

Programming Quantum Computers: A Primer with IBM Q and D-Wave Exercises

by Frank Mueller, Patrick Dreher, Greg Byrd

<http://moss.csc.ncsu.edu/~mueller/qc/qc-tut>

North Carolina State University



Overview

- **Welcome**
- **8:30am-9:30am Intro to Quantum Computing (Patrick Dreher)**
 - Postulates of Quantum Mechanics, Linear Algebra, Qubits
 - Quantum Simulator
- **9:30 am – 10:00 am Break**
- **10:30am-Noon Gate-Level Quantum Computing (Greg Byrd)**
 - Quantum Gates, Circuits, and Algorithms
 - IBM Q Operation
 - IBM Q Programming with Qiskit
- **Noon-1:00pm Lunch**
- **1:00pm-3:00pm Adiabatic Quantum Computing (Frank Mueller)**
 - Basics of Quantum Annealing and QUBOs
 - D-Wave Programming
- **3:00 pm – 3:30 pm Break**
- **3:30pm-5:00pm Programming Exercises with IBM Q and D-Wave**

Introduction to Quantum Computing

**Programming Quantum Computers:
A Primer with IBM Q and D-Wave Exercises**

Patrick Dreher
NC State University
Chief Scientist - NCSU IBM Q Hub

Outline

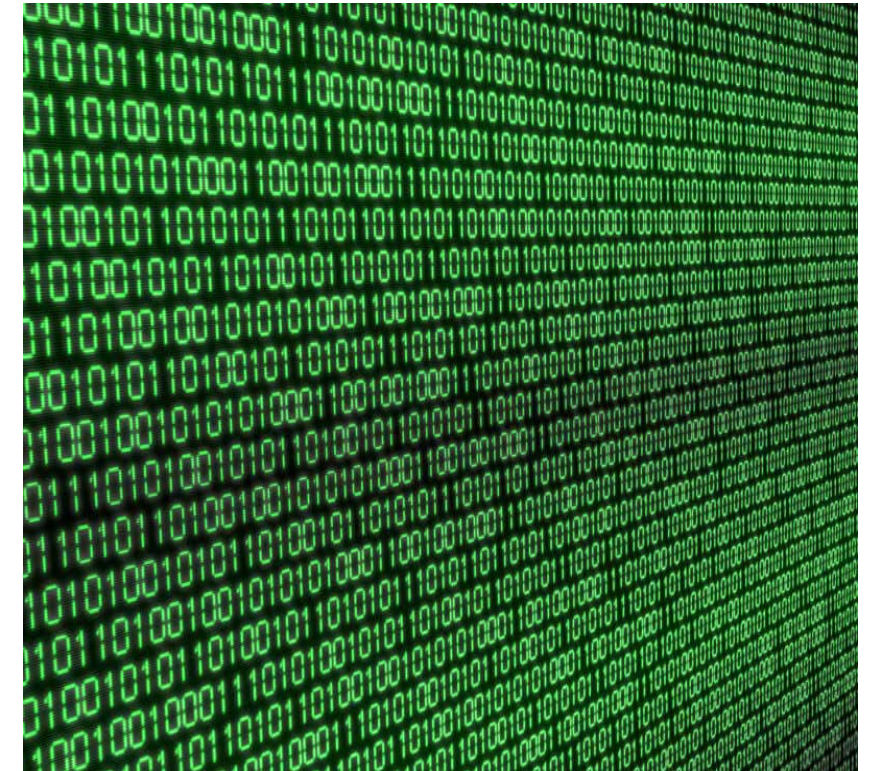
- **Conventional Computer Properties And Characteristics**
- **Quantum Computer - A New Computational Paradigm**
- **Designing a Quantum Computer**
 - Quantum Mechanics
 - Linear Algebra
- **Quantum Computer Properties And Characteristics**
- **Example of a Quantum Computer Design and Implementation**

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



Representing Information on a Computer

- Computer has two states (“off” and “on”)
- Define two states “0” and “1” (“bits”)
- Need to be able to represent the state of a system on a computer in only terms of “0”s and “1”s
- Need to understand how these “0”s and “1”s can be manipulated – how they are transformed when an operation is applied to them

Single Component Representation

- Identify general rules for transforming the state of a single bit in every possible way.
- NOT gate

Initial State		Final State
0	not(0)	1
1	not(1)	0

- RESET gate - Sets the state to 0 regardless of the input

Initial State		Final State
0	reset(0)	0
1	reset(1)	0

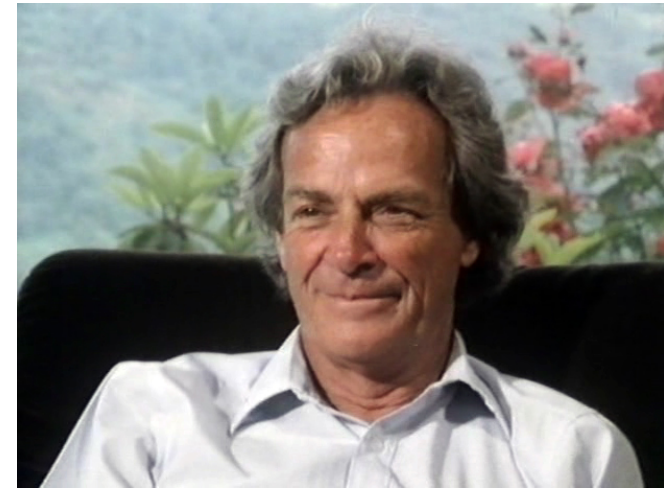
- These two operations define all possible ways to transform the state of a single bit

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 go 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 Dertouzos suggested that nobody would talk about. I want to talk about the problem of simulating physics with

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 ... Complexity theory for [such machines] deserves further investigation.”



Quantum Mechanics and Computing

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

Challenges Conceptualizing How a Quantum Computer Operates

- 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 is rooted in our classical world
- Many behaviors in the quantum world have no classical analog

Quantum Computing Challenges

Even if an algorithm or program can be shown to be based on quantum mechanical systems it must be demonstrated that the quantum mechanical algorithm is computationally superior to the classical equivalent

Quantum Supremacy

Quantum supremacy is the potential ability of quantum computing devices to solve problems that classical computers practically cannot (measured as superpolynomial speedup over the best known classical algorithm)

Foundations of Quantum Computing

- Linear Algebra
- Quantum Mechanics

Properties of Quantum Mechanics

- Quantum theory is a mathematical model of the physical world
- If the properties of quantum mechanics are going to be applied for computations, it is essential to recognize that the physical world at the quantum level exhibits behaviors that have no analogs in people's everyday experiences
- In order to properly design quantum computing devices, algorithms and programs one must
 - understand the properties and behavior of quantum mechanics and
 - the mathematics that describes it

Properties of Linear Algebra Applicable for Quantum Computing

Review Basic Linear Algebra Concepts

Vector Space

A vector space is a collection vectors, which may be added together and multiplied by scalar quantities and still be a part of the collection of vectors

Review Basic Linear Algebra Concepts

Linear Dependence and Linear Independence

A set of vectors is said to be linearly dependent if one of the vectors in the set can be defined as a linear combination of the others

A set of vectors is said to be linearly independent if no vector in the set can be written according to the previous statement

Review Basic Linear Algebra Concepts

Basis Vectors

A set of elements (vectors) in a vector space V is called a basis, or a set of basis vectors, if the vectors are

- linearly independent
- every vector in the vector space is a linear combination of this set

A basis is a linearly independent spanning set

Properties and Definitions of a Vector Space

- Given a vector space V containing vectors A, B, C the following properties apply
 - Commutativity [$A+B=B+A$]
 - Associativity of vector addition [$(A+B)+C=A+(B+C)$]
 - Additive identity [$0+A=A+0=A$] for all A
 - Existence of additive inverse: For any A , there exists a $(-A)$ such that $A+(-A)=0$

Properties and Definitions of a Vector Space

- Given a vector space V containing vectors A, B, C the following properties apply
 - Scalar multiplication identity [$1A=A$]
 - Given scalars r and s
 - Associativity of scalar multiplication [$r(sA)=(rs)A$]
 - Distributivity of scalar sums [$(r+s)A=rA+sA$]
 - Distributivity of vector sums [$r(A+B)=rA+rB$]

Vector Space and Basis Vectors Properties

- Many linear combinations can be constructed to represent the states that lie on the surface of the sphere
- Set of all vectors that can lie on the surface of the sphere can be considered as a vector space
- Use the concept of basis vectors to identify a set of linearly independent vectors in that vector space with the requirement that every vector in the vector space is a linear combination of that set

Review of Linear Algebra

- A set of basis vectors is defined $\{e_i\}_{i=1,\dots,n}$ written in “bra-ket” notation satisfies

$$\langle e_i | e_j \rangle = \delta_{ij}$$

- An arbitrary vector can be written as a linear superposition of basis states

$$a = \sum_i \alpha_i e_i$$

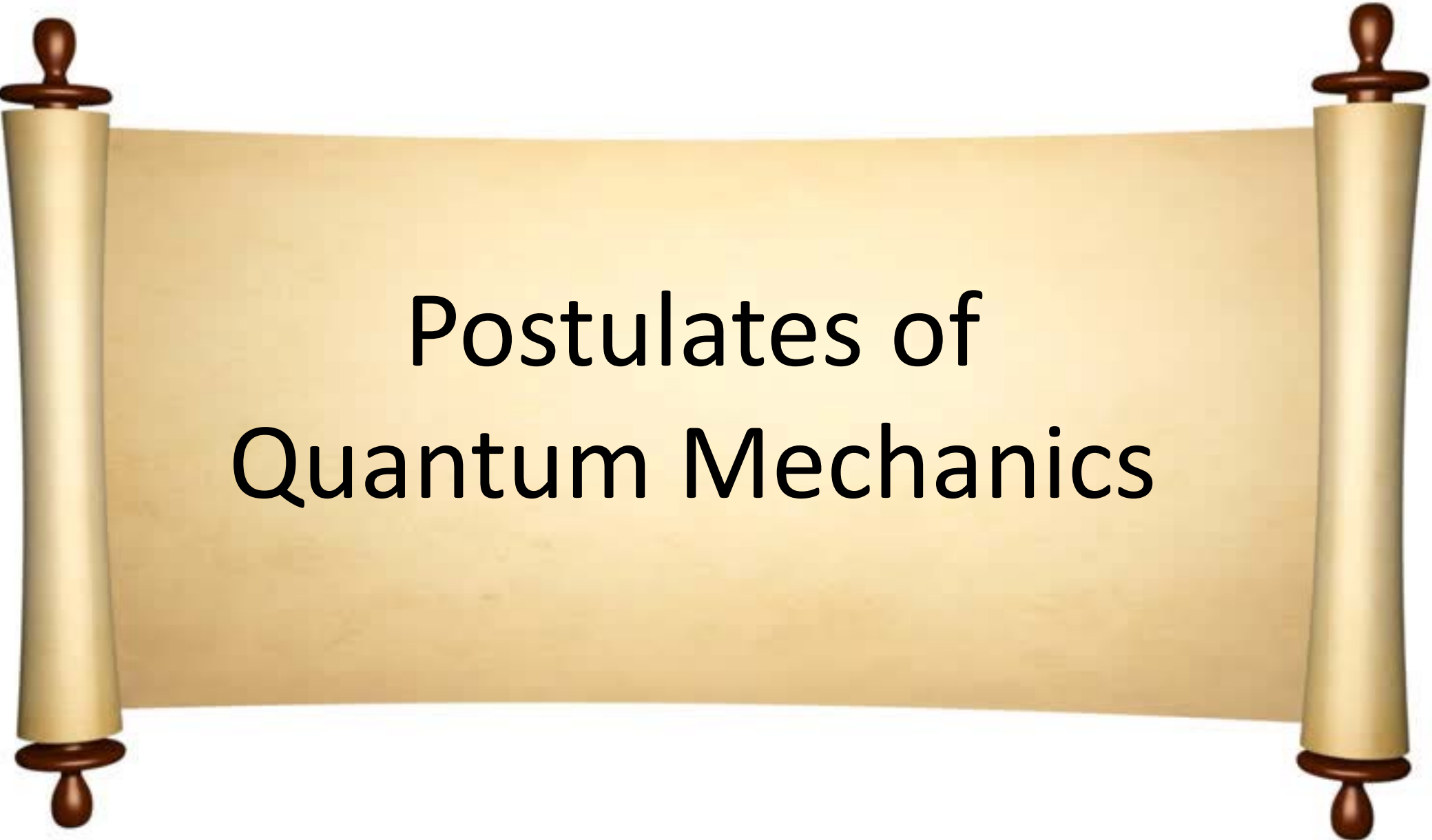
- The coefficients are determined by the inner product

$$\langle e_k | a \rangle = \langle e_k | \sum_i \alpha_i e_i \rangle = \sum_i \alpha_i \langle e_k | e_i \rangle = \alpha_k$$

$$a = \sum_i e_i \langle e_i | a \rangle$$

Hilbert Space

- A Hilbert Space is a vector space over the complex numbers with an inner product $\langle b | a \rangle$
- It maps an ordered pair of vectors to the complex numbers with the following properties
 - Positivity $\langle a | a \rangle > 0$ for $|a\rangle \neq 0$
 - Linearity $\langle c | (\alpha |a\rangle + \beta |b\rangle) = \alpha \langle c | a \rangle + \beta \langle c | b \rangle$ where α and β are complex constants
 - Skew symmetry $\langle b | a \rangle = (\langle a | b \rangle)^*$
- For these discussion the space is complete as expressed by the norm
$$||a|| = (\langle a | a \rangle)^{1/2}$$



Postulates of Quantum Mechanics

Postulate 1

1. 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

Postulate 1 Implications for Quantum Computing

Mathematical representation of a quantum system

- Every isolated system has an associated complex vector space with an inner product that is the state space of the system
- A unit vector in the system's state space is a state vector that is a complete description of the physical system

Dirac “bra” and “ket” Notation

- 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}

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

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} and is sometimes called the Hermitian conjugate

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

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

Postulate 1 Implications for Quantum Computing

- This postulate implies that the superposition of two states in the Hilbert Space A is again a state of the system.

- Composite System

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” $H_A \otimes H_B$

Tensor Product

- Let A and B be represented by the matrix formulations

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$$

$$A \otimes B = \begin{bmatrix} a \begin{pmatrix} e & f \\ g & h \end{pmatrix} & b \begin{pmatrix} e & f \\ g & h \end{pmatrix} \\ c \begin{pmatrix} e & f \\ g & h \end{pmatrix} & d \begin{pmatrix} e & f \\ g & h \end{pmatrix} \end{bmatrix}$$

Another Surprising Example of Quantum Behavior

Quantum Entanglement

- Quantum entanglement is a phenomenon in quantum mechanics when
 - 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

Entanglement

Mathematical Framework

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

$$H_A \otimes H_B$$

- 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

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

Quantum Entanglement Basis States

- 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

Quantum Entanglement 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

Postulate 2

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

Postulate 2 Implications for Quantum Computing

- Acting with an operator on a state in general changes the state.
- There are special states that are not changed (except for being multiplied by a constant) by the action of an operator

$$\hat{A}|\psi_a\rangle = a|\psi_a\rangle$$

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

Postulate 3

3. The only possible result of the measurement of an observable " O " is one of the eigenvalues of the corresponding operator " \hat{O} ".

Postulate 3 Implications for Quantum Computing

- This postulate is the basis for describing the discreteness of measured quantities i.e. “quantized”
- Experimental measurements are described by real numbers
 - ➔ the eigenvalues of quantum operators describing the real world must be Hermitian
- Hermitian operators are orthogonal ➔ $\langle a_j | a_k \rangle = \delta_{jk}$
- They span the space ➔ they form a basis
 - An arbitrary state can be expanded as a sum of the eigenstates of a Hermitian operator (with complex coefficients)
 - This implies the property that the set of states are “complete”

Postulate 4

- 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 $|a_n\rangle$, $|\langle a_n | \psi \rangle|^2$

Postulate 4 - Implications for Quantum Computing

- The complex number $\langle a_n | \psi \rangle$ is a “probability amplitude”. This quantity is not directly measurable
- To obtain an expectation value must square probability amplitude
- The probability of obtaining some result must be 1.

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

- There are complex coefficients in the probability amplitude that must be summed and then multiplied to obtain the expectation value

Postulate 5

5. The operator \hat{A} corresponding to an observable that yields a measured value “ a_n ” will correspond to the state of the system as the normalized eigenstate $|a_n\rangle$

Postulate 5 Implications for Quantum Computing

- This postulate describes the collapse of the wave packet of probability amplitudes when making a measurement on the system
- 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

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

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 of inserting
 - Intermediate print statements
 - Checkpoint re-startsdisallowed by quantum mechanics in a quantum computer

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

Postulate 6

Dynamics - Time Evolution of a Quantum Mechanical System

- 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 of the state of a closed quantum system is described by the Schrodinger equation

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

Postulate 6 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 (conservation of probability)
- Requirement that each “step-by-step” evolution must preserve unitarity (forces constraints for “programming” a quantum computer)
- The requirement of postulate 6 that the quantum mechanical system be closed for this unitary evolution of the system over time (forces constraints for “programming” a quantum computer)

Quantum Computer Properties And Characteristics

Quantum Mechanical Properties of Single Qubits

Bits, Qubits and Superposition

- A classical bit defines a state by values of either “0” or “1” (“on” or “off”)



Bits, Qubits and Superposition

- A classical bit defines a state by values of either “0” or “1” (“on” or “off”)
- A quantum bit (qubit) can also have a state of “0” or “1” but it can also have a possibility of being described by additional states



Bits, Qubits and Superposition

- A classical bit defines a state by values of either “0” or “1” (“on” or “off”)
- A quantum bit (qubit) can also have a state of “0” or “1” and it can also have a possibility of being described by additional states
- Qubit can form a superposition state represented by a vector that is a superposition or linear combination of both a “0” or “1”

$$|a\rangle = \alpha|0\rangle + \beta|1\rangle \quad |\alpha|^2 + |\beta|^2 = 1$$



Basis vectors for One Qubit

- In Dirac notation this is (α and β are complex coefficients)

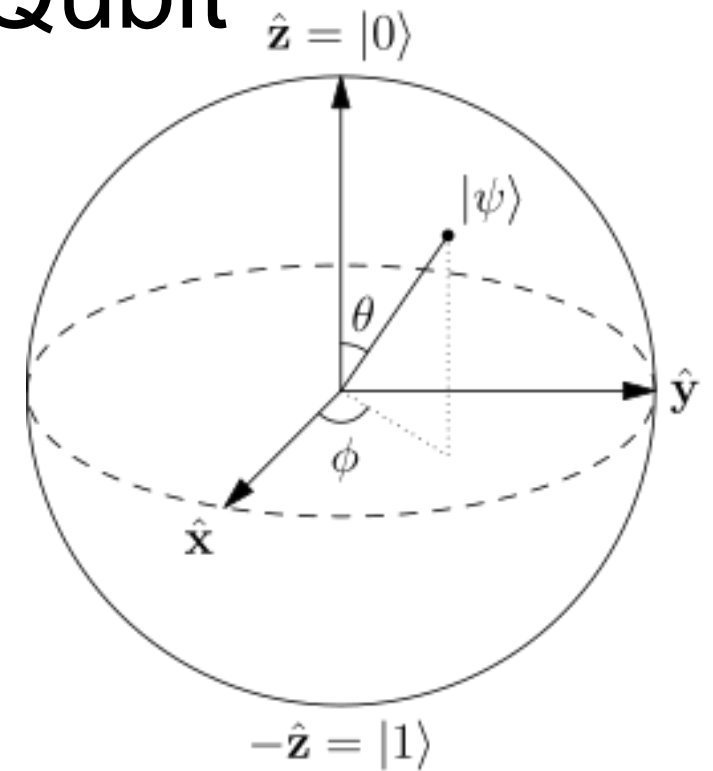
$$a = \alpha|0\rangle + \beta|1\rangle \quad |\alpha|^2 + |\beta|^2 = 1$$

- α is the probability amplitude of measuring the $|0\rangle$ state and β is the probability amplitude of measuring the $|1\rangle$ state
- Common basis is $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$
- Probability to measure the $|0\rangle$ state is $|\alpha|^2$
- Probability to measure the $|1\rangle$ state is $|\beta|^2$

Mathematical Properties of One Qubit

- Uses a data representation known as a qubit with the property that combinations of “0”s and “1”s can represent many different values simultaneously
- Can re-write $|a\rangle = \alpha|0\rangle + \beta|1\rangle$ as $|\alpha|^2 + |\beta|^2 = 1$

$$|a\rangle = e^{i\gamma} \left(\cos\left(\frac{\theta}{2}\right) |0\rangle + e^{i\phi} \sin\left(\frac{\theta}{2}\right) |1\rangle \right)$$



Bloch Sphere

Figure from Wikipedia Bloch Sphere
https://en.wikipedia.org/wiki/Bloch_sphere

- This representation is visualized by states that lie on the surface of a sphere

Matrix Representations of Single Qubit Transformations

- The matrix representation of single qubit combinations $\sum_i |input_i\rangle\langle output_i|$
- Can construct various 2x2 matrix representations

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

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

$$Z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$Y = iXZ = i \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = i \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$H = \frac{1}{\sqrt{2}} [(|0\rangle + |1\rangle)\langle 0| + (|0\rangle - |1\rangle)\langle 1|] = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Matrix Representations of Single Qubit Transformations

$$\begin{array}{lcl}
 \text{Pauli X} - \boxed{\text{X}} - & \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & = \sigma_x \\
 \text{Pauli Y} - \boxed{\text{Y}} - & \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} & = \sigma_y \\
 \text{Pauli Z} - \boxed{\text{Z}} - & \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} & = \sigma_z
 \end{array}
 \left. \vphantom{\begin{array}{l} \text{Pauli X} \\ \text{Pauli Y} \\ \text{Pauli Z} \end{array}} \right\} \boxed{\text{Pauli Spin Matrices}}$$

$$\text{Hadamard} - \boxed{\text{H}} - \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

- **Phase shift (R_ϕ) gates.** Leaves the basis state $|0\rangle$ unchanged and maps $|1\rangle$ to $e^{i\phi} |1\rangle$ modifying the phase of the quantum gate. Pictorially traces a horizontal circle on the Bloch Sphere by ϕ radians (line of latitude)

$$\text{Phase} - \boxed{\text{S}} - \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad \frac{\pi}{8} - \boxed{\text{T}} - \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$$

Qubits and Gates

- Matrices describe the rotations that takes a qubit from an initial state to a transformed state
- These rotations that operate on a qubit are labelled as “gates”
- Because qubit states can be represented as points on a sphere, reversible one-qubit gates can be thought of as rotations of the Bloch sphere. (quantum gates are often called “rotations”)
- Reversible one qubit gates viewed as rotations in this three dimensional representation

Classical Gates versus Quantum Gates

- A classical computer gate is a logical construction of an 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

Building Quantum Computing Gates

- Gates are the building blocks for constructing quantum circuits
- Quantum mechanics restricts the types of gates that can be constructed
- Quantum circuits are constructed from the combined actions of unitary transformations and single bit rotations

Imposing Quantum Mechanics on 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 transformation are described through matrix rotations

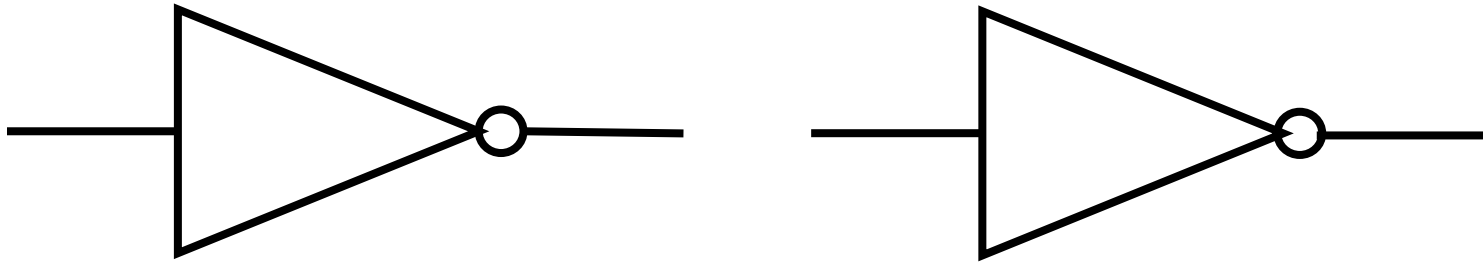
Quantum Computing Gate Operations Under the Constraints of Quantum Mechanics

- 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

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

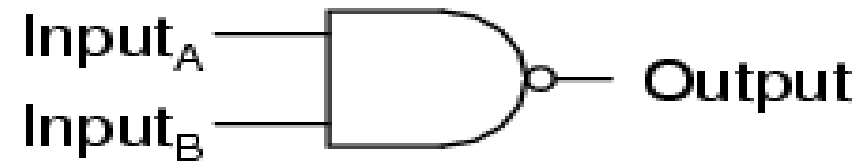
- These states can also be represented by

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

Consequences for Quantum Computing

- NAND gate is a fundamental building block for digital computers

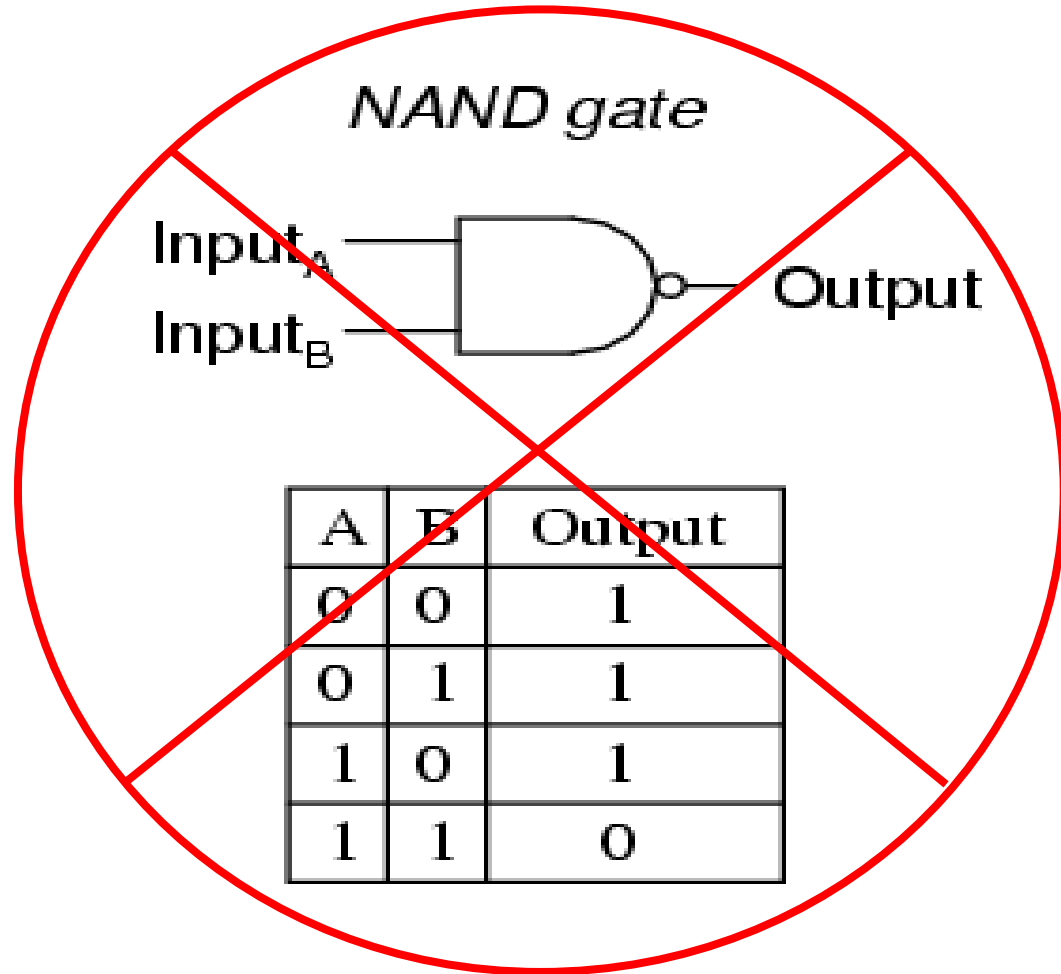
NAND gate



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

Consequences for Quantum Computing

- NAND gate is not reversible



Design Reversible 2 Qubit Gate

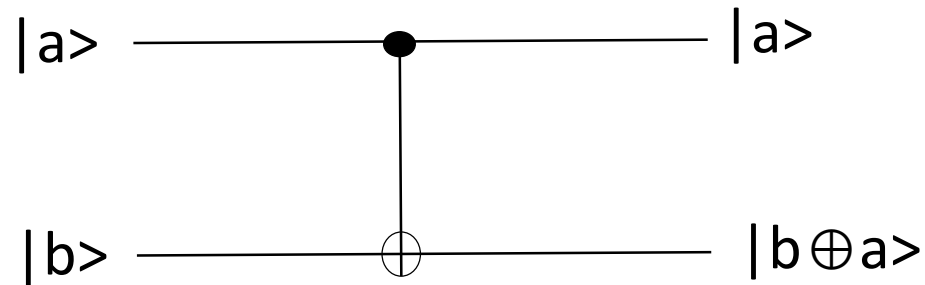
Controlled-NOT Gate

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

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

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

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

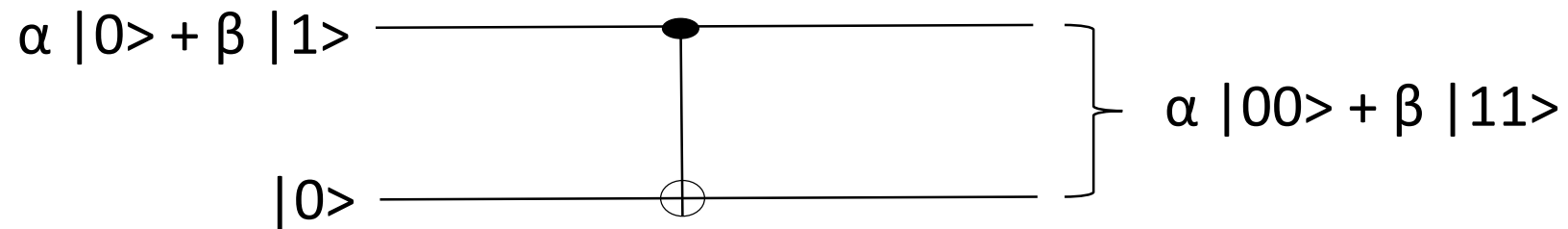
Building a Reversible 2 Qubit Gate

- 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



- This output is not possible because the general state vector transforms as

$$|a\rangle|a\rangle = (\pm |0\rangle + \pm |1\rangle) (\pm |0\rangle + \pm |1\rangle)$$

$$|a\rangle|a\rangle = \pm^2 |00\rangle + \pm^2 |01\rangle + \pm^2 |10\rangle + \pm^2 |11\rangle$$

$$(\pm^2 \neq 0 \text{ and } \pm^2 \neq 0)$$

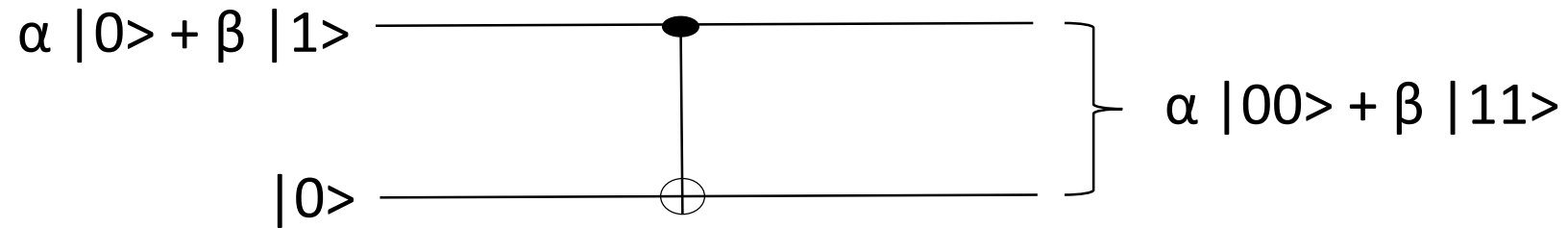
Cannot design traditional parallel programming equivalents by copying unknown quantum states in a quantum computer

Leads to The No-Cloning Theorem

It is impossible to create an identical copy of an arbitrary unknown quantum state

Quantum Information - No Cloning Theorem

- Consider the CNOT quantum gate and a linear superposition state $\alpha |0\rangle + \beta |1\rangle$ and an additional bit initialized to zero



- Quantum mechanically this output is not possible because the general state vector

$$|a\rangle|a\rangle = (\alpha |0\rangle + \beta |1\rangle) (\alpha |0\rangle + \beta |1\rangle)$$

$$|a\rangle|a\rangle = \alpha^2 |00\rangle + \alpha\beta |01\rangle + \beta\alpha |10\rangle + \beta^2 |11\rangle \quad (\alpha\beta \neq 0 \text{ and } \beta\alpha \neq 0)$$

- The quantum circuit does not copy the part of the state vector with the terms $\alpha\beta |01\rangle + \beta\alpha |10\rangle$
- The No-Cloning Theorem**: It is impossible to create an identical copy of an arbitrary unknown quantum state
- This implies that signal fanout is not permitted

Other Controlled Gates

- Controlled U gate is a gate that operates on two qubits in such a way that the first qubit serves as a control. It maps the basis states as follows

$$|00\rangle \rightarrow |00\rangle$$

$$|01\rangle \rightarrow |01\rangle$$

$$|10\rangle \rightarrow |1\rangle \otimes U|0\rangle = |1\rangle \otimes (u_{00}|0\rangle + u_{10}|1\rangle)$$

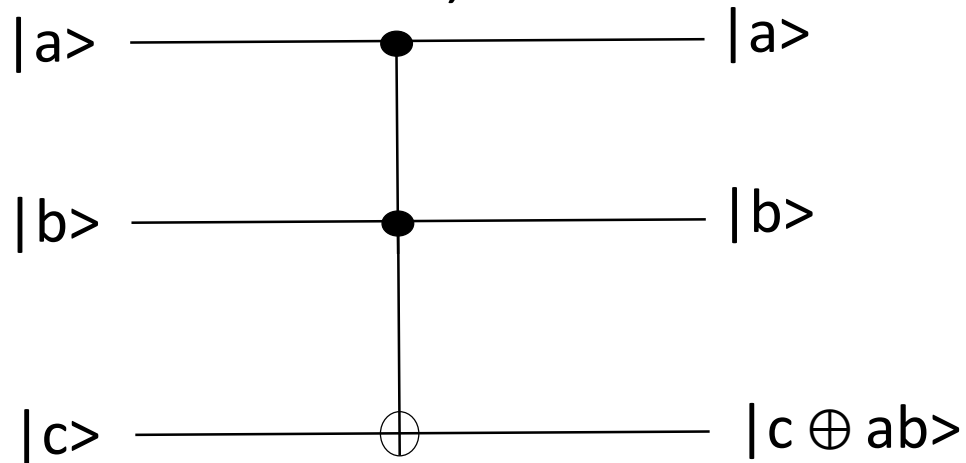
$$|11\rangle \rightarrow |1\rangle \otimes U|1\rangle = |1\rangle \otimes (u_{01}|0\rangle + u_{11}|1\rangle)$$

$$C(U) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{pmatrix}$$

- U represents one of the Pauli matrices σ_x σ_y σ_z
- Controlled-X, Controlled-Y, Controlled-Z gates

Toffoli Gate

- The Toffoli gate is a 3-bit gate, which is universal for classical computation
- If the first two bits are in the state $|1\rangle$, it applies a Pauli-X (NOT) on the third bit, otherwise the state is left unchanged



Toffoli Gate Truth Table and Matrix

INPUT			OUTPUT		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

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

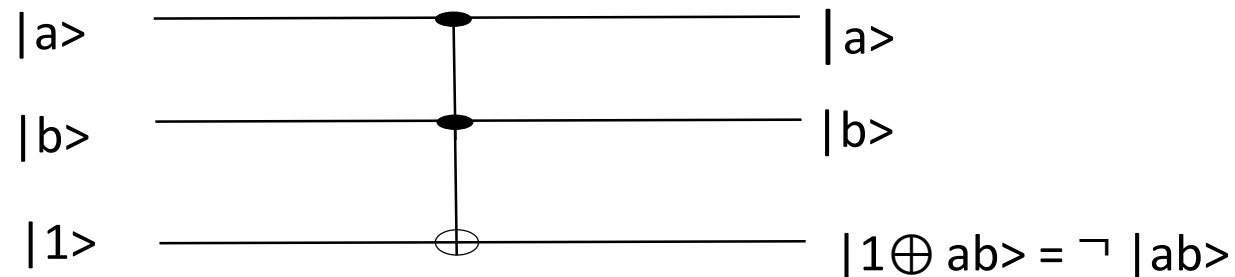
X Gate
Pauli σ_x rotation matrix

Properties of Toffoli Gates

- Toffoli Gate is a reversible gate (i.e. $U_T^{-1}U_T=I$) or
- Toffoli gate is used to replace a classical circuit with the equivalent reversible gate
- Two bits are control bits ($|a\rangle$ and $|b\rangle$) and target bit $|c\rangle$ is flipped as per the truth table

$$(a, b, c) \rightarrow (a, b, c \oplus ab) \rightarrow (a, b, c)$$

- Toffoli gate can be used to simulate a NAND Gate



Toffoli Gate as a Universal Gate

- A Toffoli gate constructs the AND logic state when $c = 0$
- A Toffoli gate constructs the NAND when $c = 1$
- Every Boolean function has a reversible implementation using Toffoli gates

Quantum Computing Simulator

- Go to the URL <http://algassert.com/quirk>
- Select “Edit Circuit”

Menu Export Clear Circuit Clear ALL Undo Redo Make Gate Version 2.1

Toolbox

Probes	Displays	Half Turns	Quarter Turns	Eighth Turns	Sixteenths	Spinning	Parametrized	Silly
	Sample	Z Swap	$Z^{1/2}$ $Z^{-1/2}$	$Z^{1/4}$ $Z^{-1/4}$	$Z^{1/8}$ $Z^{-1/8}$	Z^t Z^{-t}	$Z^{A/2^n}$ $Z^{-A/2^n}$	0 ?
$ 0\rangle\langle 0 $ $ 1\rangle\langle 1 $	Density Bloch	Y	$Y^{1/2}$ $Y^{-1/2}$	$Y^{1/4}$ $Y^{-1/4}$	$Y^{1/8}$ $Y^{-1/8}$	Y^t Y^{-t}	$Y^{A/2^n}$ $Y^{-A/2^n}$	—
	Chance Amps	\oplus H	$X^{1/2}$ $X^{-1/2}$	$X^{1/4}$ $X^{-1/4}$	$X^{1/8}$ $X^{-1/8}$	X^t X^{-t}	$X^{A/2^n}$ $X^{-A/2^n}$...

drag gates onto circuit

Local wire states (Chance/Bloch)

Final amplitudes

Toolbox2

X/Y Probes	Order	Frequency	Inputs	Arithmetic	Compare	Modular	Custom Gates
\ominus \oplus	$+[t]$ $-[t]$	QFT QFT †	input A A=# default	+1 -1	$\oplus A < B$ $\oplus A > B$	+1 -1 mod R	
\otimes \otimes	Reverse	Grad $^{1/2}$ Grad $^{-1/2}$	input B B=# default	+A -A	$\oplus A \leq B$ $\oplus A \geq B$	+A -A mod R	
$ \ominus \rangle \langle \ominus $ $ \oplus \rangle \langle \oplus $		Grad t Grad $^{-t}$	input R R=# default	+AB -AB	$\oplus A = B$ $\oplus A \neq B$	$\times A$ $\times A^{-1}$ mod R	
$ \otimes \rangle \langle \otimes $ $ \otimes \rangle \langle \otimes $				$\times A$ $\times A^{-1}$		$\times B^A$ $\times B^{-A}$ mod R	

Questions

Contact Information

Patrick Dreher

Chief Scientist

NCSU IBM Q Quantum Computing Hub

NC State University

padreher@ncsu.edu