

The Physics of Quantum Computing



Axioms of Quantum Mechanics

Patrick Dreher

CSC591 / ECE592 – Fall 2020

Roadmap For Designing a Gate Based Quantum Computer

- Assemble the mathematical language to describe the quantum mechanical dynamics being harnessed in order to build a quantum computing hardware platform
- The underlying quantum mechanical dynamics of the physical system is initialized by defining qubits in some initial state based on the axioms of quantum mechanics
- These qubits evolve through a sequence of applied unitary operations and projective measurements (called gates) that manipulate the states of the qubits
- Sequences of gates are assembled into a circuit that represents a set of instructions that model the problem being implemented on a quantum computer
- Circuit instructions are compiled and delivered to the qubits in the quantum computer as a set of microwave control pulses
- These microwave pulses implement the desired unitary quantum mechanical state-transformations and/or measurements by steering or evolving these qubits from an initialized state through final measurement
- The final measurement extracts classical information in the form of bit strings, which encode the outcome of projective measurements of the qubits in a particular measurement basis according to the axioms of quantum mechanics and the mathematics of linear algebra

Outline

- Motivation to seek a different paradigm beyond digital computation
- Challenges Applying the Physics of Quantum Mechanics to Construct a Quantum Computer
- Axioms of quantum mechanics
- How Does Quantum Mechanics Impact the Design of Algorithms and Programs for Quantum Computing?

Brief Overview Conventional Computers Properties And Characteristics

Basic Characteristic of a Classical Computer

- Binary data representation for floating point and integer quantities (“0”s and “1”s)
- Hardware is designed and constructed on this base 2 formalism
- Binary representations reflect the lowest level structure for system and application software

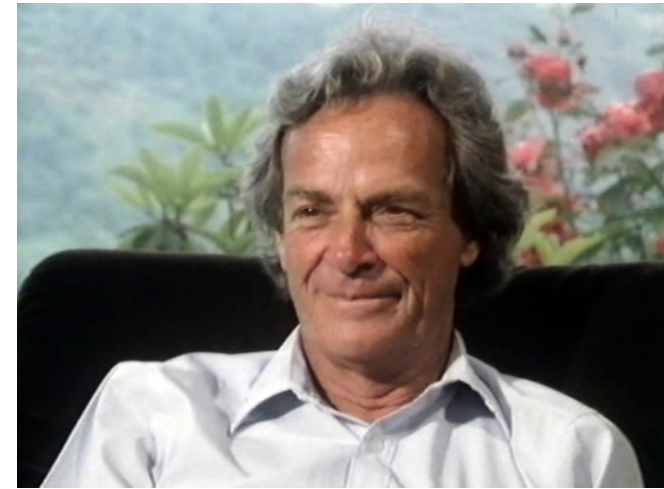


Constraint of the Digital Computing Approach

Richard Feynman (1981):

“...trying to find a computer simulation of physics, seems to me to be an excellent program to follow out...and I'm not happy with all the analyses that goes with just the classical theory, because

- *nature isn't classical, dammit*
- if you want to make a simulation of nature, you'd better *make it quantum mechanical*, and by golly it's a wonderful problem because it doesn't look so easy.”



Richard Feynman's 1981 Paper

International Journal of Theoretical Physics, Vol. 21, Nos. 6/7, 1982

Simulating Physics with Computers

Richard P. Feynman

Department of Physics, California Institute of Technology, Pasadena, California 91107

Received May 7, 1981

1. INTRODUCTION

On the program it says this is a keynote speech—and I don't know what a keynote speech is. I do not intend in any way to suggest what should be in this meeting as a keynote of the subjects or anything like that. I have my own things to say and to talk about and there's no implication that anybody needs to talk about the same thing or anything like it. So what I want to talk about is what Mike Denton suggested that nobody would talk about. I want to talk about the problem of simulating physics with

The Quantum Computer A New Computational Paradigm

David Deutsch (1985):

“Computing machines resembling the universal quantum computer could, in principle, be built and would have many remarkable properties not reproducible by any Turing machine”



Challenges Applying the Physics of Quantum Mechanics to Construct a Quantum Computer

Challenges Applying the Physics of Quantum Mechanics to Construct a Quantum Computer

If one wants to use quantum mechanics to design and build a computer, one must appreciate and understand the implications as to how a such computer will view and process the problem

Patrick Dreher

Challenges Conceptualizing How a Quantum Computer will Process a Problem

- Quantum mechanics is not a description of the classical world
- It describes the physics of the atomic and subatomic world
- Difficult conceptually
 - Our human ideas and approaches to problems are influenced by our experiences and expected behaviors
 - All known human experiences and intuition are rooted in the macroscopic world, not in the atomic and subatomic microscopic world described by quantum mechanics
 - Many quantum mechanical behaviors have no classical analog

Hurdle That Must Be Surmounted To Achieve Quantum Advantage And Ultimately Quantum Superiority

Even if an algorithm or program can be developed based on the axioms of quantum mechanics

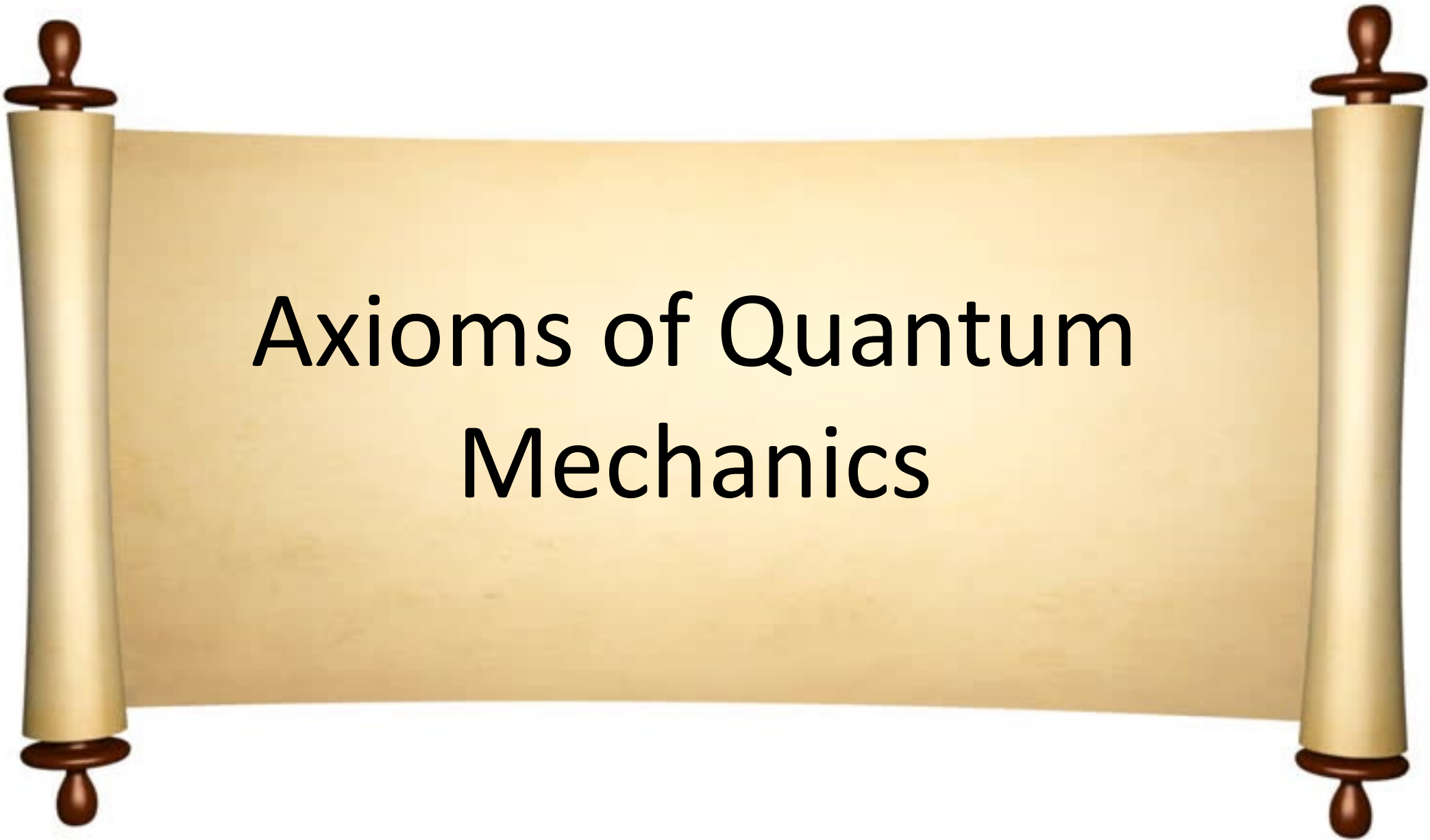
it must also

demonstrate that the quantum computing algorithm is computationally superior to the classical equivalent

Ultimate Goal of Quantum Computing

Quantum Supremacy

Quantum supremacy is the goal of demonstrating that a programmable quantum device can solve a problem that no classical computer can solve in any feasible amount of time



Axioms of Quantum
Mechanics

Axioms/Concepts That Underpin Quantum Mechanics

Axiom 1. States

- A state is a complete description of a physical system.

Axiom 2. Observables

- An observable is a property of a physical system that in principle can be measured.

Axiom 3. Measurement

- A measurement is a process in which information about the state of a physical system is acquired by an observer.

Axiom 4. Dynamics

- Dynamics describes how a state evolves over time.

Axiom 5. Composite Systems

- Given two non-interacting systems A and B described by Hilbert spaces \mathbb{H}_A and \mathbb{H}_B the composite system is expressed as the tensor product $\mathbb{H}_A \otimes \mathbb{H}_B$

Notation

Dirac “braket” or “bra” and “ket”

- Many texts use Dirac “ket” notation $|a\rangle$ to represent a column vector

$$|a\rangle = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$$

and a Dirac “bra” notation to denote the Hermitian conjugate of \vec{a}

$$\langle a| = (a_1^* \quad a_2^* \quad \dots \quad a_n^*)$$

Some basic properties of linear algebra useful in describing quantum mechanics

The transpose \mathbf{a}^T of a column vector \mathbf{a} is a row vector

The adjoint \mathbf{a}^\dagger is the complex conjugate transpose of a column vector \mathbf{a}

Unitary matrix \mathbf{U} is a complex square matrix whose adjoint equals its inverse and the product of \mathbf{U} adjoint and the matrix \mathbf{U} is the identity matrix

$$\mathbf{U}^\dagger \mathbf{U} = \mathbf{U}^{-1} \mathbf{U} = \mathbf{I}$$

Axiom 1: States

Properties of States

- Quantum mechanical states are represented by complex numbers in a vector space with the following properties
 - a. Positivity $\langle \Psi | \Psi \rangle \geq 0$ for $|\Psi\rangle \neq 0$
 - b. Linearity $\langle \Phi | (a|\Psi_1\rangle + b|\Psi_2\rangle) \rangle = a \langle \Phi | \Psi_1 \rangle + b \langle \Phi | \Psi_2 \rangle$
 - c. Skew symmetry $\langle \Phi | \Psi \rangle = \langle \Psi | \Phi \rangle^*$
 - d. Completeness $\|\Psi\| = \langle \Psi | \Psi \rangle^{1/2}$
- The totality of the mathematical representation of the state of a system can be quantum mechanically represented by a **ket** $|\Psi\rangle$ in the space of states

Axiom 1: States

Implications for Quantum Computing

- A quantum mechanical state can be described in a mathematical representation
- Every isolated quantum mechanical system has an associated complex vector space with an inner product that is the state space of the system
- A unit (normalized) vector in the system's state space is a state vector that is a complete description of the physical system
- The superposition of two states in the Hilbert Space A is again a state of the system. (see also Axiom 5 – Composite Systems)

Given that the Hilbert space of system A is H_A and the Hilbert space of system B is H_B , then the Hilbert space of the composite systems AB is the “tensor product” $H_A \otimes H_B$

Axiom 2: Observables

Implications for Quantum Computing

Every observable attribute of a physical system is described by an operator that acts on the kets that describe the system.

Axiom 2: Observables

Implications for Quantum Computing

- In quantum mechanics an observable corresponds to a self-adjoint operator
- A self-adjoint operator is a linear map taking vectors to vectors
- A self-adjoint operator in a Hilbert space \mathbb{H} has a spectral representation such that its eigenstates form a complete orthonormal basis in \mathbb{H} .
- Acting with a self-adjoint operator on a given state in general changes the set of basis vectors in one state to another orthonormal state of basis vectors.
- There are special states that are not changed (except for being multiplied by a constant) by the action of an operator A

$$A|\Psi_a\rangle = a|\Psi_a\rangle$$

- The numbers “a” are the eigenvalues of the eigenstates

Axiom 3: Measurements

Implications for Quantum Computing

- When a measurement of an observable \hat{A} is made on a generic state $|\Psi\rangle$, the probability of obtaining an eigenvalue a_n is given by the square of the inner product of $|\Psi\rangle$ with the eigenstate $|a_n\rangle$, $|\langle a_n | \Psi \rangle|^2$
- The complex number $\langle a_n | \Psi \rangle$ is a “probability amplitude”
 Note: This quantity is not directly measurable

$$|\langle \Psi | \Psi \rangle|^2 = \sum_m \sum_n c_m^* c_n \langle a_m | a_n \rangle$$

Axiom 3: Measurements

Implications for Quantum Computing

- The premise for describing the discreteness of measured quantities in a specifically constructed quantum mechanical system are the eigenvalues of the Schrodinger eq.
- The eigenvalues of quantum operators describing experimental measurement in the real world (eigenvalues) are described by real numbers (probabilities)
- States can be described in terms of a wave packet of complex valued probability amplitudes
- The consequences of a measurement of the wave packet of probability amplitudes results in the wave packet collapse to an eigenvalue with a certain probability
- Hermitian operators are orthogonal $\rightarrow \langle a_j | a_k \rangle = \delta_{jk}$
- The eigenstates span the vector space and form a basis
 - An arbitrary state can be expanded as a sum of the eigenstates of a Hermitian operator (with complex coefficients)
 - A basis description provides mathematical procedure for transformations/evolution of a state
 - The Hermitian property assures that the set of states are “complete”
(implies that energy is transformed between states but cannot be created or destroyed)

Axiom 3: Measurements

- An observable is one of the set of eigenvalues “ a_n ” of the corresponding operator “ A ”

$$A = \sum_n a_n E_n$$

- “ E_n ” is the corresponding orthogonal projection onto the space of eigenvectors with eigenvalue “ a_n ”
- The operator \hat{A} corresponding to an observable that yields a measured value of one of the eigenvalues “ a_n ” will correspond to the state of the system as the normalized eigenstate $|a_n\rangle$ measured with a priori probability

$$\text{prob}(a_n) = ||E_n|\Psi\rangle||^2 = \langle \Psi|E_n|\Psi\rangle$$

- The normalized state for a_n after the measurement is $\frac{E_n|\Psi\rangle}{||E_n|\Psi\rangle||}$

Axiom 3: Measurements

Implications for Quantum Computing

- A single measurement of a quantity will not provide an averaged or expected value $\langle a \rangle$
- A measurement of a quantum mechanical system must be repeated many times to get an expectation value of the quantity
- A system described by a wave packet $|\Psi\rangle$ and measured by an operator \hat{A} repeated times will yield a variety of results given by the probabilities $|\langle a_n | \Psi \rangle|^2$
- If many identically prepared systems are measured each described by the state $|a\rangle$ then the expectation value of the outcomes is

$$\langle a \rangle \equiv \sum_n a_n \text{Prob}(a_n) = \langle a | \hat{A} | a \rangle$$

Axiom 3: Measurements

Implications for Quantum Computing

- To obtain a quantity that can be compared to experimental measurements requires summing all of the probability amplitudes and then squaring the aggregate to get an expectation value
- The complex coefficients in the probability amplitudes are responsible for many of the phenomena and behavioral properties that impact final measurements of quantum systems
- The probability of obtaining a measured result must be 1 when summed over all possible probability amplitudes and squared.
- These properties are exploited when developing quantum computing algorithms and quantum circuits that run on quantum computing hardware platforms

Axiom 4: Dynamics

Time Evolution of a Quantum Mechanical System

Dynamics - The evolution of a closed system that evolves over time is expressed mathematically by a unitary operator that connects the system between time t_1 to time t_2 and that only depends on the times t_1 and t_2

- The time evolution dynamics of the state of a closed quantum system is described by the Schrodinger equation

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

Axiom 4: Dynamics

Implications for Quantum Computing

- Any type of “program” that would represent a step by step evolution from an initial state on a quantum computer to some final state must preserve the norm of the state (unitarity)
- The closed system constraint of axiom 4 requiring a unitary evolution of the system over time is a statement of the conservation of probability
- Axiom 4 is particularly relevant when working with actual quantum computing hardware platforms because of their inherent noisy properties (future lecture on the topic of Noisy Intermediate Scale Quantum Devices)

Axiom 5: Composite States

Implications for Quantum Computing

- Given two non-interacting systems A and B described by Hilbert spaces H_A and H_B the composite system is expressed as the tensor product $H_A \otimes H_B$

- The state of the composite system is

$$|\Psi_A\rangle \otimes |\Psi_B\rangle$$

- States of H_A and H_B that can be mathematically represented in this manner are called separable states or product states

$$|\Psi\rangle_{AB} = \sum_{i,j} c_{ij} |i\rangle_A \otimes |j\rangle_B$$

Axiom 5: Composite States

Implications for Quantum Computing

Quantum Entanglement

- Quantum entanglement is a phenomenon in quantum mechanics that describes quantum mechanical states where
 - Pairs (groups) of particles are generated and/or interact such that
 - Their quantum mechanical individual states cannot be mathematically described independently of the pair (group) state

Axiom 5: Composite States

Implications for Quantum Computing

- Define a basis vectors $|i\rangle_A$ for \mathbb{H}_A and $|j\rangle_B$ for \mathbb{H}_B
- The composite (product state) can be written in the set of basis vectors as

$$|\Psi\rangle_{AB} = \sum_{i,j} c_{ij} |i\rangle_A \otimes |j\rangle_B$$

$$|\Psi\rangle_A = \sum_i c_i^A |i\rangle_A$$

$$|\Psi\rangle_B = \sum_j c_j^B |j\rangle_B$$

- If there exist vectors c_i^A , c_j^B such that $c_{ij} = c_i^A c_j^B$ for all states then the system is considered separable

Axiom 5: Composite States

Implications for Quantum Computing

- Basis States
- If there is at least one pair c_i^A, c_j^B such that $c_{ij} \neq c_i^A c_j^B$ then the state is labelled as being entangled

- Example

$$\frac{1}{\sqrt{2}} (|0\rangle_A \otimes |1\rangle_B - (|1\rangle_A \otimes |0\rangle_B))$$

Possible Outcomes for an Entangled System

$$\frac{1}{\sqrt{2}} (|0\rangle_A \otimes |1\rangle_B - (|1\rangle_A \otimes |0\rangle_B))$$

- 2 observers (Alice and Bob) and a 2 state basis set $\{|0\rangle, |1\rangle\}$
- Alice is an observer in system A and Bob is an observer in system B
- Alice makes an observation in $\{|0\rangle, |1\rangle\}$ basis \rightarrow 2 equal outcomes
 - If Alice measures $|0\rangle$, then system states collapses to $|0\rangle_A |1\rangle_B$ and Bob must measure the $|1\rangle$ state
 - If Alice measures $|1\rangle$ then system states collapses to $|1\rangle_A |0\rangle_B$ and Bob must measure the $|0\rangle$ state

- This will happen regardless of the spatial separation of system A and B
- Completely unexpected behavior compared to everyday human experiences of causality and locality

How Does Quantum Mechanics Impact the Design of Algorithms and Programs for Quantum Computing?

Digital Computer Measurements Versus Quantum Computing Measurements

- Quantum computers output probabilities (expectation values)
 - Quantum computer output probability distribution of results for the calculation given by $|\langle a_n | \psi \rangle|^2$
-
- Quantum computer outputs are statistically independent
 - Cannot re-run the quantum computing program a 2nd time and always expect to get exactly same answer

Classical Gates versus Quantum Gates

- A classical computer gate is a logical construction of operations represented by binary inputs and an associated output.
- A quantum gate is a mathematical manipulation of qubits that adhere to the postulates of quantum mechanics and the mathematics of linear algebra

Digital Computer Measurements Versus Quantum Computing Measurements

- Quantum mechanics probability amplitude is a complex valued unobservable described by a state vector (wavefunction)
- The probability amplitude has an indeterminate specific value until a measurement is performed
- A measurement collapses the wave packet of all possible probability amplitudes down to a single measurement while preserving the normalization of the state
- Once the system is measured all information prior to that measurement is permanently lost

Digital Computer Measurements Versus Quantum Computing Measurements

- Any direct disruptions of the of the quantum computing calculation will immediately select/collapse the system to a single value state – all information prior to the measurement is lost
- Digital computing practices disallowed on a quantum computer by the axioms of quantum mechanics
 - Inserting intermediate print statements
 - Checkpoint re-starts

Applying the Axioms of Quantum Mechanics to Describe operational primitives for one and two qubits

Building Quantum Computing Operational Primitives

Fundamental Design Principle

- Quantum circuits are constructed from the combined actions of unitary transformations and single bit rotations
- There are one and two qubit primitives that follow from applying the axioms of quantum mechanics to construct one and two qubit primitives for building quantum circuits
- Quantum mechanics restricts the types of operational primitives that can be constructed

Operational Primitives That Form The Building Blocks For Gate Operations

- A quantum gate must incorporate
 - Linear superposition of pure states that includes a phase
 - Reversibility - All closed quantum state transformations must be reversible
 - Reversible transformations are described through matrix rotations

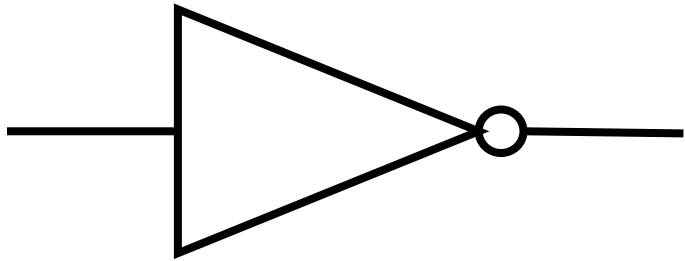
Quantum Computing Gate Operations Under the Constraints of Quantum Mechanics

- A quantum gate must incorporate
 - Unitarity - states evolve over time and are expressed mathematically by a unitary operator (transformation) for a closed quantum mechanics system
 - Unitary operator U is expressed as a complex square matrix whose adjoint equals its inverse and the product of U adjoint and the matrix U is the identity operation

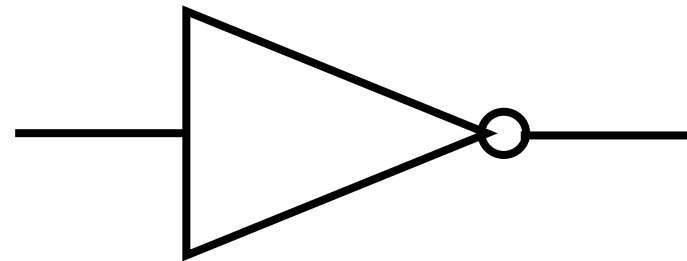
$$U^\dagger U = U^{-1} U = I$$

- Completeness - unitary matrices preserve the length of vectors

Example of a Reversible One Qubit Gate Operation



INPUT	OUTPUT
0	1
1	0



INPUT	OUTPUT
1	0
0	1

- Single bit NOT gate output can be reversed by applying another NOT gate

So Far So Good for One Qubit

but

One Qubit Has Only a Limited Number of Operations

What Does Quantum Mechanics Prescribe for 2 Qubits?

2 Qubit Gates

Two Qubit Representation of States

- Two states are represented by a pair of orthonormal 2 vectors

$$|a\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |b\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

- The four states are four orthogonal vectors in four dimensions formed by the tensor products

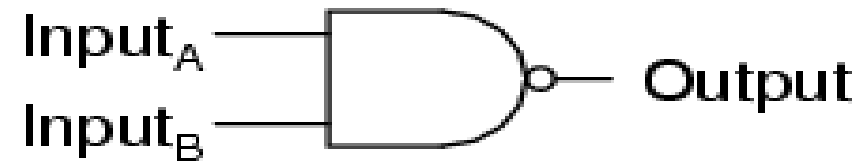
$$|a\rangle \otimes |a\rangle, |a\rangle \otimes |b\rangle, |b\rangle \otimes |a\rangle, |b\rangle \otimes |b\rangle$$

- These states can also be represented by

$$|aa\rangle, |ab\rangle, |ba\rangle, |bb\rangle$$

Consequences for Quantum Computing

NAND gate

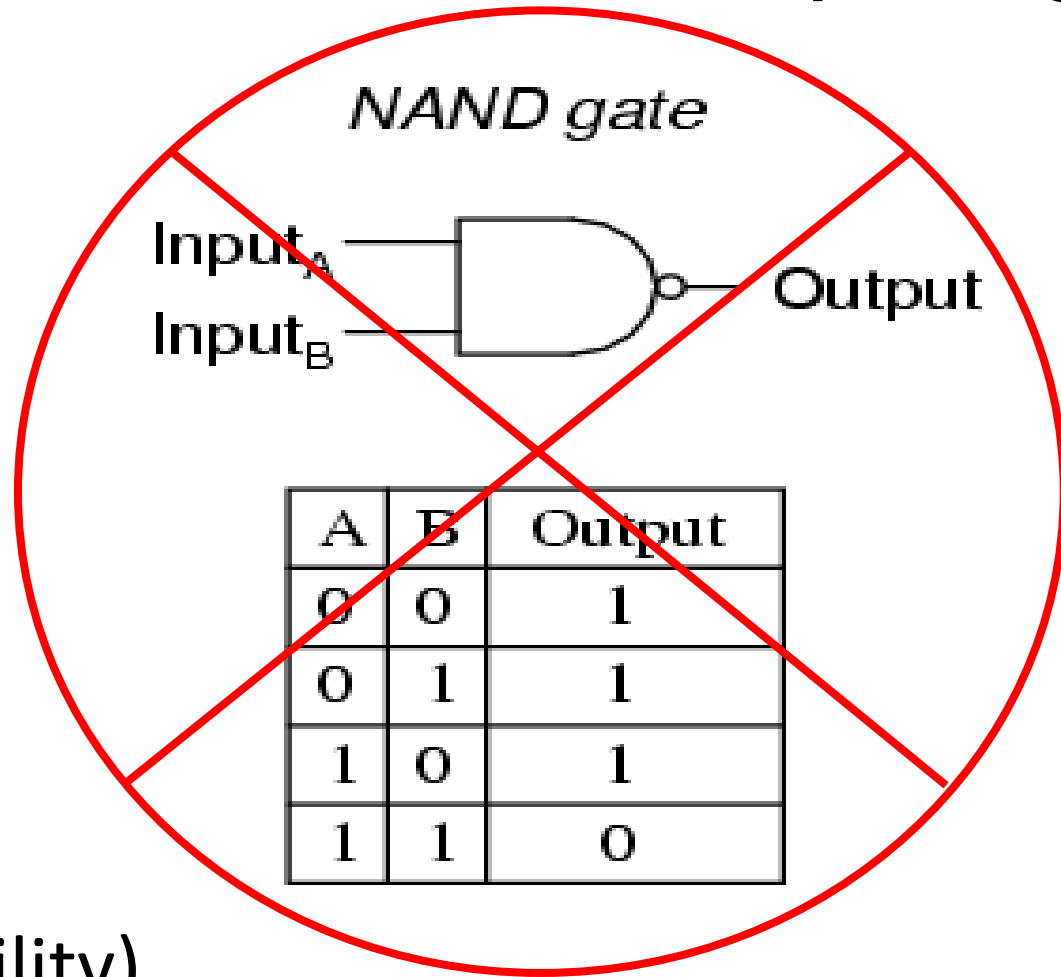


- NAND gate is a fundamental building block for digital computers

A	B	Output
0	0	1
0	1	1
1	0	1
1	1	0

Consequences for Quantum Computing

- NAND gate is not reversible
- Need to modify a 2 qubit input system so that the output can display bi-directional properties (physics property of reversibility)



Design Reversible 2 Qubit Gate

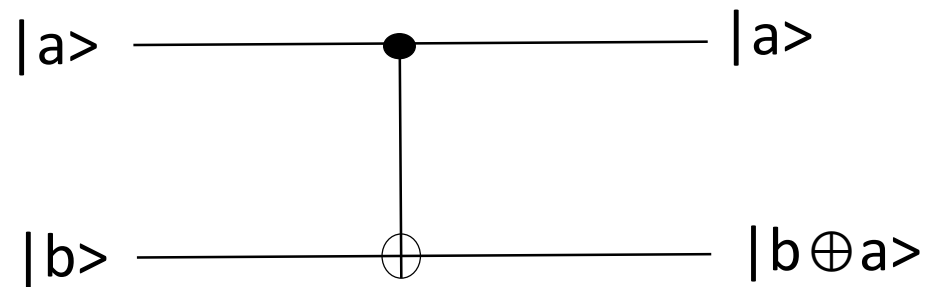
Controlled-NOT Gate

Matrix representation rules for the CNOT gate

$$|a\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |b\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$\begin{aligned} |aa\rangle &\rightarrow |aa\rangle \\ |ab\rangle &\rightarrow |ab\rangle \end{aligned}$$

$$\begin{aligned} |ba\rangle &\rightarrow |bb\rangle \\ |bb\rangle &\rightarrow |ba\rangle \end{aligned}$$



$$U_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Identity Matrix \rightarrow Reversibility

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

$$U_{CNOT}^\dagger U_{CNOT} = I$$

Additional Useful Mathematical Operation

Exclusive Disjunction

- Exclusive disjunction of $a \oplus b = (a \vee b) \wedge \neg(a \wedge b)$
- Truth table for this operation is

Input		Output
a	b	
0	0	0
0	1	1
1	0	1
1	1	0

Building a Reversible 2 Qubit Gate

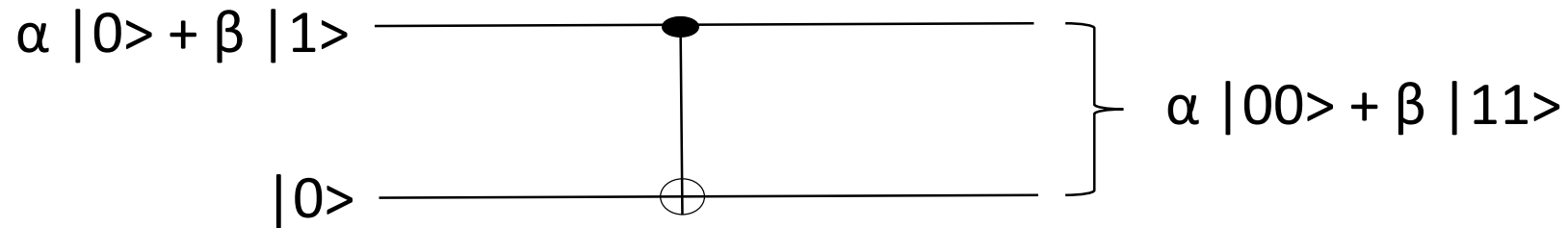
- A two qubit quantum logic gate has a control qubit and a target qubit
- The gate is designed such that if
 - the control bit is set to 0 the target bit is unchanged
 - The control bit is set to 1 the target qubit is flipped

Input	Output
$ 00\rangle$	$ 00\rangle$
$ 01\rangle$	$ 01\rangle$
$ 10\rangle$	$ 11\rangle$
$ 11\rangle$	$ 10\rangle$

- Can be expressed as $|a, b\rangle \longrightarrow |a, b \oplus a\rangle$
- The CNOT gate is generally used in quantum computing to generate entangled states

Quantum Mechanics Surprises Imposed on 2 Qubit Gates

- Consider the CNOT gate below with the given inputs



- The output will be $\alpha |00\rangle + \beta |11\rangle$

Can we Duplicate Quantum States For Programming Quantum Computers?

- Assume there exists two quantum systems P and Q both in a common Hilbert space containing those systems

- Goal: Take a state $|\alpha\rangle_P$ in system P and copy it to system Q

Start with the P state α and combine it with some unknown state Q (call it “ β ”)

$|\alpha\rangle_P \otimes |\beta\rangle_Q$ (assuming no prior information about $|\beta\rangle_Q$) in such a way that in the end a composite state $|\alpha\rangle_P \otimes |\alpha\rangle_Q$ will be constructed

Can we Duplicate Quantum States For Programming Quantum Computers?

- In digital computers stored information can be accurately replicated
- From the study of the axioms of quantum mechanics, it is known that a measurement of the system will result in a collapse of the quantum system to an eigenstate of the measurement operator with all other information related to the original state of the system completely lost
- Is there a way to copy a pure state accurately in a quantum computer

Proof – No Cloning Theorem

- Assume there exists a quantum computing cloning machine with an operation U that can duplicate an arbitrary pure state of the system

$$U(|\varphi\rangle \otimes |R\rangle \otimes |M\rangle) = |\varphi\rangle \otimes |\varphi\rangle \otimes |M\varphi\rangle$$

where

- $|\varphi\rangle$ denote an arbitrary pure state
- $|R\rangle$ an initial blank state of the cloning machine
- $|M\rangle$ as the initial state of the auxiliary state
- $|M\varphi\rangle$ as the ancillary state after the operation that depends on $|\varphi\rangle$

Proof – No Cloning Theorem

- Use the property of linearity in quantum mechanics to write an arbitrary state

$$|\varphi\rangle |R\rangle |M\rangle$$

where

$|\varphi\rangle$ is any arbitrary state

$|R\rangle$ is a blank state

$|M\rangle$ is the state of the auxiliary system (ancilla)

Proof – No Cloning Theorem

- Consider two cases for $|\varphi\rangle$ (a state $|0\rangle$ and $|1\rangle$)

$$|0\rangle|R\rangle|M\rangle \rightarrow |0\rangle|0\rangle|M(0)\rangle$$

$$|1\rangle|R\rangle|M\rangle \rightarrow |1\rangle|1\rangle|M(1)\rangle$$

- The general state $|\varphi\rangle = |(a|0\rangle+b|1\rangle)\rangle$ is a pure state and the arbitrary replication can be written

$$|(a|0\rangle+b|1\rangle)\rangle|(a|0\rangle+b|1\rangle)\rangle|M\rangle \rightarrow$$

$$a^2|00\rangle+ab|01\rangle+ab|10\rangle+b^2|11\rangle|M(\varphi)\rangle$$

- Obviously the right hand side of both expressions cannot be equal and
- **CONCLUSION:** - The premise is false that an arbitrary cloning mechanism can be constructed in a quantum computer

Next Step – Use Linear Algebra and the Axioms of Quantum Mechanics to Design Gates for Quantum Computing Algorithms and Programs

Questions