## Summer of Code

# Quantum Computing: From Theory to Practice

Aakash Tarang


IIT BOMBAY

June 2025

# Contents


**1 Linear Algebra** **1**

1.1 Vector Space $\mathbb{C}^n$ . . . 1
1.2 Bases and Linear Independence . . . 1
1.3 Linear Operators and Matrices . . . 2
1.4 The Pauli Matrices . . . 2
1.5 Inner Product . . . 2
1.5.1 Definition . . . 2
1.5.2 Properties . . . 3
1.5.3 Important Concepts . . . 3
1.6 Hilbert Space . . . 3
1.7 Gram-Schmidt Orthogonalization . . . 3
1.8 Outer Product . . . 4
1.9 Special Operators . . . 4
1.9.1 Hermitian Operators . . . 4
1.9.2 Unitary Operators . . . 4
1.9.3 Positive Operators . . . 4
1.10 Eigenvectors and Eigenvalues . . . 4
1.11 Hermitian and Unitary Operators . . . 4
1.12 Projectors . . . 5
1.13 Tensor Products . . . 5
1.13.1 Tensor Product Examples and Notation . . . 5
1.14 Operator Functions . . . 6
1.15 Commutators and Anti-commutators . . . 6
1.16 Matrix Decompositions . . . 7
1.17 Matrix Exponentials . . . 7
1.18 Trace . . . 7

**2 Quantum Measurement Theory** **9**

2.1 The Standard Lore and Its Limitations . . . 9
2.1.1 Traditional Quantum Measurement Framework . . . 9
2.1.2 Limitations of the Standard Framework . . . 9
2.1.3 Table Explanation . . . 10

**3 Introduction to Quantum Computing** **11**

3.1 The Quantum Advantage . . . 11
3.2 Historical Milestones . . . 11
3.3 A practical example : **Superdense Coding** . . . 11

**4 Qubits and Quantum Gates** **13**
4.1 Qubit States . . . 13
4.2 Superposition Principle . . . 13
4.3 Bloch Sphere Representation . . . 13
4.4 Single-Qubit Gates . . . 13
4.5 Quantum Dynamics . . . 14
4.6 Key Properties . . . 14

**5 Quantum Search** **15**
5.1 Grover's Algorithm . . . 15

# CHAPTER 1

# Linear Algebra

## 1.1 Vector Space $\mathbb{C}^n$

A vector space of complex numbers is a set of $n$-tuples of complex numbers, whose elements are called vectors, which satisfy certain vector space axioms. The vectors are indicated using column matrix notation:

$$\begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix}$$

In $\mathbb{C}^n$, addition for vectors is defined as:

$$\begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix} + \begin{bmatrix} z'_1 \\ \vdots \\ z'_n \end{bmatrix} = \begin{bmatrix} z_1 + z'_1 \\ \vdots \\ z_n + z'_n \end{bmatrix}$$

Multiplication is defined as:

$$z \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix} = \begin{bmatrix} zz_1 \\ \vdots \\ zz_n \end{bmatrix}$$

The standard quantum mechanical notation for representing a vector in a vector space is $|\psi\rangle$, where $\psi$ is a label for the vector, and the entire expression is called a ket.

The zero vector is represented by 0 (the ket notation is not used for the zero vector).

A vector subspace of a vector space $V$ is a subset $W$ of $V$ such that $W$ is also a vector space.

## 1.2 Bases and Linear Independence

A spanning set for a vector space is a set of vectors $\{|v_1\rangle, \ldots, |v_n\rangle\}$ such that any vector $|v\rangle$ in the vector space can be written as a linear combination $|v\rangle = \sum_i a_i |v_i\rangle$ of vectors in that set.

A set of non-zero vectors $\{|v_1\rangle, \ldots, |v_n\rangle\}$ are linearly dependent if there exists a set of complex numbers $a_1, \ldots, a_n$ with $a_i \neq 0$ for at least one value of $i$, such that:

$$a_1 |v_1\rangle + a_2 |v_2\rangle + \cdots + a_n |v_n\rangle = 0$$

A set of vectors is linearly independent if it is not linearly dependent. Any two sets of linearly independent vectors which span a vector space $V$ contain the same number of elements. Such a set is called a basis and the cardinality of a basis is called its dimension.

## 1.3 Linear Operators and Matrices

A linear operator between vector spaces $V$ and $W$ is defined to be any function $A : V \to W$ which is linear in its inputs:

$$A\left(\sum_i a_i |v_i\rangle\right) = \sum_i a_i A(|v_i\rangle)$$

An important linear operator on any vector space $V$ is the identity operator $I_V$ defined by $I_V |v\rangle = |v\rangle$ for all vectors $|v\rangle$. Another important linear operator is the zero operator denoted by 0 which maps all vectors to the zero vector, $0 |v\rangle = 0$.

Once the action of a linear operator $A$ on a basis is specified, the action of $A$ is completely determined on all inputs.

Suppose $V$, $W$, and $X$ are vector spaces, and $A : V \to W$ and $B : W \to X$ are linear operators. Then $BA$ denotes the composition of $B$ with $A$, defined as $BA |v\rangle = B(A(|v\rangle))$.

Linear operators can be understood in terms of their matrix representations. Matrices can be regarded as linear operators and linear operators can be represented as matrices, thereby making the two completely equivalent. Suppose $A : V \to W$ is a linear operator between vector spaces $V$ and $W$. Suppose $\{|v_1\rangle, \ldots, |v_m\rangle\}$ is a basis for $V$ and $\{|w_1\rangle, \ldots, |w_n\rangle\}$ is a basis for $W$. Then for each $j$ in the range $1, \ldots, m$, there exist complex numbers $A_{1j}$ through $A_{nj}$ such that:

$$A |v_j\rangle = \sum_i A_{ij} |w_i\rangle$$

The matrix whose entries are the values $A_{ij}$ is said to form a matrix representation of the operator $A$.

## 1.4 The Pauli Matrices

Four useful $2 \times 2$ matrices used occasionally are the Pauli matrices:

$$\sigma_0 = I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \sigma_1 = \sigma_x = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\sigma_2 = \sigma_y = Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_3 = \sigma_z = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

## 1.5 Inner Product

An inner product is a function that takes two vectors $|v\rangle$ and $|w\rangle$ from a vector space and produces a complex number, denoted $\langle v|w\rangle$.

### 1.5.1 Definition

In quantum mechanics, the inner product is typically defined as:

$$\langle v|w\rangle = \int v^*(x) w(x) t(x) dx$$

where $t(x)$ is a weight factor (e.g., $t(x) = 1$ for Cartesian coordinates, $t(x) = r^2 \sin\theta$ for spherical coordinates).

### 1.5.2 Properties

- **Linearity in the second argument**:

$$\langle v|aw_1 + bw_2\rangle = a\langle v|w_1\rangle + b\langle v|w_2\rangle$$

- **Conjugate symmetry**:

$$\langle v|w\rangle = \langle w|v\rangle^*$$

- **Positive-definiteness**:

$$\langle v|v\rangle \geq 0 \quad \text{with equality iff } |v\rangle = 0$$

- **Orthogonality**:

$$\langle v|w\rangle = 0 \quad \text{if } |v\rangle \text{ and } |w\rangle \text{ are orthogonal}$$

### 1.5.3 Important Concepts

- **Norm**: $\| |v\rangle \| = \sqrt{\langle v|v\rangle}$
- **Cauchy-Schwarz inequality**:

$$|\langle v|w\rangle|^2 \leq \langle v|v\rangle \langle w|w\rangle$$

- **Triangle inequality**:

$$\| |v\rangle + |w\rangle \| \leq \| |v\rangle \| + \| |w\rangle \|$$

- **Projection**:

$$\text{proj}_w(v) = \frac{\langle w|v\rangle}{\langle w|w\rangle} |w\rangle$$

## 1.6 Hilbert Space

In quantum computation, a Hilbert space is an inner product space with additional completeness properties. Key features:

- $\langle v|$ is the dual vector (bra) to $|v\rangle$ (ket)
- Vectors $|w\rangle$ and $|v\rangle$ are orthogonal if $\langle w|v\rangle = 0$
- A set $\{|i\rangle\}$ is orthonormal if $\langle i|j\rangle = \delta_{ij}$

## 1.7 Gram-Schmidt Orthogonalization

Given a basis $\{|w_1\rangle, ..., |w_d\rangle\}$, we can construct an orthonormal basis $\{|v_1\rangle, ..., |v_d\rangle\}$:

$$|v_1\rangle = \frac{|w_1\rangle}{\| |w_1\rangle \|}, \quad |v_{k+1}\rangle = \frac{|w_{k+1}\rangle - \sum_{i=1}^{k} \langle v_i|w_{k+1}\rangle |v_i\rangle}{\| |w_{k+1}\rangle - \sum_{i=1}^{k} \langle v_i|w_{k+1}\rangle |v_i\rangle \|}$$

## 1.8 Outer Product

The outer product $|w\rangle\langle v|$ is a linear operator defined by:

$$(|w\rangle\langle v|)(|v'\rangle) = \langle v|v'\rangle|w\rangle$$

Key applications:

- **Projection operator**: $P = |v\rangle\langle v|$
- **Completeness relation**: $\sum_i |i\rangle\langle i| = I$
- **Operator representation**: $A = \sum_{ij} \langle w_j|A|v_i\rangle |w_j\rangle\langle v_i|$

## 1.9 Special Operators

### 1.9.1 Hermitian Operators

An operator $A$ is Hermitian if $A^\dagger = A$, where:

$$\langle v|A|w\rangle = \langle A^\dagger v|w\rangle = \langle w|A|v\rangle^*$$

### 1.9.2 Unitary Operators

An operator $U$ is unitary if $UU^\dagger = I$. They preserve inner products:

$$\langle Uv|Uw\rangle = \langle v|w\rangle$$

### 1.9.3 Positive Operators

An operator $A$ is positive if $\langle v|A|v\rangle \geq 0$ for all $|v\rangle$.

## 1.10 Eigenvectors and Eigenvalues

Let $A$ be a linear operator on vector space $V$. A non-zero vector $|v\rangle$ is an **eigenvector** of $A$ with **eigenvalue** $v \in \mathbb{C}$ if:

$$A|v\rangle = v|v\rangle$$

The **eigenspace** for eigenvalue $v$ is the subspace of all corresponding eigenvectors.

An operator is **diagonalizable** if it has a **diagonal representation**:

$$A = \sum_i \lambda_i |i\rangle\langle i|$$

where $\{|i\rangle\}$ form an orthonormal eigenbasis with eigenvalues $\lambda_i$.

## 1.11 Hermitian and Unitary Operators

The **adjoint** $A^\dagger$ satisfies:

$$(|v\rangle, A|w\rangle) = (A^\dagger|v\rangle, |w\rangle)$$

In matrix form, $A^\dagger = (A^*)^T$.

Key operator classes:

- **Hermitian**: $A^\dagger = A$
- **Unitary**: $UU^\dagger = I$ (preserves inner products)
- **Normal**: $AA^\dagger = A^\dagger A$ (diagonalizable)
- **Positive**: $\langle v|A|v\rangle \geq 0$ for all $|v\rangle$

## 1.12 Projectors

For subspace $W \subseteq V$ with orthonormal basis $\{|i\rangle\}_{i=1}^{k}$, the **projector** is:

$$P = \sum_{i=1}^{k} |i\rangle \langle i|$$

Properties:

- $P^\dagger = P$ (Hermitian)
- $P^2 = P$ (idempotent)
- $Q = I - P$ is the orthogonal complement

## 1.13 Tensor Products

For vector spaces $V$ and $W$, the tensor product $V \otimes W$ has:

- Elements: linear combinations of $|v\rangle \otimes |w\rangle$
- Basis: $\{|i\rangle \otimes |j\rangle\}$ for bases $\{|i\rangle\}$, $\{|j\rangle\}$
- Operator action: $(A \otimes B)(|v\rangle \otimes |w\rangle) = A|v\rangle \otimes B|w\rangle$

### 1.13.1 Tensor Product Examples and Notation

The tensor product combines vectors from different vector spaces, essential for constructing multi-qubit systems in quantum computing.

#### Why Tensor Products? (Enlarging the Hilbert Space)

- **Purpose**:
  - A single qubit lives in a 2D Hilbert space ($\mathbb{C}^2$)
  - For $n$ qubits, the state space must describe all $2^n$ possible combinations
  - The tensor product $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2 = \mathbb{C}^{2^n}$ gives the correct dimension
- **Physical Interpretation**:
  - Combines independent systems: $|0\rangle \otimes |1\rangle = |01\rangle$
  - Emerges naturally from quantum mechanics postulates
  - Physically achieved through qubit coupling (e.g., trapped ions, superconducting circuits)

#### Notation

- $|a\rangle \otimes |b\rangle$ - Explicit tensor product
- $|ab\rangle$ or $|a, b\rangle$ - Common shorthand
- $|abc\rangle \equiv |a\rangle \otimes |b\rangle \otimes |c\rangle$ - Multi-qubit states
- $|00010001111\rangle$ - 11-qubit state (one-hot encoded)

**One-Hot Encoded States**

States like $|00010001111\rangle$ represent:

- Binary string interpretation: $00010001111_2 = 271_{10}$
- One-hot vector with 1 at position 271 (0-indexed)
- In $\mathbb{C}^{2048}$ space (since $2^{11} = 2048$)
- Computational basis state for 11-qubit systems

**Example: Two-Qubit System**

$$|00\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}$$

$$|01\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$$

$$|10\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}$$

$$|11\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

**Key Properties**

- **Dimension Growth**: $\dim(V^{\otimes n}) = (\dim V)^n$
- **Basis Construction**: $\{|i_1\rangle \otimes \cdots \otimes |i_n\rangle\}$ forms basis for $\mathbb{C}^{2^n}$
- **Physical Realization**: Implemented through quantum gates acting on multiple qubits (e.g., CNOT entangles qubits)

## 1.14 Operator Functions

For normal operator $A = \sum_a a\,|a\rangle\langle a|$ and function $f$:

$$f(A) = \sum_a f(a)\,|a\rangle\langle a|$$

## 1.15 Commutators and Anti-commutators

- **Commutator**: $[A, B] = AB - BA$
- **Anti-commutator**: $\{A, B\} = AB + BA$

**Simultaneous Diagonalization**: Hermitian $A$ and $B$ commute iff they share an eigenbasis.

## 1.16 Matrix Decompositions

- **Polar**: $A = UJ = KU$ with $U$ unitary, $J, K$ positive
- **SVD**: $A = UDV$ with $U, V$ unitary, $D$ diagonal
- **Spectral**: $A = \sum_i \lambda_i |i\rangle \langle i|$ for normal $A$

## 1.17 Matrix Exponentials

For Hermitian $H$:

$$e^{i\gamma H} = \sum_{n=0}^{\infty} \frac{(i\gamma H)^n}{n!}$$

If $B^2 = I$ (involutory):

$$e^{i\gamma B} = \cos(\gamma) I + i \sin(\gamma) B$$

## 1.18 Trace

The trace satisfies:

- $\operatorname{tr}(AB) = \operatorname{tr}(BA)$ (cyclic)
- $\operatorname{tr}(A + B) = \operatorname{tr}(A) + \operatorname{tr}(B)$ (linear)
- $\operatorname{tr}\left(UAU^\dagger\right) = \operatorname{tr}(A)$ (unitary invariance)
- $\operatorname{tr}(A |\psi\rangle \langle\psi|) = \langle\psi| A |\psi\rangle$

# CHAPTER 2

# Quantum Measurement Theory

## 2.1 The Standard Lore and Its Limitations

### 2.1.1 Traditional Quantum Measurement Framework

In conventional quantum mechanics courses, we learn the following postulates about quantum measurement:

- The **state** of a system is represented by a vector $|\psi\rangle$ in a Hilbert space $\mathcal{H}$
- **Observables** correspond to Hermitian operators $A = A^\dagger$ on $\mathcal{H}$
- The **spectral theorem** guarantees diagonalization: $A = \sum_a a \, |a\rangle \langle a|$
- Measurement yields outcome $a$ with probability $P(a) = |\langle a|\psi\rangle|^2$
- **State collapse** occurs: $|\psi\rangle \to |a\rangle$ after measurement

Table 2.1: The standard quantum measurement rules

| | **Pure states** | **General states** |
|---|---|---|
| **State** | $\|\psi\rangle \in \mathcal{H}$ | $\rho = \sum_i p_i \, \|i\rangle \langle i\|$ |
| **Measurement outcomes** | Eigenvalues $a$ of $A = A^\dagger$ | Same |
| **Probabilities** | $P(a) = \|\langle a\|\psi\rangle\|^2$ | $P(a) = \mathrm{tr}(\|a\rangle \langle a\| \, \rho)$ |
| **State update** | $\|\psi\rangle \to \|a\rangle$ | $\rho \to \|a\rangle \langle a\|$ |

### 2.1.2 Limitations of the Standard Framework

The traditional measurement paradigm has several notable limitations:

- **Measurement implementation unspecified**: The rules describe outcomes but provide no mechanism for how measurements are physically realized
- **Measurement problem**: The framework doesn't explain the transition from quantum superposition to definite measurement outcomes
- **Narrow applicability**: While valid for projective measurements, many realistic measurement scenarios don't fit this idealized picture
- **State collapse postulate**: The instantaneous nature of state collapse remains philosophically problematic and experimentally untestable

### 2.1.3 Table Explanation

Table 2.1 compares the measurement rules for pure states versus general (mixed) states:

- The **pure state** column describes systems with definite state vectors
- The **general state** column handles statistical mixtures using density matrices $\rho$
- Both cases share the same measurement outcomes (eigenvalues of $A$)
- Probability calculations differ: pure states use inner products while mixed states require the trace operation
- State update rules maintain consistency between the two representations

This traditional framework, while mathematically elegant, leaves open fundamental questions about the nature of measurement in quantum mechanics.

# CHAPTER 3

# Introduction to Quantum Computing

## 3.1 The Quantum Advantage

Quantum computing represents a paradigm shift from classical computing...

## 3.2 Historical Milestones

The concept was first proposed by Richard Feynman in 1982...

## 3.3 A practical example : Superdense Coding

# CHAPTER 4

# Qubits and Quantum Gates

## 4.1 Qubit States

A qubit is the quantum analog of a classical bit, with two basis states:

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

The general state of a qubit is a superposition:

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

## 4.2 Superposition Principle

Unlike classical bits, qubits can exist in superposition states that are linear combinations of the basis states:

- Enables parallel computation on multiple states
- Measurement collapses the state: $P(|x\rangle) = |\,\langle x|\psi\rangle\,|^2$
- Global phase ($e^{i\phi}$) is physically unobservable

## 4.3 Bloch Sphere Representation

Any qubit state can be visualized on the Bloch sphere:

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

- $|0\rangle$ at north pole, $|1\rangle$ at south pole
- $\theta$: polar angle, $\phi$: azimuthal angle

## 4.4 Single-Qubit Gates

Unitary operators acting on qubits:

- **Pauli gates**:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},\ Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

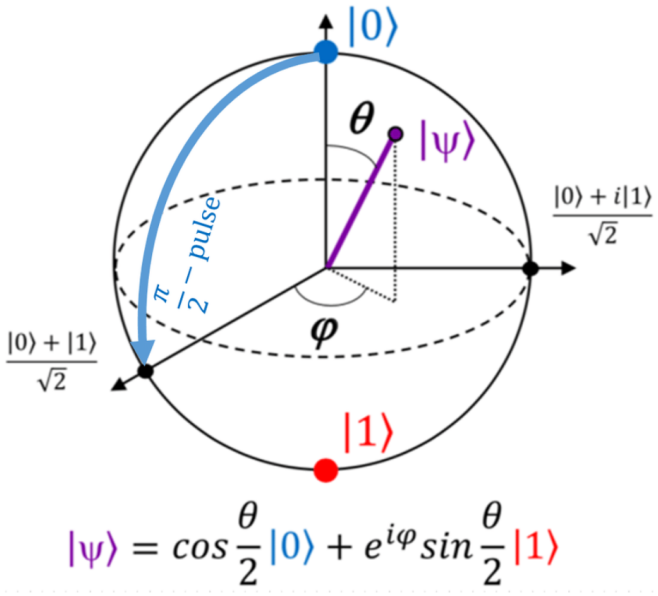


Figure 4.1: Block Sphere Representation

- **Hadamard** (creates superposition):

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

- **Phase gate**:

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

## 4.5 Quantum Dynamics

- Closed system evolution: $|\psi(t)\rangle = U(t)\,|\psi(0)\rangle$
- Governed by Schrödinger equation: $i\hbar \frac{d}{dt}\,|\psi\rangle = H\,|\psi\rangle$
- Hamiltonian generates unitary evolution: $U = e^{-iHt/\hbar}$

## 4.6 Key Properties

- **No-cloning**: Cannot copy unknown quantum states
- **Entanglement**: Qubits can exhibit non-classical correlations
- **Measurement**: Projective and irreversible

# CHAPTER 5

# Quantum Search

## 5.1 Grover's Algorithm