

Quantum Computing Fundamentals

PHYS 370

Spring 2025

Contents

1	Lecture 3: Quantum Gates and Circuits	3
1.1	Matrix Representation of Quantum Gates	3
1.2	Pauli Matrices as Quantum Gates	3
1.3	Controlled-NOT (CNOT) Gate	3
1.4	Hadamard Gate and Bell State Generation	3
1.5	Quantum Circuit Representation	4
1.6	Controlled Gates and Universal Quantum Gates	4
1.7	Gate Decomposition	4
1.8	No-Cloning Theorem and Quantum Cloning	4
1.9	Multi Qubit or Composite States	4
1.9.1	Tensor Product State	5
1.9.2	Bell States	5
1.9.3	CNOT 2-qubit Operator	6
1.10	Key Takeaways for Class Questions	6
2	Lecture 4: Advanced Quantum Operations	7
2.1	Checkpoint: Quiz Questions and Answers	7
2.2	No-Cloning Theorem	7
2.3	Quantum Teleportation	7
2.4	Superdense Coding	8
2.5	Tools of Quantum Information Theory	8
2.5.1	Fidelity and Distance Measures	8
3	Lecture 6: Operators in Quantum Mechanics	10
3.1	Adjoint and Hermitian Operators	10
3.2	Eigenvalues and Eigenvectors	11
3.3	Spectral Decomposition	13
3.4	The Trace of an Operator	13
3.5	The Expectation Value of an Operator	15
4	Lecture 7: Quantum Algorithms	16
4.1	Introduction to Quantum Algorithms	16
4.2	Mathematical Foundations	16
4.3	Hadamard Gates and Quantum Superposition	16
4.4	Parallel Hadamard Operations	16
4.5	Phase Gates	16
4.6	Matrix Representations	17
4.7	Deutsch's Algorithm	17
5	Lecture 8: Quantum Interference and Deutsch's Algorithm	18
5.1	Quantum Interference	18
5.2	Quantum Parallelism and Function Evaluation	18
5.3	Deutsch's Algorithm Implementation	18
5.4	Deutsch-Jozsa Algorithm	19

1. LECTURE 3: QUANTUM GATES AND CIRCUITS

January 29, 2025

1.1 Matrix Representation of Quantum Gates

In quantum computing, the state of an n -qubit system is represented by a 2^n -dimensional vector. Quantum gates are represented by $2^n \times 2^n$ unitary matrices. A six-qubit quantum gate must be represented by a 64×64 unitary matrix. The unitary condition:

$$U^\dagger U = U U^\dagger = I,$$

where U^\dagger is the Hermitian conjugate (conjugate transpose) of U .

1.2 Pauli Matrices as Quantum Gates

Definition 1.2.1 (Pauli Matrices). *The Pauli matrices (X, Y, Z) are fundamental single-qubit gates:*

$$\begin{aligned} X &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} & (\text{Bit-flip gate}) \\ Y &= \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} & (\text{Bit \& Phase-flip}) \\ Z &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} & (\text{Phase-flip gate}) \end{aligned}$$

These matrices are unitary ($U^\dagger = U^{-1}$) and Hermitian ($U = U^\dagger$), ensuring valid quantum operations.

1.3 Controlled-NOT (CNOT) Gate

Definition 1.3.1 (CNOT Gate). *The CNOT gate acts on two qubits, with one acting as a control and the other as a target. It performs a NOT operation on the target if and only if the control qubit is $|1\rangle$.*

Example 1.3.2 (CNOT Matrix Representation).

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

Theorem 1.3.3 (CNOT Action). *Using Dirac notation, its action is:*

$$\begin{aligned} |00\rangle &\rightarrow |00\rangle \\ |01\rangle &\rightarrow |01\rangle \\ |10\rangle &\rightarrow |11\rangle & (\text{flips target qubit}) \\ |11\rangle &\rightarrow |10\rangle \end{aligned}$$

1.4 Hadamard Gate and Bell State Generation

Definition 1.4.1 (Hadamard Gate). *The Hadamard gate (H) puts a qubit into an equal superposition:*

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

Example 1.4.2 (Bell State). *A fundamental Bell state:*

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

The circuit construction consists of:

1. Applying H to the first qubit.
2. Applying CNOT, with the first qubit as the control.
3. H turns the $|0\rangle$ into $|+\rangle$ and $|1\rangle$ into $|-\rangle$

1.5 Quantum Circuit Representation

- Wires represent qubits and their evolution through time, not physical movement.
- Single-qubit gates (X, H, Z , etc.) act on one qubit.
- Multi-qubit gates (CNOT, Toffoli) involve entanglement.
- Measurement collapses the quantum state and is usually represented by an encircled M in diagrams.

1.6 Controlled Gates and Universal Quantum Gates

Definition 1.6.1 (Controlled Gates). *Controlled gates allow conditional operations:*

- Controlled-Z (CZ): Applies a Z gate to the target when control is $|1\rangle$.
- Controlled-Hadamard (CH): Applies H to the target when control is $|1\rangle$.
- Toffoli Gate (CCNOT): Uses two control qubits and one target, flipping the target only when both controls are $|1\rangle$.
- Fredkin Gate (CSWAP): Swaps two qubits based on a control qubit.

1.7 Gate Decomposition

Complex multi-qubit gates can be decomposed into single-qubit gates and CNOTs. Example: Controlled- U decomposition replaces a controlled- U gate with a sequence of CNOTs and single-qubit rotations, used for efficient quantum circuit optimization.

1.8 No-Cloning Theorem and Quantum Cloning

Theorem 1.8.1 (No-Cloning). *The CNOT gate cannot clone an arbitrary quantum state due to the no-cloning theorem. Example: Trying to copy $\alpha|0\rangle + \beta|1\rangle$ results in entanglement, not an identical copy. Some specific states, like $|0\rangle$ or $|1\rangle$, can be cloned, but arbitrary superpositions cannot.*

1.9 Multi Qubit or Composite States

Definition 1.9.1 (Multi-Qubit States). • *An n -qubit diagram will have n wires/lines*

- *Tensor product state*
- *entangled states (Bell) $\alpha|0\rangle + \beta|1\rangle$ and $|1\rangle$ **bold***

1.9.1 Tensor Product State

Definition 1.9.2 (Tensor Product). *A tensor product state is a product of single-qubit states. An example of this is 2 $|0\rangle$ qubits in tensor product state: $|0\rangle \otimes |0\rangle = |0\rangle|0\rangle = |00\rangle$*

Example 1.9.3 (Matrix Representations). • $|00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$

• $|11\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$

• $|01\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$

1.9.2 Bell States

Bell states are quintessential entangled 2-qubit states. Pauli exclusion principle states that no two fermions can occupy the same quantum state. So if you have one electron spin up and one spin down, the sign is minus. Also, a cheat sheet for signs is any state with a 1 first is minus, and 0 first is plus.

Bell State 1 $|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$

- In this state you know the bit on the right by measuring the bit on the left.
- If the left bit is $|0\rangle$ then the right bit is $|0\rangle$
- If the left bit is $|1\rangle$ then the right bit is $|1\rangle$
- This is a Bell state because it is an entangled state.

Bell State 2 $|\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$

- In this state you know the bit on the left by measuring the bit on the right.
- If the right bit is $|0\rangle$ then the left bit is $|1\rangle$
- If the right bit is $|1\rangle$ then the left bit is $|0\rangle$
- This is a Bell state because it is an entangled state.

Bell State 3 $|\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$

- In this state you know the bit on the right by measuring the bit on the left.
- If the left bit is $|0\rangle$ then the right bit is $|1\rangle$
- If the left bit is $|1\rangle$ then the right bit is $|0\rangle$
- This is a Bell state because it is an entangled state.

Bell State 4 $|\beta_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$

- In this state you know the bit on the left by measuring the bit on the right.
- If the right bit is $|0\rangle$ then the left bit is $|1\rangle$
- If the right bit is $|1\rangle$ then the left bit is $|0\rangle$
- This is a Bell state because it is an entangled state.

1.9.3 CNOT 2-qubit Operator

Definition 1.9.4 (CNOT 2-qubit Operator). *To make Bell states we need the CNOT 2-qubit operator. Given by:*

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

- If the control qubit is $|0\rangle$ then the target qubit is unchanged.
- If the control qubit is $|1\rangle$ then the target qubit is flipped.

1.10 Key Takeaways for Class Questions

- What size matrix represents an n -qubit gate? $2^n \times 2^n$ unitary matrix.
- Why are Pauli matrices quantum gates? They are unitary and Hermitian.
- What is the role of CNOT? Flips the target qubit if the control is $|1\rangle$.
- How does Hadamard create superposition? Equal probability of $|0\rangle$ and $|1\rangle$.
- What do wires in a circuit mean? Time evolution of a quantum state.
- Can quantum states be cloned? No, due to the no-cloning theorem.

2. LECTURE 4: ADVANCED QUANTUM OPERATIONS

February 3, 2025

2.1 Checkpoint: Quiz Questions and Answers

Key Questions and Answers:

1. **Q: What is the problem with trying to make copies of quantum data?**
A: There is no unitary operator that exists which could be used to clone arbitrary quantum states, and so it simply isn't possible.
2. **Q: In the teleportation example with Alice and Bob, why is the overall interaction remarkable?**
A: Because a measurement on Alice's end seemingly 'caused' a change on Bob's end across space and time through no classical communication, only quantum.
3. **Q: Why is it necessary for Alice to make a measurement during the teleportation process?**
A: Because the very act of measurement will 'collapse' the unknown state into one of the other four possible states, depending on what Alice measures.

2.2 No-Cloning Theorem

Definition 2.2.1 (No-Cloning Theorem). *It is impossible to create an identical copy of an arbitrary unknown quantum state. There is no universal unitary operator that will allow us to create a copy of an arbitrary quantum state.*

Theorem 2.2.2 (Mathematical Explanation). *Suppose a unitary operation U could clone states:*

$$U(|\psi\rangle \otimes |\chi\rangle) = |\psi\rangle \otimes |\psi\rangle$$

$$U(|\phi\rangle \otimes |\chi\rangle) = |\phi\rangle \otimes |\phi\rangle$$

By taking the inner product and using the properties of unitarity, we reach a contradiction. This means cloning only works for orthogonal states but not for arbitrary quantum states.

2.3 Quantum Teleportation

Definition 2.3.1 (Quantum Teleportation). *Quantum teleportation allows the transfer of a quantum state from Alice to Bob using an entangled pair and classical communication.*

• **Key Steps:**

1. Alice and Bob share an **entangled Bell state or EPR(Einstein-Podolsky-Rosen) pair**
2. Alice **applies a CNOT gate and Hadamard gate** to her qubit
3. Alice **measures her qubits**, collapsing the system (her qubit vanishes)
4. Alice sends **classical information** (two classical bits or phone call) to Bob
5. Bob applies appropriate **quantum gate operations** (X, Z, or both)

Definition 2.3.2 (Quantum Teleportation). *Alice want to "send" a state $|\chi\rangle$ to Bob and:*

$$|\chi\rangle = \alpha|0\rangle + \beta|1\rangle$$

- **Key Steps:**

1. Alice and Bob share an entangled (Bell) state:

$$|\beta_{00}\rangle = \frac{|00\rangle_{AB} + |11\rangle_{AB}}{\sqrt{2}}$$

$$|\psi\rangle_1 = (\alpha|0\rangle_A + \beta|1\rangle_A) \otimes \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}) = \frac{\alpha}{\sqrt{2}}(|000\rangle_{AAB} + |011\rangle_{AAB}) + \frac{\beta}{\sqrt{2}}(|100\rangle_{AAB} + |111\rangle_{AAB})$$

2. Alice applies a CNOT operator with the control qubit from $|\chi\rangle$ and the target is Alice's member of entangled pair
3. Alice applies a Hadamard operator to the $|\chi\rangle$ qubit: $|\psi\rangle_2 = \frac{\alpha}{\sqrt{2}}|0\rangle_A \otimes (|00\rangle_{AB} + |11\rangle_{AB}) + \frac{\beta}{\sqrt{2}}(|1\rangle_A \otimes (|10\rangle_{AB} + |01\rangle_{AB}))$
4. Alice measures her two qubits
5. Alice sends **classical information** (two classical bits or phone call) to Bob
6. Bob applies appropriate **quantum gate operations** (X, Z, or both)

Important Note: Teleportation **does not allow faster-than-light communication** because classical communication is required.

2.4 Superdense Coding

Definition 2.4.1 (Superdense Coding). *A technique for sending two classical bits of information using only one qubit, leveraging entanglement.*

- **Process:**

1. Alice and Bob share an entangled qubit pair
2. Alice applies specific operations to encode two classical bits:
 - Identity (I) \rightarrow **00**
 - X gate \rightarrow **01**
 - Z gate \rightarrow **10**
 - ZX gate \rightarrow **11**
3. Alice sends the qubit to Bob
4. Bob measures in the Bell basis to extract information

2.5 Tools of Quantum Information Theory

2.5.1 Fidelity and Distance Measures

- **Trace Distance:** Measures how distinguishable two quantum states are
- **Fidelity:** Measures how similar two quantum states are
- **Entanglement Measures:** Concurrence and Entanglement of Formation quantify entanglement

Key Summary Points:

- Quantum teleportation and superdense coding demonstrate practical applications of entanglement
- The No-Cloning Theorem ensures security in quantum communication
- Quantum operations (Hadamard, CNOT) are fundamental for state manipulation
- Classical communication remains necessary despite quantum advantages

3. LECTURE 6: OPERATORS IN QUANTUM MECHANICS

February 10, 2025

3.1 Adjoints and Hermitian Operators

A final rule to note is that the adjoint of a sum is equal to the sum of the adjoints:

$$(\hat{A} + \hat{B} + \hat{C})^\dagger = \hat{A}^\dagger + \hat{B}^\dagger + \hat{C}^\dagger \quad (3.29)$$

Example 3.4: Find the adjoint of the operator $\hat{A} = 2|0\rangle\langle 1| - i|1\rangle\langle 0|$.

Solution: First we note that (3.29) tells us that

$$\hat{A}^\dagger = (2|0\rangle\langle 1|)^\dagger - (i|1\rangle\langle 0|)^\dagger.$$

We can compute the adjoint of each term by taking the complex conjugate of the constants in each expression and then applying the usual rules for bras and kets. We find that

$$\hat{A}^\dagger = 2|1\rangle\langle 0| + i|0\rangle\langle 1|.$$

You Try It: Show that the adjoint of

$$\hat{B} = \begin{pmatrix} 3i & 0 \\ 0 & 2i \end{pmatrix}$$

is given by

$$\hat{B}^\dagger = \begin{pmatrix} -3i & 0 \\ 0 & -2i \end{pmatrix}.$$

Considering the matrix representation of an operator, we compute its Hermitian adjoint in two steps:

- Compute the transpose of the matrix (swap rows and columns).
- Compute the complex conjugate of each element.

For a general 2×2 matrix given by

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad (3.30)$$

the Hermitian conjugate is

$$A^\dagger = \begin{pmatrix} a^* & c^* \\ b^* & d^* \end{pmatrix} \quad (3.31)$$

Definition 3.1.1 (Hermitian Operator). *An operator \hat{A} is said to be Hermitian if*

$$\hat{A} = \hat{A}^\dagger. \quad (3.32)$$

Clearly, the operator used in Example 3.3, $\hat{A} = \begin{pmatrix} 2 & 0 \\ 1 & i \end{pmatrix}$, is not Hermitian. However, the Pauli operators are Hermitian. For example, the operator Y is written as

$$Y = -i|0\rangle\langle 1| + i|1\rangle\langle 0|$$

using the computational basis. The adjoint of this expression is

$$Y^\dagger = (-i|0\rangle\langle 1| + i|1\rangle\langle 0|)^\dagger = i|1\rangle\langle 0| - i|0\rangle\langle 1| = Y \quad (3.33)$$

It turns out that in quantum mechanics, operators that represent physical observables are Hermitian.

The matrix representation of a Hermitian operator has real matrix elements along its diagonal. In the space \mathbb{C}^2 , given a matrix representation (3.30) it must be the case that a and d are real ($a = a^*$, $d = d^*$) and $c = b^*$.

Definition 3.1.2 (Unitary Operator). *The inverse of an operator \hat{A} is denoted by \hat{A}^{-1} . This operator satisfies $\hat{A}\hat{A}^{-1} = \hat{A}^{-1}\hat{A} = I$, where I is the identity operator. An operator is said to be unitary if its adjoint is equal to its inverse. Unitary operators are often denoted using the symbol U , and we can state its definition as*

$$UU^\dagger = U^\dagger U = I. \quad (3.34)$$

Unitary operators are important because they describe the time evolution of a quantum state. The Pauli operators are both Hermitian and Unitary.

Definition 3.1.3 (Normal Operator). *An operator \hat{A} is said to be normal if*

$$\hat{A}\hat{A}^\dagger = \hat{A}^\dagger\hat{A}. \quad (3.35)$$

Later in the chapter when we consider the commutator of two operators, we will see that this means a normal operator is one that commutes with its adjoint. Hermitian and unitary operators are normal.

3.2 Eigenvalues and Eigenvectors

A given vector is said to be an eigenvector of an operator \hat{A} if the following equation is satisfied, where λ is a complex number:

$$\hat{A}|\psi\rangle = \lambda|\psi\rangle.$$

The number λ is called an eigenvalue of the operator \hat{A} . For example, looking at (3.11) and Example 3.3, we see that the computational basis states are the eigenvectors of the Z operator.

A common problem in quantum mechanics is the following: given an operator, find its eigenvalues and eigenvectors. The first step in this process is to find the eigenvalues using what is known as the characteristic equation.

The Characteristic Equation: The characteristic equation for an operator \hat{A} is found by solving the following equation:

$$\det(\hat{A} - \lambda I) = 0, \quad (3.36)$$

where λ is an unknown variable, I is the identity matrix, and \det denotes the determinant of the matrix $\hat{A} - \lambda I$. The values of λ that are the solutions to this equation are the eigenvalues of the operator \hat{A} . The determinant of a 2×2 matrix (3.30) is

$$\det(A) = ad - bc. \quad (3.37)$$

Example 3.5: Find the eigenvalues of an operator with matrix representation

$$\begin{pmatrix} 2 & 1 \\ -1 & -1 \end{pmatrix}.$$

Solution: First we construct the matrix $A - \lambda I$:

$$A - \lambda I = \begin{pmatrix} 2 & 1 \\ -1 & -1 \end{pmatrix} - \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} = \begin{pmatrix} 2 - \lambda & 1 \\ -1 & -1 - \lambda \end{pmatrix}.$$

Then we compute the determinant:

$$\det(A - \lambda I) = (2 - \lambda)(-1 - \lambda) - (-1)(1).$$

Expanding:

$$(2 - \lambda)(-1 - \lambda) + 1 = -2 + \lambda - 2\lambda + \lambda^2 + 1 = \lambda^2 - \lambda - 1.$$

Setting this equal to zero, we get

$$\lambda^2 - \lambda - 1 = 0.$$

Solving via the quadratic formula,

$$\lambda_{1,2} = \frac{1 \pm \sqrt{5}}{2}.$$

You Try It: Using the matrix representation of the Z operator, show that its eigenvalues are ± 1 .

Once the eigenvalues are known, the eigenvectors can be found. This is done by writing out the eigenvalue equation

$$\hat{A}|\psi\rangle = \lambda|\psi\rangle$$

for each eigenvalue λ and an eigenvector $|\psi\rangle$ with unknown components that we call α, β . This leads to a set of equations we can solve. Usually the equations allow us to relate the two variables but leave one undetermined. In quantum mechanics, we also require normalization:

$$|\alpha|^2 + |\beta|^2 = 1.$$

Hence the procedure works as follows: 1. Solve the characteristic equation to find the eigenvalues. 2. For each eigenvalue, use the eigenvalue equation to generate relations among the components of the eigenvector. 3. Use the normalization condition to find those components.

If each of the eigenvectors of an operator is associated with a unique eigenvalue, we say that they are nondegenerate. If two or more eigenvectors are degenerate, this means that they correspond to the same eigenvalue.

Example 3.6: Find the eigenvalues and eigenvectors for the " $\pi/8$ " gate, which has the matrix representation

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

Solution: We begin by solving the characteristic equation:

$$0 = \det(T - \lambda I) = \det \begin{pmatrix} 1 - \lambda & 0 \\ 0 & e^{i\pi/4} - \lambda \end{pmatrix}.$$

Since the determinant of a diagonal matrix is the product of its diagonal elements, we have

$$(1 - \lambda)(e^{i\pi/4} - \lambda) = 0.$$

Hence the eigenvalues are

$$\lambda_1 = 1, \quad \lambda_2 = e^{i\pi/4}.$$

Next, we find the corresponding eigenvectors. For $\lambda_1 = 1$, let

$$|\phi_1\rangle = \begin{pmatrix} a \\ b \end{pmatrix}.$$

Then

$$T|\phi_1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \\ e^{i\pi/4}b \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}.$$

Equating the lower components gives $e^{i\pi/4}b = b$. Since $e^{i\pi/4} \neq 1$, we must have $b = 0$. Using normalization $|a|^2 = 1$, we get $a = 1$. So

$$|\phi_1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

For $\lambda_2 = e^{i\pi/4}$, again let

$$|\phi_2\rangle = \begin{pmatrix} a \\ b \end{pmatrix}.$$

Then

$$T|\phi_2\rangle = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \\ e^{i\pi/4}b \end{pmatrix},$$

and we want this to equal

$$e^{i\pi/4} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} e^{i\pi/4}a \\ e^{i\pi/4}b \end{pmatrix}.$$

We see $a = 0$ is required, and with $|b|^2 = 1$, we get $b = 1$. So

$$|\phi_2\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

It is straightforward to verify these solutions satisfy the eigenvalue equations. An important fact is that for a Hermitian operator, eigenvalues are real, and for a unitary operator, eigenvalues lie on the complex unit circle (they have modulus 1).

3.3 Spectral Decomposition

An operator \hat{A} is said to be normal if and only if it has a diagonal matrix representation with respect to some orthonormal basis of the vector space. This result is known as the spectral decomposition theorem. Suppose that an operator \hat{A} satisfies the spectral decomposition theorem for some basis $\{|u_i\rangle\}$. Then we can write

$$\hat{A} = \sum_{i=1}^n a_i |u_i\rangle\langle u_i|, \quad (3.38)$$

where a_i are the eigenvalues of the operator. In the computational basis, the Z operator is diagonal. We have already seen the Z operator written in the form of (3.38) when we considered $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$.

Example 3.7: Using the spectral decomposition theorem, write down the representation (3.38) for the operator

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

Solution: The eigenvectors of this matrix are (you can verify):

$$|u_1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \quad |u_2\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}, \quad |u_3\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}.$$

The corresponding eigenvalues are $a_1 = -1$, $a_2 = 1$, and $a_3 = 0$. Since this matrix is Hermitian, its eigenvectors form an orthonormal basis. We can therefore write

$$A = -|u_1\rangle\langle u_1| + |u_2\rangle\langle u_2| + |u_3\rangle\langle u_3|.$$

3.4 The Trace of an Operator

If an operator is in a matrix representation, the trace of the operator is the sum of the diagonal elements. For example, for

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad \text{Tr}(A) = a + d.$$

If an operator is written as an outer product, we take the trace by summing over inner products with basis vectors. If we label a basis $\{|u_i\rangle\}$, then

$$\text{Tr}(\hat{A}) = \sum_{i=1}^n \langle u_i | \hat{A} | u_i \rangle.$$

Example 3.8: An operator expressed in the $\{|0\rangle, |1\rangle\}$ basis is given by

$$A = 2i |0\rangle\langle 0| + 3 |0\rangle\langle 1| - 2 |1\rangle\langle 0| + 4 |1\rangle\langle 1|.$$

Find the trace.

Solution: We compute

$$\text{Tr}(A) = \langle 0|A|0\rangle + \langle 1|A|1\rangle.$$

Focusing on $\langle 0|A|0\rangle$:

$$\langle 0|(2i|0\rangle\langle 0| + 3|0\rangle\langle 1| - 2|1\rangle\langle 0| + 4|1\rangle\langle 1|)|0\rangle = 2i(\langle 0|0\rangle\langle 0|0\rangle) = 2i.$$

Similarly,

$$\langle 1|A|1\rangle = 4(\langle 1|1\rangle\langle 1|1\rangle) = 4.$$

Hence,

$$\text{Tr}(A) = 2i + 4.$$

Example 3.9: Find the trace of the Z operator.

Solution: Using the matrix representation of Z in the computational basis:

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

we sum the diagonal elements:

$$\text{Tr}(Z) = 1 + (-1) = 0.$$

Important Properties of the Trace:

- The trace is cyclic: $\text{Tr}(ABC) = \text{Tr}(CAB) = \text{Tr}(BCA)$.
- $\text{Tr}(|\phi\rangle\langle\psi|) = \langle\psi|\phi\rangle$.
- More generally, $\text{Tr}(A|\psi\rangle\langle\phi|) = \langle\phi|A|\psi\rangle$.
- The trace is basis-independent.
- The trace of an operator is equal to the sum of its eigenvalues.

Example 3.10: Show that the trace of a matrix is equal to the sum of its eigenvalues for

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 3 & 4 \\ 1 & 0 & 2 \end{pmatrix}.$$

Solution:

$$\text{Tr}(X) = 0 + 0 = 0, \quad \text{Tr}(T) = 1 + e^{i\pi/4}, \quad \text{Tr}(B) = 1 + 3 + 2 = 6.$$

We found that

$$\begin{aligned} \text{eigenvalues}(X) &= \{1, -1\}, & \text{sum} &= 0, \\ \text{eigenvalues}(T) &= \{1, e^{i\pi/4}\}, & \text{sum} &= 1 + e^{i\pi/4}, \\ \text{eigenvalues}(B) &= \{0, 3, 3\}, & \text{sum} &= 6. \end{aligned}$$

Hence each trace matches the sum of the corresponding eigenvalues.

Example 3.11: Prove that

$$\text{Tr}(A|\phi\rangle\langle\psi|) = \langle\psi|A|\phi\rangle.$$

Solution: Using an arbitrary basis $\{|u_i\rangle\}$,

$$\text{Tr}(A|\phi\rangle\langle\psi|) = \sum_i \langle u_i|A|\phi\rangle\langle\psi|u_i\rangle = \langle\psi|\left(\sum_i |u_i\rangle\langle u_i|\right)A|\phi\rangle = \langle\psi|A|\phi\rangle.$$

We used the completeness relation $\sum_i |u_i\rangle\langle u_i| = I$ and the fact that inner products are just scalars that can be rearranged.

3.5 The Expectation Value of an Operator

The expectation value of an operator is the mean or average value of that operator with respect to a given quantum state. Symbolically,

$$\langle A \rangle = \langle\psi|A|\psi\rangle. \quad (3.39)$$

Example 3.12: A quantum system is in the state

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

What is the expectation value of X in this state?

4. LECTURE 7: QUANTUM ALGORITHMS

February 17, 2025

4.1 Introduction to Quantum Algorithms

Definition 4.1.1 (Quantum Algorithm). *A quantum algorithm is a set of instructions designed to be executed on a quantum computer, leveraging quantum mechanics to perform calculations more efficiently than classical computers.*

Key advantages of quantum computing arise from:

- **Superposition:** A quantum system can exist in multiple states simultaneously
- **Quantum Parallelism:** Evaluation of functions at multiple inputs simultaneously
- **Quantum Interference:** Manipulation of quantum states to extract useful information

4.2 Mathematical Foundations

Given a function $f(x)$, a quantum algorithm can evaluate $f(x)$ at multiple values simultaneously:

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

where U_f represents a quantum operation acting on an input state $|x\rangle$.

4.3 Hadamard Gates and Quantum Superposition

Definition 4.3.1 (Hadamard Gate). *The Hadamard gate H creates superposition states:*

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

Example 4.3.2 (Hadamard on Arbitrary Qubit). *For an arbitrary qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, the Hadamard transformation is:*

$$H|\psi\rangle = \frac{\alpha + \beta}{\sqrt{2}}|0\rangle + \frac{\alpha - \beta}{\sqrt{2}}|1\rangle$$

4.4 Parallel Hadamard Operations

Definition 4.4.1 (Hadamard Transform). *The Hadamard Transform $H^{\otimes n}$ applies Hadamard gates to multiple qubits in parallel:*

$$H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$$

Example 4.4.2 (Two-Qubit Hadamard). *For two qubits initialized in $|00\rangle$:*

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

4.5 Phase Gates

Definition 4.5.1 (Phase Gate). *The discrete phase gate R_k applies a phase shift:*

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}$$

4.6 Matrix Representations

Common quantum gates in matrix form:

- **Hadamard Gate:**

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

- **Phase Gate:**

$$P(\theta) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}$$

4.7 Deutsch's Algorithm

Definition 4.7.1 (Deutsch's Algorithm). *An algorithm that determines whether a function $f : \{0, 1\} \rightarrow \{0, 1\}$ is constant or balanced using a single function evaluation.*

Theorem 4.7.2 (Deutsch's Algorithm Steps). 1. *Prepare input state:*

$$|\psi\rangle = H|0\rangle H|1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

2. *Apply function as quantum operation:*

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

3. *Measure to determine if $f(x)$ is constant or balanced*

Key Takeaways:

- Quantum algorithms leverage superposition and parallelism
- Hadamard gates create quantum superposition
- Phase gates introduce complex phase factors
- Deutsch's Algorithm demonstrates quantum speedup

5. LECTURE 8: QUANTUM INTERFERENCE AND DEUTSCH'S ALGORITHM

February 24, 2025

5.1 Quantum Interference

The Hadamard gate transformation of $|\psi\rangle = |0\rangle$ demonstrates quantum interference through:

- **Positive interference:** Probability amplitudes add constructively for basis state $|0\rangle$, increasing measurement probability to unity
- **Negative interference:** Terms $|1\rangle$ and $-|1\rangle$ cancel, reducing measurement probability to zero

Quantum interference plays a crucial role in quantum algorithms by allowing us to gain information about a function $f(x)$ that depends on evaluating the function at many values of x simultaneously. This enables deduction of certain global properties of the function.

5.2 Quantum Parallelism and Function Evaluation

Definition 5.2.1 (Function Types). *For a single-bit input function $f : \{0, 1\} \rightarrow \{0, 1\}$, we have:*

- *Identity function:*

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

- *Constant functions:* $f(x) = 0$ or $f(x) = 1$

- *Bit flip function:*

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

The identity and bit flip functions are called **balanced** because outputs are opposite for half the inputs.

5.3 Deutsch's Algorithm Implementation

Definition 5.3.1 (Unitary Operation U_f). *The operation U_f acts on two qubits:*

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

where $x, y \in \{0, 1\}$.

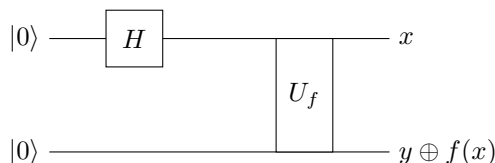


Figure 1: Circuit diagram for $U_f|x, y\rangle = |x, y \oplus f(x)\rangle$ where the first qubit is in superposition and second qubit is $|0\rangle$

The algorithm's steps:

1. Apply Hadamard gates to input state $|0\rangle|1\rangle$ to produce product state of superpositions
2. Apply U_f to that product state
3. Apply Hadamard gate to first qubit only

Let's examine how U_f acts on the computational basis states:

$$U_f|00\rangle = |0, 0 \oplus f(0)\rangle = (1 - f(0))|00\rangle + f(0)|01\rangle$$

This result accounts for both possibilities where $0 \oplus f(0) = 0$ and $0 \oplus f(0) = 1$. To understand this:

- If $f(0) = 0$, then $0 \oplus f(0) = 0 \oplus 0 = 0$ and:

$$|0, 0 \oplus f(0)\rangle = (1 - f(0))|00\rangle + f(0)|01\rangle = |00\rangle + (0)|01\rangle = |00\rangle$$

- If $f(0) = 1$, then $0 \oplus f(0) = 0 \oplus 1 = 1$ and:

$$|0, 0 \oplus f(0)\rangle = (1 - f(0))|00\rangle + f(0)|01\rangle = (0)|00\rangle + (1)|01\rangle = |01\rangle$$

Similar logic applies to the other basis states:

$$U_f|01\rangle = |0, 1 \oplus f(0)\rangle = f(0)|00\rangle + (1 - f(0))|01\rangle$$

$$U_f|10\rangle = |1, 0 \oplus f(1)\rangle = (1 - f(1))|10\rangle + f(1)|11\rangle$$

$$U_f|11\rangle = |1, 1 \oplus f(1)\rangle = f(1)|10\rangle + (1 - f(1))|11\rangle$$

Theorem 5.3.2 (Deutsch's Algorithm Output). *The final output state is:*

$$|\psi_{out}\rangle = \begin{cases} (1 - 2f(0))|0\rangle \oplus \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) & \text{if } f(0) = f(1) \text{ (constant)} \\ \pm|1\rangle \oplus \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) & \text{if } f(0) \neq f(1) \text{ (balanced)} \end{cases}$$

5.4 Deutsch-Jozsa Algorithm

Definition 5.4.1 (Deutsch-Jozsa Algorithm). *A generalization of Deutsch's algorithm for functions with multiple input values. For $f(x)$ with n input values:*

- **Constant:** *Output is same for all input values x*
- **Balanced:** *$f(x) = 0$ for half inputs and $f(x) = 1$ for other half*

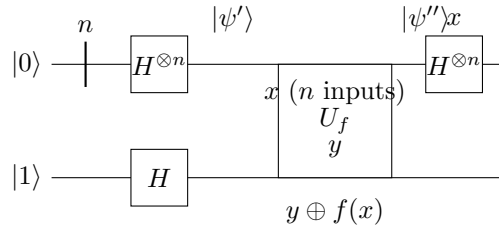


Figure 2: Circuit diagram for the Deutsch-Jozsa algorithm showing the n -qubit input register and auxiliary qubit

Theorem 5.4.2 (Measurement Results). *After measuring the n input qubits in the final state:*

- If all qubits are 0: $f(x)$ is constant
- If at least one qubit is 1: $f(x)$ is balanced

Example 5.4.3 (Constant Function). For $f(x) = 1$ with two inputs:

1. Initial state: $|\psi_{in}\rangle = |0\rangle|0\rangle|1\rangle$

2. After Hadamard gates:

$$|\psi_t\rangle = \frac{1}{2\sqrt{2}}(|000\rangle - |001\rangle + |010\rangle - |011\rangle + |100\rangle - |101\rangle + |110\rangle - |111\rangle)$$

3. Final state after all operations:

$$|\psi_{out}\rangle = -|00\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

4. Measurement of first two qubits gives 00, confirming constant function

Example 5.4.4 (Balanced Function). For $f(00) = f(01) = 0$, $f(10) = f(11) = 1$:

1. Initial state: $|\psi_{in}\rangle = |0\rangle|0\rangle|1\rangle$

2. After all operations:

$$|\psi_{out}\rangle = |10\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

3. Measurement of first two qubits gives 10, confirming balanced function