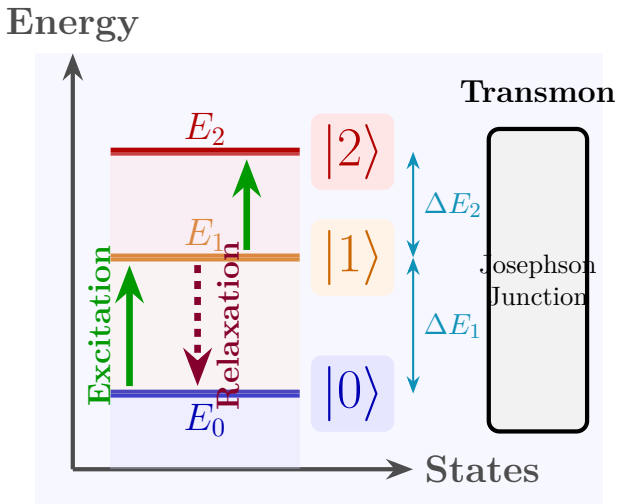


Figure 1.5: Anharmonic energy levels of a transmon qubit. The deliberately engineered anharmonicity $\alpha = (E_2 - E_1) - (E_1 - E_0) < 0$ enables selective addressing of the computational subspace $\{|0\rangle, |1\rangle\}$ through resonant microwave pulses at frequency $\omega_{01}/2\pi \approx 5$ GHz without populating higher levels. Modern transmons achieve $|\alpha|/2\pi \sim 200 - 300$ MHz, providing sufficient spectral separation while maintaining long coherence times through reduced charge noise sensitivity. The transition from harmonic oscillator (equal level spacing) to transmon (decreasing spacing) arises from the nonlinear Josephson inductance $L_J(\varphi) = \Phi_0/(2\pi I_c \cos\varphi)$, where $\Phi_0 = h/2e$ is the magnetic flux quantum and I_c the junction critical current. This anharmonicity is essential for quantum gate operations: a π-pulse resonant with ω_{01} implements an X gate rotating $|0\rangle \leftrightarrow |1\rangle$ while leaving $|2\rangle$ virtually unpopulated due to off-resonant detuning.

potential $V(r) = -e^2/(4\pi\epsilon_0 r)$ yields the energy eigenvalues:

$$E_n = -\frac{m_e e^4}{2(4\pi\epsilon_0)^2\hbar^2}\frac{1}{n^2} = -\frac{13.6 \text{ eV}}{n^2} \tag{1.50}$$

where $n \in \{1, 2, 3, \ldots\}$ denotes the principal quantum number. The ground state ($n = 1$, $E_1 = -13.6$ eV) and first excited state ($n = 2$, $E_2 = -3.4$ eV) differ by approximately 10.2 eV, corresponding to ultraviolet photons with wavelength $\lambda \approx 122$ nm (the Lyman-α transition). When considering only these two levels and neglecting spontaneous emission and other decay mechanisms, the electron dynamics in this truncated Hilbert space precisely mirror the mathematics of a single qubit. The superposition of energy eigenstates:

$$\alpha\,|0\rangle + \beta\,|1\rangle \tag{1.51}$$

1.2.2 Example: Possible States of the System and Probability Amplitudes

To illustrate the concept of states and probability amplitudes, let us consider three possible states of the system:

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \tag{1.52}$$

$$\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \tag{1.53}$$

$$\left(\frac{1}{2} + \frac{i}{2}\right)|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \tag{1.54}$$

In all cases, when measuring the system, the normalization condition must be satisfied:

$$|\alpha|^2 + |\beta|^2 = 1 \tag{1.55}$$

Here, α and β are complex numbers, which can be expressed as:

$$\alpha = a + bi \tag{1.56}$$

Where the absolute value of α is defined as:

$$|\alpha| = \sqrt{a^2 + b^2} \tag{1.57}$$

The question that arises is: What is the probability that the electron is in state $|0\rangle$ or in state $|1\rangle$?

To calculate this, we take the value of $|\alpha|^2$ for each of the states described in the previous equations. This defines the probability that the electron is in a given state. For example, if α is $\frac{1}{\sqrt{2}}$, then:

$$|\alpha|^2 = \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2} \tag{1.58}$$

Similarly, we find that the probability amplitude for $|\beta|^2 = \frac{1}{2}$. Therefore, when a measurement is made, there is a probability $|\alpha|^2$ that the electron is in the lowest energy state, $|0\rangle$, and a probability $|\beta|^2$ that it is in the excited state, $|1\rangle$.

1.2.3 Qubits in Dirac Notation and Matrix Notation

In Dirac notation, a quantum state of a two-level system is represented as $\alpha|0\rangle + \beta|1\rangle$, where α and β are complex coefficients indicating the probability amplitudes of states $|0\rangle$ and $|1\rangle$. An alternative way to write these coefficients in matrix notation is:

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix} \tag{1.59}$$

This is a unit vector in a two-dimensional space in the domain of complex numbers. If we consider the particular case in equation $\alpha|0\rangle + \beta|1\rangle$ where $\alpha = 1$ and $\beta = 0$, we can rewrite the ket $|0\rangle$ in matrix notation as:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \tag{1.60}$$

Similarly, if we take $\alpha = 0$ and $\beta = 1$, the ket $|1\rangle$ can be expressed in matrix notation as:

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{1.61}$$

Graphically, this correspondence between Dirac notation and matrix notation can be visualized in an orthonormal system of vectors:

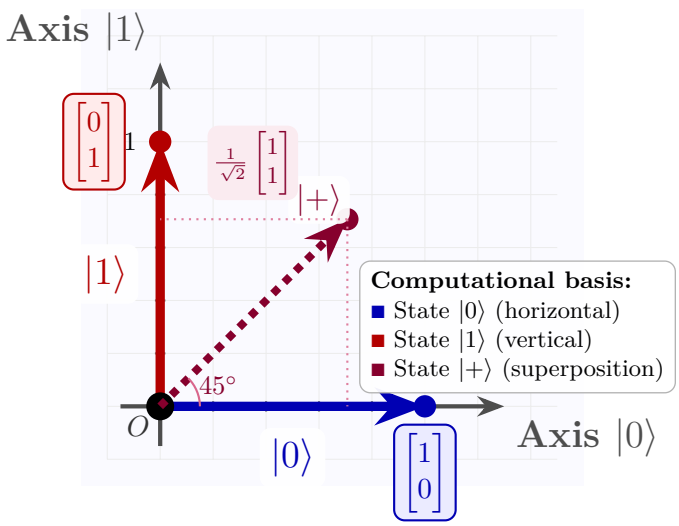


Figure 1.6: Geometric representation of the computational basis vectors $\{|0\rangle, |1\rangle\}$ in the state space of a qubit. The basis vectors are orthogonal and normalized. As an example of superposition, the state $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ is shown, which forms a 45° angle with both axes, indicating equal probability amplitude for both basis states.

The graph in Figure 1.6 represents the basis vectors $|0\rangle$ and $|1\rangle$ of the Hilbert space in a two-dimensional Cartesian system. The vector $|0\rangle$, oriented in the horizontal direction, corresponds to $\begin{bmatrix}1\\0\end{bmatrix}$, while the vector $|1\rangle$, oriented in the vertical direction, corresponds to $\begin{bmatrix}0\\1\end{bmatrix}$. The point **O** denotes the origin of the coordinate system. This representation is fundamental in quantum mechanics for describing quantum states and constructing superpositions.

A general state of the quantum system, such as the state of the electron in a hydrogen atom, can be represented graphically in this orthonormal space as a point in the plane, defined by an angle θ with respect to the $|0\rangle$ axis.

The probability of finding the system in a given state $|\psi\rangle$ at an angle θ in the plane is expressed as:

$$|\psi\rangle = \cos(\theta)\,|0\rangle + \sin(\theta)\,|1\rangle \tag{1.62}$$

In matrix notation, this can be written as:

$$|\psi\rangle = \begin{bmatrix}\cos(\theta)\\ \sin(\theta)\end{bmatrix} \tag{1.63}$$

When measuring the quantum system, the probability that the system is in state $|0\rangle$ is $\cos^2(\theta)$, and the probability that it is in state $|1\rangle$ is $\sin^2(\theta) = \cos^2\left(\frac{\pi}{2} - \theta\right)$.

1.2.4 Qubits Using Photon Polarization

Photon polarization is a fundamental mechanism for implementing qubits in quantum computing. A photon can have different polarizations, and these can be used to represent quantum states. The following image illustrates the polarization of an electric field:

The scheme in Figure 1.7 shows how an incident light beam is polarized through a polarizer, interacts with a thin crystal section and finally passes through a second polarizer. This process illustrates the phenomenon of dephasing and polarization components in different directions.

The electric field $\vec{E}$ can oscillate in a horizontal plane, which we can represent as the ket $|0\rangle$, or in a vertical plane, which corresponds to state $|1\rangle$. In this case, ket $|1\rangle$ is denoted as $|\uparrow\rangle$ and state $|0\rangle$ as $|\downarrow\rangle$. The basis of these states will be defined as:

The reference system shown in Figure 1.6 illustrates the basis states of a two-level system typically used in quantum computing, such as a qubit or a spin-$\frac{1}{2}$ system. The vectors $|\downarrow\rangle$ and $|\uparrow\rangle$ are represented through their corresponding column matrices. This representation is fundamental for analyzing the mathematical and physical properties of quantum systems.

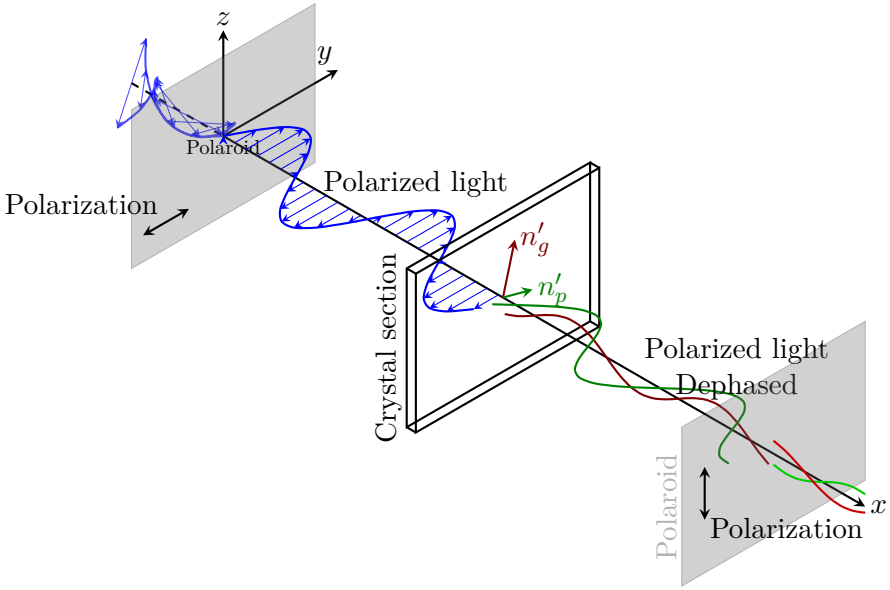


Figure 1.7: Schematic representation of light polarization and dephasing through a polarizer and a birefringent crystal, analogous to measurement and phase rotation operations on qubits.

Similarly, when measuring the state of a photon, the result we obtain is the projection of the quantum state onto each of the axes. Mathematically, we can describe a quantum state of a polarized photon as:

$$|\psi\rangle = \cos(\theta)\,|\downarrow\rangle + \sin(\theta)\,|\uparrow\rangle \quad \text{or} \quad |\psi\rangle = \begin{bmatrix}\cos(\theta)\\ \sin(\theta)\end{bmatrix} \tag{1.64}$$

The probability that the photon passes through a polarizer in a direction given by angle θ is given by $\cos^2(\theta)$, while the probability that it is blocked is $\sin^2(\theta)$, which can also be expressed as $\cos^2\left(\frac{\pi}{2} - \theta\right)$ [3].

If instead of using a horizontally or vertically aligned polarizer, we use a polarizer tilted at 45 degrees, some photons will pass with a certain probability density, while others will be blocked. This will depend on the specific experimental arrangement being used.

1.2.5 Principle of Superposition

The principle of superposition is a fundamental characteristic of quantum mechanics. It states that any linear combination of two or more quantum states, provided they are normalized, is also a valid quantum state. Additionally, any quantum state that satisfies this condition can be expressed as a linear combination of a set of basis states, such as $|0\rangle$ and $|1\rangle$, or $|+\rangle$ and $|-\rangle$. These orthonormal bases, formed by the 2^n states of bit strings, are known as *computational bases*.

When dealing with systems of three or more qubits, as in previous examples,

these can be decomposed using tensor products. However, in quantum mechanics, there exist states that cannot be represented as tensor products of individual qubits independently. An example of this type of state is the entangled state $|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$. Systems that cannot be expressed as tensor products of their individual qubits are called *entangled states*.

Entanglement is a crucial property in quantum computing, as it allows the creation of a complex vector space of dimension 2^n using only n qubits. This property is one of the reasons why quantum computers can be more powerful than classical computers.

Suppose a quantum system with k energy levels, which we can express in Dirac notation as $|0\rangle, |1\rangle, |2\rangle, \ldots, |k-1\rangle$. The general state of the system can be represented according to the superposition principle as a linear combination of these states:

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle + \cdots + \alpha_{k-1} |k-1\rangle \tag{1.65}$$

Where $\alpha_j \in \mathbb{C}$, and the normalization condition must be satisfied:

$$\sum_{j=0}^{k-1} |\alpha_j|^2 = 1 \tag{1.66}$$

Additionally, the axiom of measurement probability states that the probability of obtaining a specific state $|j\rangle$ when performing a measurement is:

$$\mathbb{P}\left[[]\, j\right] = |\alpha_j|^2 \tag{1.67}$$

After performing the measurement, the system will collapse to a new state, which we call $|\psi'\rangle$.

When working with multiple qubits, the system states are represented by tensor products. For example, if we have two qubits, the tensor product of their states is expressed as:

$$\begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} ac \\ ad \\ bc \\ bd \end{bmatrix} \tag{1.68}$$

For this system to be normalized, it must be satisfied that the sum of the probabilities of all possible states equals one:

$$|ac|^2 + |ad|^2 + |bc|^2 + |bd|^2 = 1 \tag{1.69}$$

Let us see a more specific example. Consider two qubits in a superposed state and represent it in tensor notation:

$$\begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} \otimes \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \end{bmatrix} \tag{1.70}$$

We verify that the postulate that the sum of probabilities equals one is satisfied:

$$\left|\frac{1}{2}\right|^2 + \left|\frac{1}{2}\right|^2 + \left|\frac{1}{2}\right|^2 + \left|\frac{1}{2}\right|^2 = 1 \tag{1.71}$$

The physical interpretation of this result is as follows: *There is a probability of* $\frac{1}{4}$ *or* 25% *that the system is in any of the states* $|00\rangle$, $|01\rangle$, $|10\rangle$ *or* $|11\rangle$.

Example of the Superposition Principle

Consider a quantum system in a superposition of states:

$$|\psi\rangle = \left(\frac{1}{2} + \frac{i}{2}\right)|0\rangle - \frac{1}{2}|1\rangle + \left(\frac{i}{2}\right)|2\rangle \tag{1.72}$$

When measuring the system, what is the probability of finding the system in states $|0\rangle$, $|1\rangle$ or $|2\rangle$? What is the new state $|\psi'\rangle$ of the system after each measurement?

Solution

According to equation $\mathbb{P}\left[[]\, j\right] = |\alpha_j|^2$, we can calculate the probabilities for each of the states:

- State $|0\rangle$: The probability of finding the system in state $|0\rangle$ is:

$$\mathbb{P}\left[[]\, 0\right] = \left|\frac{1}{2} + \frac{i}{2}\right|^2 = \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2} \tag{1.73}$$

The new state of the system after this measurement would be $|\psi'\rangle = |0\rangle$.

- State $|1\rangle$: The probability of finding the system in state $|1\rangle$ is:

$$\mathbb{P}\left[[]\, 1\right] = \left|-\frac{1}{2}\right|^2 = \frac{1}{4} \tag{1.74}$$

The new state of the system after this measurement would be $|\psi'\rangle = |1\rangle$.

- State $|2\rangle$: The probability of finding the system in state $|2\rangle$ is:

$$\mathbb{P}\left[[]\, 2\right] = \left|\frac{i}{2}\right|^2 = \frac{1}{4} \tag{1.75}$$

The new state of the system after this measurement would be $|\psi'\rangle = |2\rangle$.

1.2.6 Geometric Interpretation for a System with k Energy Levels

The state $|\psi\rangle \in \mathbb{C}^k$ can be represented as a unit vector in a Hilbert space $\mathbb{C}^k$. For a system with three energy levels, we can write:

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle + \alpha_2 |2\rangle = \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \end{bmatrix} \tag{1.76}$$

where $\alpha_j \in \mathbb{C}$ and it is satisfied that:

$$\sum_{j=0}^{k-1} |\alpha_j|^2 = 1 \tag{1.77}$$

The probability of finding the system in a specific state, such as $|0\rangle$, is expressed as:

$$\mathbb{P}\left[[]\, 0\right] = \cos^2(\theta) \tag{1.78}$$

To define the angle θ between two states $|\psi\rangle$ and $|\phi\rangle$, we first define these states as:

$$|\psi\rangle = \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \end{bmatrix}, \quad |\phi\rangle = \begin{bmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \end{bmatrix} \tag{1.79}$$

The inner product between these two states is defined as:

$$\langle\psi| \, |\phi\rangle = \overline{\alpha_0}\beta_0 + \overline{\alpha_1}\beta_1 + \overline{\alpha_2}\beta_2 \tag{1.80}$$

Now, let us consider what happens when we perform measurements in a rotated orthonormal basis, such as $|+\rangle$ and $|-\rangle$, instead of the original basis $|0\rangle$ and $|1\rangle$. We define the new basis as:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{1.81}$$

Consider, as a concrete example, the state $|\psi\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$. If we measure it in this new basis, the probability of finding state $|+\rangle$ is, using $\langle +|\psi\rangle = \frac{1}{\sqrt{2}}\left(\frac{1}{2} + \frac{\sqrt{3}}{2}\right)$:

$$\mathbb{P}\left[[]\, +\right] = |\langle +|\psi\rangle|^2 = \left(\frac{1}{2\sqrt{2}} + \frac{\sqrt{3}}{2\sqrt{2}}\right)^2 = \frac{2+\sqrt{3}}{4} \tag{1.82}$$

And the probability of finding state $|-\rangle$ is:

$$\mathbb{P}\left[[]\, -\right] = \frac{2-\sqrt{3}}{4} \tag{1.83}$$

The new state of the system after measurement is expressed as:

$$|\psi\rangle = \left(\frac{1+\sqrt{3}}{2\sqrt{2}}\right)|+\rangle + \left(\frac{1-\sqrt{3}}{2\sqrt{2}}\right)|-\rangle \tag{1.84}$$

Thus, the probabilities of obtaining $|+\rangle$ or $|-\rangle$ are the same regardless of the chosen basis, demonstrating that probability density is independent of the chosen coordinate system.

1.2.7 Fidelity as a Measure of State Proximity

The practical implementation of quantum information protocols necessitates quantitative metrics for comparing quantum states. While classical states admit straightforward distance measures—binary strings differ in their Hamming distance, probability distributions in their total variation—quantum states require a more subtle treatment due to the phase degrees of freedom and normalization constraints inherent in Hilbert space geometry.

The *fidelity* between two pure quantum states $|\psi\rangle$ and $|\phi\rangle$ quantifies their proximity through the squared overlap:

$$F(|\psi\rangle, |\phi\rangle) = |\langle\psi|\phi\rangle|^2 \tag{1.85}$$

This definition possesses several essential properties. The fidelity takes values in the interval $[0, 1]$, achieving its maximum $F = 1$ if and only if the states are identical up to an irrelevant global phase, and its minimum $F = 0$ for orthogonal states. Notably, fidelity is invariant under unitary transformations: $F(\mathbf{U}|\psi\rangle, \mathbf{U}|\phi\rangle) = F(|\psi\rangle, |\phi\rangle)$ for any unitary operator $\mathbf{U}$, reflecting the physical equivalence of states related by reversible evolution.

Consider a target state $|\psi\rangle = |0\rangle$ and an imperfectly prepared state $|\phi\rangle = \cos(\epsilon)|0\rangle + \sin(\epsilon)|1\rangle$, where ϵ parametrizes the preparation error. The fidelity computes as:

$$F = |\langle 0|\phi\rangle|^2 = |\cos(\epsilon)|^2 = \cos^2(\epsilon) \tag{1.86}$$

For small errors $\epsilon \ll 1$, Taylor expansion yields $F \approx 1 - \epsilon^2$, demonstrating that fidelity exhibits quadratic sensitivity to angular deviations in the Bloch sphere representation. This quadratic scaling has profound implications for error thresholds in quantum error correction: protocols typically require gate fidelities exceeding 99.9% (corresponding to $\epsilon \lesssim 0.03$ radians) to satisfy the conditions of the threshold theorem.

The extension to mixed states requires the density matrix formalism. For density operators ρ and σ, the Uhlmann fidelity is defined as:

$$F(\rho, \sigma) = \left[\mathrm{Tr}\left(\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right)\right]^2 \tag{1.87}$$

where the square root of an operator $\mathbf{A}$ denotes the unique positive operator $\mathbf{B}$ satisfying $\mathbf{B}^2 = \mathbf{A}$. This expression reduces to the pure-state definition when

both $\rho = |\psi\rangle\langle\psi|$ and $\sigma = |\phi\rangle\langle\phi|$ represent pure states. For the important special case where σ is pure, the formula simplifies considerably:

$$F(\rho, |\phi\rangle\langle\phi|) = \langle\phi|\rho|\phi\rangle \tag{1.88}$$

Contemporary quantum processors achieve fidelities that determine their computational capabilities. Single-qubit gates in superconducting transmon qubits routinely exceed $F > 99.9\%$, while two-qubit entangling gates operate at $F \sim 99\%$. State preparation and measurement (SPAM) errors contribute additional infidelity, typically limiting readout fidelity to $95 - 99\%$ depending on the measurement protocol. These empirical benchmarks establish the operational regime of noisy intermediate-scale quantum (NISQ) devices and motivate the development of error mitigation techniques for near-term applications preceding full fault tolerance.

1.2.8 Representation of Multiple Qubits

In the representation of multiple qubits, we use tensor product notation to describe their combined states. For example, quantum states $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$ are represented as follows:

$$|00\rangle = \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}1\\0\\0\\0\end{bmatrix} \tag{1.89}$$

$$|01\rangle = \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}0\\1\\0\\0\end{bmatrix} \tag{1.90}$$

$$|10\rangle = \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}0\\0\\1\\0\end{bmatrix} \tag{1.91}$$

$$|11\rangle = \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}0\\0\\0\\1\end{bmatrix} \tag{1.92}$$

This representation extends naturally to more qubits. For example, state $|100\rangle$ can be expressed as:

$$\begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}0\\0\\0\\0\\1\\0\\0\\0\end{bmatrix} \tag{1.93}$$

This approach is known as the tensor representation of quantum states. This notation is especially useful, as it allows factoring the tensor product to return to the representation of individual states, which facilitates the manipulation and analysis of quantum systems with multiple qubits. Additionally, this method generalizes to n qubits, producing a state vector with 2^n components, which reflects the dimensionality of the corresponding Hilbert space.

Two Qubits: Detailed Example

In this section, we will explore the interaction of two qubits and how their quantum states are described. The general equation for a two-qubit system can be expressed as:

$$|\psi\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle \tag{1.94}$$

where the coefficients α_{ij} belong to the domain of complex numbers $\mathbb{C}$. These coefficients must satisfy the normalization condition:

$$\sum |\alpha_{ij}|^2 = 1 \tag{1.95}$$

This condition ensures that the sum of the probabilities of the possible quantum states equals one. When performing measurements on this quantum system, the probabilities of finding the system in the different possible states are expressed as:

$$\mathbb{P}\left[[]\,00\right] = |\alpha_{00}|^2, \quad \mathbb{P}\left[[]\,01\right] = |\alpha_{01}|^2, \quad \mathbb{P}\left[[]\,10\right] = |\alpha_{10}|^2, \quad \mathbb{P}\left[[]\,11\right] = |\alpha_{11}|^2 \tag{1.96}$$

Example of Probabilities and Measurements in Two Qubits

Consider a quantum system described by the following state equation:

$$|\psi\rangle = \left(\frac{1}{2} + \frac{i}{2}\right)|00\rangle + \frac{1}{2}\,|01\rangle - \frac{i}{2}\,|11\rangle \tag{1.97}$$

Problem: What are the probabilities of finding the system in states $|00\rangle$, $|01\rangle$, and $|11\rangle$? What is the result of measuring only the first qubit?

The probabilities of finding the system in each of the mentioned states are calculated as follows:

$$\mathbb{P}\left[[]\,00\right] = \left|\frac{1}{2} + \frac{i}{2}\right|^2 = \frac{1}{2}, \quad \mathbb{P}\left[[]\,01\right] = \left|\frac{1}{2}\right|^2 = \frac{1}{4}, \quad \mathbb{P}\left[[]\,11\right] = \left|\frac{-i}{2}\right|^2 = \frac{1}{4} \tag{1.98}$$

Now, if we perform a measurement of the first qubit, the probability of obtaining the result $|0\rangle$ is calculated by summing the probabilities of states $|00\rangle$ and $|01\rangle$:

$$\mathbb{P}\left[[]\,0\right] = |\alpha_{00}|^2 + |\alpha_{01}|^2 = \frac{1}{2} + \frac{1}{4} = \frac{3}{4} \tag{1.99}$$

The new state of the system, conditioned on obtaining the first qubit in state $|0\rangle$, can be written as:

$$|\psi'\rangle = \frac{\alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}} \tag{1.100}$$

For the given system, this new state is:

$$|\psi'\rangle = \frac{\left(\frac{1}{2} + \frac{i}{2}\right)|00\rangle + \frac{1}{2}\,|01\rangle}{\sqrt{\frac{3}{4}}} = \frac{\left(\frac{1}{2} + \frac{i}{2}\right)|00\rangle + \frac{1}{2}\,|01\rangle}{\frac{\sqrt{3}}{2}} \tag{1.101}$$

This result reflects the normalization of the quantum state after measurement, showing how the probability of states adjusts after measuring one of the qubits.

1.2.9 Rotational Invariance of States

Consider a system composed of two qubits that are in an entangled state. The quantum state of these two qubits can be represented as:

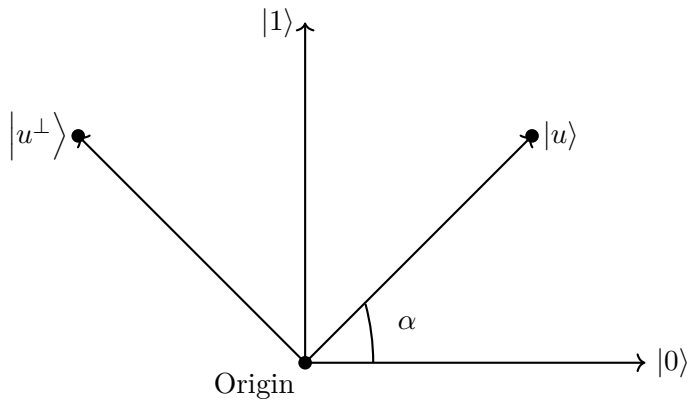
$$|\psi\rangle = \frac{1}{\sqrt{2}}\,|00\rangle + \frac{1}{\sqrt{2}}\,|11\rangle \tag{1.102}$$

This state is an example of what is known as a Bell state, which is a type of maximum entangled state. Now, let us analyze how this state behaves when we express it in a different basis, for example, in a rotated basis $|u\rangle$, $\left|u^{\perp}\right\rangle$, where $\left|u^{\perp}\right\rangle$ is the state orthogonal to $|u\rangle$. In this new basis, the state $|\psi\rangle$ can be rewritten as:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\,|uu\rangle + \frac{1}{\sqrt{2}}\left|u^{\perp}u^{\perp}\right\rangle \tag{1.103}$$

This means that if we measure both qubits in the $|u\rangle$ basis, there is a 50% probability ($\frac{1}{\sqrt{2}}$ squared) that both qubits are in state $|u\rangle$, and a 50% probability that both are in state $\left|u^{\perp}\right\rangle$.

The bases $|u\rangle$, $\left|u^{\perp}\right\rangle$ for qubits 1 and 2 can be visualized graphically as follows:



If we rotate the basis $|u\rangle$, $\left|u^{\perp}\right\rangle$ by an angle θ to obtain a new basis $|v\rangle$, $\left|v^{\perp}\right\rangle$, the quantum state of the system remains invariant in its form, but the probabilities of finding the system in the new states $|v\rangle$ and $\left|v^{\perp}\right\rangle$ change according to the rotation. Specifically, the probabilities will be given by:

$$\mathbb{P}\left[[]\, v\right] = \cos^2(\theta), \quad \mathbb{P}\left[[]\, v^{\perp}\right] = \sin^2(\theta) \tag{1.104}$$

This result shows that the probabilities of measurement outcomes depend on the angle of rotation between the bases. However, what is invariant is the fact that the quantum state remains entangled and that the superposition relationship is preserved under rotation, meaning that the structure of the state does not change—only the probabilities in the new basis are rearranged.

This property is called *rotational invariance*. It is a fundamental characteristic in quantum mechanics, especially in entangled systems, and is crucial for understanding phenomena such as Bell inequalities and non-local quantum correlations.

Rotational Invariance and Bell Inequalities

The rotational invariance of quantum states is key in demonstrating Bell inequalities and proof of quantum non-locality. According to quantum theory, correlations measured in an entangled system can violate Bell inequalities, which cannot be explained by any local hidden variable theory. This fact highlights how rotational invariance and quantum superposition challenge classical intuitions about the physical world [2].

Applications in Quantum Computing

In quantum computing, rotational invariance allows manipulating qubits in different bases, which is essential for implementing quantum algorithms and performing quantum operations. For example, quantum gates, such as Hadamard or Pauli gates, can be understood as operations that rotate qubits in Hilbert space, changing their probabilities according to the applied rotation angles.

1.3 The EPR Paradox and Bell Inequalities: Exploring Quantum Non-locality

The EPR paradox, posed by Albert Einstein, Boris Podolsky and Nathan Rosen in 1935, is one of the most fundamental and debated questions in quantum mechanics. The paradox arises from Einstein and his colleagues' concern about the apparent incompleteness of quantum mechanics, as follows from the principle of superposition and quantum entanglement. The paradox is formulated in terms of two particles that have interacted and, therefore, are in an entangled quantum state. According to the Copenhagen interpretation, the system state is not determined until a measurement is performed on one of the particles, which instantaneously determines the state of the other particle, regardless of the distance separating them. This phenomenon was what Einstein called "spooky action at a distance".

To formalize the paradox, consider a pair of particles in an entangled state, described by the wave function:

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

If we measure the spin of the first particle in some direction, suppose we obtain $|0\rangle$. Immediately, the second particle collapses to state $|0\rangle$ as well, and the same occurs if we measure $|1\rangle$. The paradox arises when considering that if the two particles are separated by a great distance, any change in the state of the second particle must occur instantaneously when the first is measured, which seems to violate the locality principle of special relativity, which states that no signal or interaction can travel faster than light.

In 1964, John Bell mathematically formulated this problem through the inequalities that bear his name, which are derived under the assumption that there exist local hidden variables that predetermine the measurement outcomes. Bell inequalities establish an upper limit on the correlations that can exist between measurements of entangled particles if they are governed by a local hidden variable theory. Consider two observables A and B measured on two entangled particles, with results taking values ± 1. Bell showed that if a local realist theory exists, the following inequality must be satisfied:

$$\langle AB\rangle - \langle AB'\rangle + \langle A'B\rangle + \langle A'B'\rangle \leq 2$$

However, when experiments are performed with entangled particles, such as those by Alain Aspect in the 1980s, it is observed that correlations violate Bell inequalities, that is, the left side of the equation can be greater than 2, which suggests that entangled particles can influence each other in a way that cannot be explained by any local hidden variable theory. This result reinforces the quantum interpretation in which locality and realism are replaced by a non-locality inherent to quantum mechanics, where quantum correlations cannot be explained classically [8].

1.3.1 Bell Inequalities

Bell inequalities, formulated by John S. Bell in 1964, are a series of inequalities that allow distinguishing between the predictions of quantum mechanics and local hidden variable theories. These inequalities provide an experimental way to test the intrinsic non-locality of quantum mechanics.

To understand the derivation of Bell inequalities, it is important to consider two fundamental concepts:

- **Realism**: The belief that physical properties exist and have defined values independent of whether they are measured or not.
- **Locality**: The idea that a physical influence cannot propagate faster than the speed of light, that is, that an event at one point cannot instantaneously affect another event at a distant point.

Local hidden variable theories are based on these two principles, postulating that measurement outcomes are determined by preexisting (hidden) variables and that no information can travel faster than light.

Consider a pair of entangled particles moving in opposite directions toward two observers, Alice and Bob, located at distant places. Both can perform measurements on their respective particles, choosing between two different measurement configurations:

- Alice chooses between observables A and A'.
- Bob chooses between observables B and B'.

Each measurement can result in $+1$ or -1.

1.3.2 Hidden Variables

We introduce a hidden variable λ, which represents the complete set of parameters that completely determine the measurement outcomes. We assume that λ is distributed according to a probability density function $\rho(\lambda)$, normalized such that:

$$\int \rho(\lambda)\, d\lambda = 1 \tag{1.105}$$

Alice and Bob's measurement outcomes depend on λ and the chosen measurement configuration:

$$\begin{aligned} A(\lambda) \in \{+1, -1\}, \quad A'(\lambda) \in \{+1, -1\} \\ B(\lambda) \in \{+1, -1\}, \quad B'(\lambda) \in \{+1, -1\} \end{aligned} \tag{1.106}$$

1.3.3 Derivation of Bell's Inequality

Consider the correlation between Alice and Bob's results for different measurement configurations:

$$E(X, Y) = \int A_X(\lambda) B_Y(\lambda) \rho(\lambda)\, d\lambda \tag{1.107}$$

where X and Y can be different measurement configurations (A, A', B, B').
Now define the following combination of correlations:

$$S = E(A, B) - E(A, B') + E(A', B) + E(A', B') \tag{1.108}$$

Proceed to evaluate S:

$$\begin{aligned} S &= \int [A(\lambda)B(\lambda) - A(\lambda)B'(\lambda) + A'(\lambda)B(\lambda) + A'(\lambda)B'(\lambda)]\rho(\lambda)\, d\lambda \\ &= \int [A(\lambda)(B(\lambda) - B'(\lambda)) + A'(\lambda)(B(\lambda) + B'(\lambda))]\rho(\lambda)\, d\lambda \end{aligned} \tag{1.109}$$

Note that, since $A(\lambda)$ and $A'(\lambda)$ take values of ± 1, we can apply the following property:

$$|A(\lambda)(B(\lambda) - B'(\lambda)) + A'(\lambda)(B(\lambda) + B'(\lambda))| \leq 2 \tag{1.110}$$

This is because $B(\lambda)$ and $B'(\lambda)$ also take values of ± 1, so the expression inside the absolute value can be at most 2.
Therefore:

$$|S| \leq \int 2 \cdot \rho(\lambda)\, d\lambda = 2 \tag{1.111}$$

This is **Bell's inequality**, also known as the **CHSH inequality** (by Clauser, Horne, Shimony and Holt):

$$|S| \leq 2 \tag{1.112}$$

1.3.4 Quantum Predictions

Now, let us analyze what quantum mechanics predicts for this same scenario. Consider that the particles are in the entangled Bell state:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{1.113}$$

We define Alice and Bob's observables in terms of Pauli operators:

$$\begin{aligned} A &= \sigma_{\mathbf{a}}, \quad A' = \sigma_{\mathbf{a}'} \\ B &= \sigma_{\mathbf{b}}, \quad B' = \sigma_{\mathbf{b}'} \end{aligned} \tag{1.114}$$

where $\sigma_{\mathbf{n}} = \mathbf{n} \cdot \boldsymbol{\sigma}$, and $\boldsymbol{\sigma}$ is the Pauli matrix vector, and $\mathbf{n}$ is a unit vector indicating the measurement direction.

The quantum correlation between measurements is:

$$E_{QM}(\mathbf{a}, \mathbf{b}) = \langle\psi| \sigma_{\mathbf{a}} \otimes \sigma_{\mathbf{b}} |\psi\rangle = \cos(\theta_{\mathbf{a},\mathbf{b}}) \tag{1.115}$$

where $\theta_{\mathbf{a},\mathbf{b}}$ is the angle between the measurement directions $\mathbf{a}$ and $\mathbf{b}$, both taken in the x–z plane. (For the state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ the correlation is $+\cos\theta$; the singlet state $|\Psi^-\rangle$ would instead give $-\cos\theta$.)

Appropriately choosing the measurement directions, for example:

$$\begin{aligned} \mathbf{a} &= 0^\circ, \quad \mathbf{a}' = 90^\circ \\ \mathbf{b} &= 45^\circ, \quad \mathbf{b}' = 135^\circ \end{aligned} \tag{1.116}$$

We obtain:

$$\begin{aligned} E_{QM}(\mathbf{a}, \mathbf{b}) &= \cos(45^\circ) = \frac{\sqrt{2}}{2} \\ E_{QM}(\mathbf{a}, \mathbf{b}') &= \cos(135^\circ) = -\frac{\sqrt{2}}{2} \\ E_{QM}(\mathbf{a}', \mathbf{b}) &= \cos(45^\circ) = \frac{\sqrt{2}}{2} \\ E_{QM}(\mathbf{a}', \mathbf{b}') &= \cos(45^\circ) = \frac{\sqrt{2}}{2} \end{aligned} \tag{1.117}$$

where each angle is the separation between the two directions: $\theta_{\mathbf{a},\mathbf{b}} = 45^\circ$, $\theta_{\mathbf{a},\mathbf{b}'} = 135^\circ$, $\theta_{\mathbf{a}',\mathbf{b}} = 45^\circ$, and $\theta_{\mathbf{a}',\mathbf{b}'} = 45^\circ$. Calculating S:

$$\begin{aligned} S_{QM} &= E_{QM}(\mathbf{a}, \mathbf{b}) - E_{QM}(\mathbf{a}, \mathbf{b}') + E_{QM}(\mathbf{a}', \mathbf{b}) + E_{QM}(\mathbf{a}', \mathbf{b}') \\ &= \frac{\sqrt{2}}{2} - \left(-\frac{\sqrt{2}}{2}\right) + \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} \\ &= 4 \cdot \frac{\sqrt{2}}{2} = 2\sqrt{2} \\ |S_{QM}| &= 2\sqrt{2} \approx 2.828 \end{aligned} \tag{1.118}$$

This value, $|S_{QM}| = 2\sqrt{2}$, is the maximum violation permitted by quantum mechanics, known as *Tsirelson's bound*.

We observe that $|S_{QM}| > 2$, which violates Bell's inequality. This implies that quantum mechanics predictions cannot be explained by any local hidden variable theory.

The violation of Bell inequalities has been confirmed experimentally on multiple occasions, with Alain Aspect's experiments in the 1980s being particularly notable. These experiments demonstrated that quantum correlations between entangled particles exceed the limits imposed by local hidden variable theories, thus supporting the non-local nature of quantum mechanics and refuting the possibility of a classical explanation of these phenomena.

These results have profound implications for our understanding of physical reality and have laid the groundwork for the development of technologies such as quantum cryptography and quantum computing, which exploit entanglement and non-locality properties to perform tasks that would be impossible within the framework of classical physics.

1.4 Key Experiments Confirming Bell Inequalities

The three key experiments that confirmed Bell inequalities are fundamental in the history of quantum mechanics, as they provided solid experimental evidence of quantum non-locality and refuted local hidden variable theories. The following describes these experiments in detail.

1.4.1 Freedman and Clauser Experiment (1972)

The first successful experiment to test Bell inequalities was performed by Stuart Freedman and John Clauser in 1972 at the University of California, Berkeley. This experiment was pioneering in experimentally confirming quantum predictions related to entanglement and Bell inequality violation.

Freedman and Clauser used excited calcium atoms to produce pairs of entangled photons through the atomic cascade process. The photons were emitted in opposite directions and detected using polarizers on both sides. Unlike Aspect's experiments, the polarizers in this experiment did not change their configuration during photon flight.

The researchers measured correlations between photon polarizations and compared results with quantum mechanics predictions and expectations of local hidden variable theories.

The experiment showed a violation of Bell inequalities, confirming that correlations between photons could not be explained by any local theory. Although the results were not as conclusive as Aspect's, this experiment was the first to demonstrate experimental violation of Bell inequalities [7].

The Freedman and Clauser experiment was fundamental in establishing the viability of testing Bell inequalities experimentally and paved the way for more

refined experiments, such as Aspect's. It was a crucial first step in demonstrating that quantum mechanics could not be reconciled with local realist theories.

1.4.2 Alain Aspect Experiment (1981-1982)

French physicist Alain Aspect carried out a series of experiments between 1981 and 1982 at the Institute of Optics at the University of Paris. These experiments were designed to directly test Bell inequalities using a pair of entangled photons.

Aspect used a process known as parametric down-conversion, in which an ultraviolet photon strikes a nonlinear crystal and produces two entangled photons in opposite directions. The entangled photons were sent to two polarizers located at different detection stations, distant from each other.

Aspect introduced a key innovation in his experiment: the ability to change polarizer configurations during photon flight, using high-frequency modulators. This avoided the possibility that any signal could travel between detectors at the speed of light and adjust results, eliminating possible "communication loopholes" that could have allowed a local explanation [1].

Aspect's experimental results showed clear violations of Bell inequalities, which implied that correlations between entangled photons could not be explained by any local hidden variable theory. The measurements confirmed quantum mechanics predictions with a high degree of confidence.

Aspect's experiment is considered a milestone because it resolved earlier criticisms about possible flaws in previous experiments. Additionally, it convincingly demonstrated that reality cannot be completely described by local hidden variable theories, which supported the quantum interpretation of non-locality.

1.4.3 Zeilinger, Weihs, Jennewein, and Others Experiment (1998)

The experiment led by Anton Zeilinger and his team in 1998 at the University of Innsbruck, Austria, is notable for closing the "configuration loophole" and further improving experimental tests of quantum non-locality.

This experiment used a configuration similar to Aspect's, with the generation of entangled photons through parametric down-conversion. The key difference was the improvement in photon detection and implementation of a greater degree of spatial separation between detection stations, which were more than 400 meters apart.

Additionally, Zeilinger and his team used a mechanism of random polarization configuration change, which ensured that measurement choices were truly independent and made at the last minute, further reducing the possibility that any hidden signal could affect results.

Zeilinger's experiment showed an even more robust violation of Bell inequalities, with great spatial separation and independent measurement times, which made earlier criticisms about possible "loopholes" even less plausible.

This experiment was one of the first to implement what is known as a "loophole-free Bell test", in which the main loopholes (such as configuration and commu-

nication) that could have allowed alternative explanations are closed. It was a significant step toward definitive demonstration of quantum non-locality and has been fundamental for the development of advanced quantum technologies, such as quantum cryptography and quantum teleportation.

These three experiments, performed at different times and with different levels of technological sophistication, have provided solid experimental confirmation that Bell inequalities are violated, meaning that the quantum world cannot be explained by local hidden variable theories. Each of these experiments significantly contributed to our understanding of quantum mechanics and has laid the groundwork for future quantum technologies [16].

1.4.4 Loophole-Free Bell Experiment (2015)

The definitive experiment that consolidated the validity of Alain Aspect's and other previous experiments' results, confirming non-locality in quantum mechanics, was carried out in 2015 by a team led by Ronald Hanson at Delft University of Technology (Netherlands). This experiment is known as the **"loophole-free Bell test"** [9].

The experiment's objective was to verify whether quantum correlations violate Bell inequalities without the presence of the main experimental loopholes that had been discussed in previous tests, such as the detection loophole (limited efficiency of detectors) and the locality loophole (possible communication between particles during the experiment).

Individual electrons trapped in nitrogen-vacancy centers in diamonds separated by more than one kilometer were used. Entanglement states were generated between the electrons, and measurements were performed under spatially separated configurations. The researchers used randomly selected measurement configurations to ensure that decisions could not be causally influenced by the particles.

A violation of Bell inequalities was observed, confirming that quantum correlations cannot be explained by local hidden variable theories. The experiment eliminated any possible classical communication between particles, resolving the critical experimental loopholes that affected previous tests.

Impact:

This experiment offered the strongest evidence to date that the quantum world is inherently non-local, and that quantum correlations cannot be explained within the framework of a classical theory with local realism. It equally consolidated the modern quantum interpretation based on entanglement.

1.5 The First Quantum Computer

The first successful experiment with a quantum computer was performed in 1998 by a team of MIT researchers, led by Isaac Chuang, Neil Gershenfeld, and Mark Kubinec. This experiment is notable because it successfully implemented a 2-qubit quantum computer using nuclear magnetic resonance (NMR) in chloroform molecules ($CHCl_3$). In this system, the qubits were represented by the nuclear spins of the carbon-13 atom and the hydrogen atom [6].

In this experiment, the researchers used the NMR technique to manipulate and read the quantum state of the two qubits in the chloroform molecule. The qubits were initially prepared in a specific state through radiofrequency pulses, and then quantum logic operations were applied to perform a simple quantum algorithm, known as the Deutsch-Jozsa algorithm. This algorithm is significant because, in an ideal quantum computer, it allows determining whether a function is constant or balanced with just one evaluation, while in a classical computer multiple evaluations would be required.

Basic Calculation Performed in the Experiment

The initial state of the two qubits can be described as:

$$|\psi\rangle = |00\rangle$$

After applying a Hadamard gate (H) to both qubits, the system state is:

$$H \otimes H\,|00\rangle = \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

Next, function $f(x)$ corresponding to the Deutsch-Jozsa algorithm was applied, which, in the balanced case, changes the sign of one of the terms. Finally, another Hadamard gate is applied to both qubits and measurement is performed.

The obtained results confirmed the system's ability to perform quantum operations, demonstrating the principle of superposition and quantum parallelism in a real system.

The experiment successfully demonstrated the operation of a 2-qubit quantum computer, which was an important milestone in the history of quantum computing. This system allowed performing basic quantum calculations and showed the viability of quantum computing using NMR techniques. Although limited in the number of qubits and calculation complexity, this experiment was the first practical implementation of a quantum algorithm on quantum hardware, earning it the title of "first quantum computer".

This experiment laid the groundwork for future developments in quantum computing, demonstrating that it was possible to build and operate a coherent and controllable quantum system on a small scale.

1.6 Theorems: No-Cloning, No-Deleting, No-Hiding in Quantum Information

Quantum measurements are usually considered destructive, since when measuring a quantum system, we inevitably alter its state. Faced with this reality, one might think about the possibility of making an exact copy of the system before measuring it, in order to preserve the original state. However, quantum information theory prohibits exact cloning of arbitrary quantum states, a principle known as the **no-cloning theorem** [17].

In classical computing, information can be copied and deleted at will. However, in quantum computing, information conservation implies that it cannot be arbitrarily created or destroyed. This concept derives from two fundamental theorems: the **no-cloning theorem** and the **no-deleting theorem**. A third theorem, related to quantum information conservation, is the **no-hiding theorem**, proposed by physicists Samuel L. Braunstein and Arun K. Pati in 2007 [4].

1.6.1 No-Cloning Theorem

In 1982, William Wootters and Wojciech Zurek, together with Dennis Dieks working independently, formulated the no-cloning theorem, which states that *it is not possible to construct a device that, according to the unitary properties of quantum mechanics, performs an exact copy of an arbitrary quantum state.* This theorem has important implications in quantum computing and quantum cryptography. For example, in quantum cryptography, it guarantees that messages encoded in quantum states cannot be copied by a spy without being detected [17].

***Proof of the theorem:**

Suppose we have a quantum state $|\psi\rangle$ that we want to copy into an auxiliary system $|X\rangle$. Ideally, the device would copy the state as follows:

$$\mathbf{U}(|\psi\rangle\,|X\rangle) = |\psi\rangle\,|\psi\rangle$$

Where $\mathbf{U}$ is a unitary operator. However, due to the linearity of quantum mechanics, if we consider an arbitrary quantum state $|\psi\rangle = \alpha\,|\psi_1\rangle + \beta\,|\psi_2\rangle$, the cloning operation would produce:

$$\mathbf{U}(|\psi\rangle\,|X\rangle) = \alpha\,|\psi_1\rangle\,|\psi_1\rangle + \beta\,|\psi_2\rangle\,|\psi_2\rangle$$

This is not equal to $(\alpha\,|\psi_1\rangle + \beta\,|\psi_2\rangle)\,(\alpha\,|\psi_1\rangle + \beta\,|\psi_2\rangle)$, which demonstrates that an arbitrary quantum state cannot be cloned without altering the original state.

Physical Consequences and Circumventions

The no-cloning theorem imposes fundamental constraints on quantum information processing that distinguish it sharply from classical computation. In classical systems, arbitrary copying operations $\text{COPY} : (x, 0) \mapsto (x, x)$ represent standard primitives, enabling fault tolerance through redundancy, backup storage, and information broadcast. The prohibition of analogous quantum operations necessitates alternative paradigms for error management and information distribution.

The most profound implication manifests in quantum error correction. Since $|\psi\rangle$ cannot be cloned, naive approaches to fault tolerance—maintaining multiple identical copies to detect and correct errors through majority voting—fail immediately. The resolution, pioneered by Shor [14] and Steane [15], employs a subtle strategy: encoding a single logical qubit into an entangled state of multiple physical qubits. The nine-qubit Shor code, for instance, embeds one logical qubit as:

$$|\bar{0}\rangle = \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)^{\otimes 3}, \quad |\bar{1}\rangle = \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle)^{\otimes 3} \tag{1.119}$$

Error syndromes are extracted through ancilla measurements that project onto subspaces without collapsing the logical qubit state itself—a mechanism respecting no-cloning while achieving redundancy sufficient to correct arbitrary single-qubit errors.

Quantum cryptography derives its information-theoretic security directly from no-cloning. In the BB84 protocol, Alice transmits qubits to Bob encoded in non-orthogonal states drawn from conjugate bases. An eavesdropper Eve cannot clone these states to retain a copy while forwarding an undisturbed original to Bob. Any measurement strategy Eve employs necessarily introduces detectable disturbances: the no-cloning theorem guarantees that quantum key distribution achieves security rooted in physical law rather than computational hardness assumptions.

The theorem does not prohibit all forms of quantum state transfer or duplication. Quantum teleportation circumvents no-cloning by destroying the original state: Alice's qubit at location A and Bob's reconstituted qubit at location B never simultaneously exist, satisfying the constraint that total information remains conserved. Similarly, while perfect universal cloning fails, approximate cloning succeeds with optimal fidelity $F = \frac{5}{6}$ for qubits [5]. For known states from a discrete set, probabilistic exact cloning becomes possible—the key restriction is the impossibility of deterministically cloning arbitrary unknown states.

The no-cloning theorem also provides a consistency check for quantum mechanics itself. Were cloning possible, one could measure complementary observables on cloned copies, violating the Heisenberg uncertainty principle. Consider a qubit in state $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$. If cloning succeeded, producing $|\psi\rangle \otimes |\psi\rangle$, one could measure the first copy in the $\{|0\rangle, |1\rangle\}$ basis to determine $|\alpha|^2$ and $|\beta|^2$, then measure the second copy in the $\{|+\rangle, |-\rangle\}$ basis to extract phase information. These complementary measurements would yield complete knowledge of α and β, including their relative phase—information that quantum mechanics

forbids obtaining from a single system. Thus no-cloning serves as a consistency requirement preserving the probabilistic structure of quantum theory.

1.6.2 No-Deleting Theorem

The no-deleting theorem, which complements the no-cloning theorem, states that *it is not possible to completely delete information from a quantum state without leaving a trace elsewhere in the universe.* This principle derives from quantum information conservation and reinforces the idea that quantum information cannot be created or destroyed at will.

1.6.3 No-Hiding Theorem

In 2007, Braunstein and Pati introduced the no-hiding theorem, which states that *if information is missing in a quantum system, it must reside elsewhere in the universe; it cannot be hidden in correlations between a system and its environment.* In other words, quantum information that appears to be "lost" due to decoherence or interaction with the environment, is not actually destroyed, but rather redistributed in the universe.

In 2010, Jharana Rani Samal and her team achieved the first experimental proof of the no-hiding theorem, confirming that quantum information continues to be conserved, even when it appears to have been lost. The results of this experiment were published in 2011, consolidating the no-hiding theorem as a cornerstone of quantum information theory [12].

Consequences and Applications of the Theorems

The no-cloning theorem has profound implications in quantum computing, especially in the field of error correction. Unlike classical computing, it is not possible to make backup copies of a quantum state in the middle of a calculation to correct later errors. This presented a significant challenge until Peter Shor and Andrew Steane proposed the first quantum error correction codes in 1995, partially overcoming the limitations imposed by the no-cloning theorem.

Additionally, the no-cloning theorem also protects Heisenberg's uncertainty principle. If arbitrary quantum states could be cloned, it would be possible to measure any variable with arbitrary precision, thus violating this fundamental principle of quantum mechanics.

On the other hand, the no-cloning theorem prohibits faster-than-light communication using quantum entanglement, maintaining causality in relativistic physics.

Although perfect cloning is impossible, it is possible to create imperfect or approximate copies of a quantum state, which may have applications in eavesdropping attacks in quantum cryptography and other uses in quantum computing.

Regarding the no-hiding theorem, its experimental verification supports the idea that quantum information is always conserved, even if it appears to have been lost. This has important implications for quantum coherence and the development of secure quantum communication protocols.

Summary

In this chapter, we have explored the fundamental concepts of quantum computing, beginning with the representation of quantum information through qubits and the essential difference between classical and quantum computing. We discussed the principle of superposition, which allows a qubit to exist in multiple states simultaneously, which is crucial for quantum parallelism. This principle was illustrated through detailed mathematical examples, showing how probabilities of different states are calculated and how the quantum system collapses to a defined state after measurement.

We also explored the graphical representation of qubits using the Bloch sphere, which provides an intuitive visualization of quantum states and their transformations. Additionally, we discussed the concept of quantum entanglement, where the states of multiple qubits become entangled in such a way that they cannot be described independently of each other, which is fundamental to the power of quantum computing.

Bell inequalities were presented and analyzed, along with the EPR paradox, to demonstrate quantum non-locality and how these properties have been experimentally confirmed, challenging classical intuitions about the nature of reality. The three key experiments that verified these inequalities and their implications for quantum physics were detailed.

Finally, a section on the first quantum computer built at MIT in 1998 was included, highlighting its historical importance as the first quantum system that performed basic calculations using qubits. This milestone in the history of quantum computing demonstrated the viability of building and operating a coherent quantum system on a small scale.

This chapter lays the foundation for understanding quantum computing and prepares the way for exploring more complex quantum algorithms and systems with multiple qubits in subsequent chapters.

Bridge to the Next Chapter

We have established the mathematical and physical foundations of qubits. In Chapter 5, we will study **quantum gates** (unitary operators) that manipulate these qubits, enabling the construction of quantum circuits and algorithms. We will see how the unitary matrices we studied here are physically implemented and how they combine to perform universal quantum computation.

Key questions for Chapter 5:

- What are the fundamental single-qubit gates (X, Y, Z, H, T)?
- How do we construct multi-qubit gates (CNOT, Toffoli)?
- What gates are needed for universal quantum computation?
- How are gates implemented in real quantum hardware?

1.7 Exercises

Exercise 1: Pauli Matrix Algebra

The Pauli matrices σ_x, σ_y, and σ_z form a non-commutative algebra fundamental to qubit manipulation. Consider a qubit in the general pure state $|\psi\rangle = \cos(\theta/2)\,|0\rangle + e^{i\phi}\sin(\theta/2)\,|1\rangle$.

(a) Apply each Pauli operator to $|\psi\rangle$ and express the resulting states in terms of θ and ϕ.

(b) Verify by explicit calculation that $\sigma_x^2 = \sigma_y^2 = \sigma_z^2 = \mathbf{I}$, where $\mathbf{I}$ denotes the 2×2 identity matrix.

(c) Compute the commutators $[\sigma_i, \sigma_j] = \sigma_i\sigma_j - \sigma_j\sigma_i$ for all pairs $(i, j) \in \{x, y, z\}^2$. Express your results in terms of the Pauli matrices and the imaginary unit.

(d) Calculate the expectation values $\langle\sigma_x\rangle_\psi$, $\langle\sigma_y\rangle_\psi$, and $\langle\sigma_z\rangle_\psi$ for the state $|\psi\rangle$ defined above. Verify that these expectation values correspond to the Cartesian coordinates of the Bloch vector $(x, y, z) = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$.

Exercise 2: Tensor Product Calculations

Consider two qubits prepared in the states $|\psi_1\rangle = \frac{1}{\sqrt{3}}\,|0\rangle + \sqrt{\frac{2}{3}}\,|1\rangle$ and $|\psi_2\rangle = \frac{1}{2}\,|0\rangle + \frac{\sqrt{3}}{2}\,|1\rangle$.

(a) Construct the composite state $|\Psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ by computing the tensor product. Express your answer as a superposition over the computational basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

(b) Calculate the probability of measuring each computational basis state. Verify that these probabilities sum to unity.

(c) Suppose a measurement is performed on the first qubit only, yielding the outcome $|0\rangle$. What is the post-measurement state of the second qubit? What is the probability that this measurement outcome occurred?

(d) Compare the calculation in part (c) with measuring both qubits simultaneously and post-selecting on outcomes where the first qubit is $|0\rangle$. Explain why these procedures yield identical results.

Exercise 3: Measurements in Non-Computational Bases

The standard computational basis $\{|0\rangle, |1\rangle\}$ represents only one of infinitely many orthonormal bases for the single-qubit Hilbert space. Consider the state $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

(a) Calculate the probability of obtaining outcome $|+\rangle$ when measuring in the basis $\{|+\rangle, |-\rangle\}$ where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$.

(b) More generally, consider the rotated basis $\{|\theta\rangle, \left|\theta^\perp\right\rangle\}$ defined by:

$$|\theta\rangle = \cos(\theta/2)\,|0\rangle + \sin(\theta/2)\,|1\rangle, \quad \left|\theta^\perp\right\rangle = -\sin(\theta/2)\,|0\rangle + \cos(\theta/2)\,|1\rangle$$

Derive the probabilities $P(\theta)$ and $P(\theta^\perp)$ of measuring $|\psi\rangle$ in these basis states as functions of θ.

(c) Verify that $P(\theta) + P(\theta^{\perp}) = 1$ for all values of $\theta \in [0, 2\pi)$, confirming probability conservation.

(d) At what angle θ is the measurement outcome maximally uncertain (i.e., both probabilities equal 1/2)? Interpret this result geometrically on the Bloch sphere.

Exercise 4: Quantum Entanglement and Measurement Correlations

The Bell state $\left|\Phi^{+}\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ exhibits perfect correlations between spatially separated measurements.

(a) Suppose Alice measures her qubit in the computational basis $\{|0\rangle, |1\rangle\}$ and obtains outcome $|0\rangle$. What is the state of Bob's qubit after Alice's measurement? What is the probability that Alice obtained this outcome?

(b) Repeat part (a) assuming Alice instead measures in the basis $\{|+\rangle, |-\rangle\}$. Show that Bob's reduced state depends on Alice's measurement basis choice, even though they are spatially separated.

(c) Express $\left|\Phi^{+}\right\rangle$ in the product basis $\{|++\rangle, |+-\rangle, |-+\rangle, |--\rangle\}$. Verify that the state retains its maximally entangled character in this alternative representation.

(d) Calculate the correlation function $E(\theta_A, \theta_B) = \left\langle\Phi^{+}\right| (\sigma_z^A \otimes \sigma_z^B) \left|\Phi^{+}\right\rangle$ where subscripts indicate on which qubit the Pauli operator acts. Generalize to measurements along arbitrary directions $\hat{n}_A = (\sin\theta_A, 0, \cos\theta_A)$ and $\hat{n}_B = (\sin\theta_B, 0, \cos\theta_B)$ on the Bloch sphere.

Exercise 5: Bell Inequality Violation

Consider the CHSH inequality derived from local hidden variable theories: $|S| \leq 2$ where $S = E(A, B) - E(A, B') + E(A', B) + E(A', B')$.

(a) For the Bell state $|\Phi^{-}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$, choose measurement directions $A = \sigma_z$, $A' = \sigma_x$, $B = \frac{1}{\sqrt{2}}(\sigma_z + \sigma_x)$, and $B' = \frac{1}{\sqrt{2}}(\sigma_z - \sigma_x)$. Calculate each correlation function $E(X, Y) = \langle\Phi^{-}| (X \otimes Y) |\Phi^{-}\rangle$.

(b) Evaluate S using the correlations from part (a). Demonstrate explicitly that $|S| > 2$, violating the CHSH inequality.

(c) Explain physically why local hidden variable theories must satisfy $|S| \leq 2$. What assumption is violated by the quantum mechanical prediction?

(d) The maximal quantum violation of the CHSH inequality is $|S|_{\max} = 2\sqrt{2}$ (Tsirelson's bound). Argue on physical grounds why $|S|$ cannot exceed 4 for any theory, quantum or otherwise, that respects basic locality and signal causality constraints.

Exercise 6: Coherence Time Requirements

A quantum algorithm implementing Grover's search over a database of $N = 1024$ elements requires approximately $\frac{\pi}{4}\sqrt{N} \approx 25$ iterations. Each iteration consists of 20 gates, and each gate operation requires 50 ns.

(a) Calculate the total execution time for the algorithm.

(b) If the qubit coherence time is $T_2 = 25$ μs, what fraction of the coherence time is consumed by the algorithm?

(c) To ensure reliable operation, a conservative design rule requires execution time $t_{\text{exec}} \leq T_2/5$. Does this algorithm satisfy this criterion? If not, what minimum coherence time is required?

(d) Suppose each gate has infidelity $\epsilon = 0.1\%$ (fidelity $F = 99.9\%$). Assuming errors compound independently, estimate the total algorithm fidelity using $F_{\text{total}} \approx (1-\epsilon)^{n_{\text{gates}}}$. Is this sufficient for obtaining the correct result with probability exceeding 90%?

Exercise 7: Separability and Entanglement Detection

Determine whether each of the following two-qubit states is separable or entangled. For separable states, provide the explicit factorization $|\phi_1\rangle \otimes |\phi_2\rangle$. For entangled states, prove non-separability by contradiction.

(a) $|\psi_1\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$

(b) $|\psi_2\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$

(c) $|\psi_3\rangle = \frac{1}{\sqrt{3}}|00\rangle + \sqrt{\frac{2}{3}}|11\rangle$

(d) For the entangled states identified above, calculate the *concurrence* $C(|\psi\rangle) = |\alpha\delta - \beta\gamma|$ where $|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$. The concurrence quantifies entanglement, with $C = 0$ for separable states and $C = 1$ for maximally entangled Bell states.

Exercise 8: Fidelity and State Discrimination

Two quantum states $|\psi\rangle$ and $|\phi\rangle$ can be distinguished with certainty only if they are orthogonal.

(a) Calculate the fidelity $F(|\psi\rangle, |\phi\rangle)$ for $|\psi\rangle = |0\rangle$ and $|\phi\rangle = \cos(\epsilon)|0\rangle + \sin(\epsilon)|1\rangle$ where $\epsilon \ll 1$. Show that $F \approx 1 - \epsilon^2/2$ to leading order in ϵ.

(b) Suppose you possess a single copy of an unknown state guaranteed to be either $|\psi\rangle$ or $|\phi\rangle$. Design an optimal measurement strategy (i.e., specify an orthonormal basis $\{|m_0\rangle, |m_1\rangle\}$) that maximizes the probability of correctly identifying which state you have.

(c) Calculate the maximum success probability P_{succ} for the optimal strategy in part (b) as a function of ϵ. Verify that $P_{\text{succ}} \to 1$ as $\epsilon \to \pi/2$ (orthogonal states) and $P_{\text{succ}} \to 1/2$ as $\epsilon \to 0$ (identical states).

(d) Explain why the no-cloning theorem implies that perfect state discrimination is impossible for non-orthogonal states. If cloning were possible, how could one achieve $P_{\text{succ}} = 1$ for any $\epsilon > 0$?